ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО
ПУБЛИЧНА АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ

КИБЕРСИГУРНОСТ И ВЪЗМОЖНОСТИ ЗА ПРИЛОЖЕНИЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ

Димитрина Полимирова, Велизар Шаламанов, Николай Стоянов,
Тодор Тагарев, Янцислав Янакиев, Георги Шарков,
Явор Папазов, Васил Ризов, Красимира Иванова

Проект „Работим за хората“ – укрепване капацитета на институциите за посрещане на предизвикателствата на съвременните публични политики“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

www.eufunds.bg

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО ПУБЛИЧНА АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА ДОБРО УПРАВЛЕНИЕ

ДОКЛАД

ОТ ПРОВЕЖДАНЕ НА ИЗСЛЕДВАНЕ ЗА УКРЕПВАНЕ НА АДМИНИСТРАЦИЯТА

НА ТЕМА:

КИБЕРСИГУРНОСТ И ВЪЗМОЖНОСТИ ЗА ПРИЛОЖЕНИЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ

НЛКВ – БАН

София, 2018 г.

Проект „Работим за хората“ - укрепване капацитета на институциите за посрещане на предизвикателствата на съвременните публични политики“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО ПУБЛИЧНА
АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ

Димитрина Полимирова, Велизар Шаламанов, Николай Стоянов, Тодор Тагарев, Янцислав Янакиев, Георги Шарков, Явор Папазов, Васил Ризов, Красимира Иванова, *Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България* (София: Институт за публична администрация, 2019 г.).

Научни редактори:
доц. Димитрина Полимирова
доц. Велизар Шаламанов
доц. Николай Стоянов

Научен рецензент: проф. Аврам Ескенази

ISBN 978-619-7262-14-8

Настоящата монография е издадена по проект *„Работим за хората“ - укрепване капацитета на институциите за посрещане на предизвикателствата на съвременните публични политики“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд*

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО ПУБЛИЧНА АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА ДОБРО УПРАВЛЕНИЕ

СЪДЪРЖАНИЕ

СПИСЪК НА ФИГУРИТЕ

СПИСЪК НА СЪКРАЩЕНИЯТА

ACERTA	Academic CERT Association
ADKAR	Awareness, Desire, Knowledge, Ability, Reinforcement
AHP	Analytic Hierarchy Process
AI	Artificial Intelligence
BG-CERT	Екип за реагиране при кибер инциденти в България
BSc	Balanced Score Cards
CCOMC	Център за управление на сложни кризисни операции към НАТО
CEF	Connecting Europe Facility
CEPOL	Европейски полицейски колеж
CERT	Computer Emergency Response Team
CERT-RMM	Resilience Management Model
CMMI	Capability Maturity Model Integration
CSDP	Common Security and defense Policy
DNS	Domain Name System
DOTMLPFI	Компоненти на способностите: Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Interoperability
EC3	Европейски център за кибер престъпления към Европол
ECTEG	Европейската група за обучение и образование в областта на кибер престъпленията
EDA	Европейска агенция по отбрана
EDA CAPTECHs	Европейска агенция по отбрана – технологии за развитие на способности
EDTIB	Европейска отбранителна технологична и индустриална база
ELISA	Европейска агенция за големи информационни истеми
ENISA	Европейска агенция за мрежова сигурност
EP3R	European Public-Private Partnership for Resilience
ESDC	European Security and Defence College
ETEE	Образование, обучение, учения и експериментиране
EUMS INT	Дирекция „Разузнаване“ на Военния комитет на ЕС
GDPR	Обща регулация за защита на данните на ЕС
INTCEN	Център за анализ на разузнавателните служби на ЕС
IT	Информационнни технологии
ITIL	IT Infrastructure Library
JTSAC	Център за съвместно обучение, симулации и анализ
MASFAD	Multi-Agent System For Advanced persistent threat Detection

MISP	Платформа за разпространение на информация за зловреден софтуер
MISP	Malware Information Sharing Platform
MITRE	Корпорация за управление на приложни изследвания в САЩ
MN CD E & T	многонационално образование и обучение в кибернетичната отбрана
MSP	Management Successful Programs
NATO CCD CoE	NATO Cooperative Cyber Defence Centre of Excellence
NATO STO	Организация за наука и технологии на НАТО
NCI Academy	Академия за комуникация, информация и кибер отбрана на НАТО
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCIRC	център на НАТО за реагиране при компютърни инциденти
NDC	Колеж по отбраната на НАТО в Рим, Италия
NSS	Училище на НАТО в Оберамергау, Германия
P2P	Peer-to-Peer
PEST	Political, Economic, Social, Technological analysis
PoS	Proof of Stake, Доказателство за залог
PoW	Proof of Work, Доказателство за работа
RACI	Матрица на процесите: Responsible, Accountable, Coordinated, Informed
Sitroom	Ситуационен център
SWOT	Strengths, Weaknesses , Opportunities, Threats
TLD	Top-level domain
VNC	Voluntary National Contribution
АИС	Автоматизирана информационна система
ГИМ	Главен информационен мениджър
ДА	Държавна администрация
ДАЕУ	Държавна агенция „Електронно управление“
ДАК	Държавна агенция „Киберсигурност“
ДАНС	Държавна агенция „Национална сигурност”
ДЦУ	Доставчици на цифрови услуги
ЕК	Европейска комисия
ЕП	Европейски парламент
ЕРИКС	Екипи за реакция при инциденти в киберсигурността
ЕС	Европейски съюз
ЗЕУ	Закон за електронното управление
ЗКС	Закон за кибер сигурност

ЗУФСЗНС	Закон за управление и функциониране на системата за защита на националната сигурност
ИИ	Изкуствен интелект
ИИКТ	Институт по информационни и комуникационни технологии
ИКТ	информационни и комуникационни технологии
ИМИ	Институт по математика и информатика
ИР	информационни ресурси
ИТ	информационни технологии
КС	Кибер сигурност / консултативен съвет
МВР	Министерство на вътрешните работи
МИС	мрежова и информационна сигурност
МКС	мениджър по киберсигурност
МОН	Министерство на образованието и науката
МС	Министерски съвет
МТИТС	Министерството на транспорта, информационните технологии и съобщенията
НАТО	Организацията на Северноатлантическия договор
НИТ	Нови информационни технологии
НЛКВ	Национална лабораторията по компютърна вирусология
ННП	Национална научна програма
НПО	Национална програма за обучение
НФНИ	(национален) Фонд научни изследвания
ООН	Организация на обединените нации
ОП ОНИР	Оперативна програма „Наука и образование за интелигентен растеж“
ОПСО	Обща политика за сигурност и отбрана
ОССЕ	Организация за сигурност и сътрудничество в Европа
ОСУ	оператори на съществени услуги
ПА	публична администрация
ПКЗНБАК	Постоянна комисия за защита на населението при бедствия, аварии и катастрофи
СЦОСА	Съвместен център за обучение, симулации и анализ
ТУ-София	Технически университет
Х2020	Хоризонт 2020
Х-Е	Хоризонт Европа

УВОД

Настоящият отчет по проект с предмет: „Провеждане на изследване за укрепване на администрацията на тема: „Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България“[1] следва зададените дейности в техническата спецификация на Заявителя – Института за Публична Администрация към Министерския съвет:

Дейност 1: *Анализ на държавната политика в областта на кибер сигурността. Обзор и анализ на регулаторните инструменти, политики и стратегии на НАТО и ЕС, които влияят на кибер сигурността на България.*

Дейност 2: *Идентифициране на критични точки и перспективи. Представяне на ясна визия за подобряване на кибер сигурността на публичния сектор в България.*

Дейност 3: *Общ преглед на блокчейн технологията. Сравнение между публични и частни блокчейни - особености, предимства и недостатъци. Анализ на същността и възможностите за приложение на блокчейн технологиите в работата на държавната администрация и връзката им с кибер сигурността.*

Дейност 4: *Представяне на примери и визия за приложение на блокчейн в работата на държавната администрация, включително при изграждането и поддържането на публични регистри и очакваните резултати от това.*

Дейност 5: *Анализ на възможностите за използване на изкуствен интелект и чатботове при предоставяне на услуги и комуникация с потребителите, както и за поддържане на кибер сигурността.*

Дейност 6: *Представяне на визия за бъдещето. Очаквани резултати на всички нива, от внедряването на иновативни решения в дейността на държавната и публичния сектор.*

Изследването е проведено под ръководството на **доц. Димитрина Полимирова** (НЛКВ-БАН) от съвместен екип с експерти от няколко звена (ИИКТ-БАН, ИО-МО, ЕСИ ЦИЕ).

[1] Проектът е стартирал на 19.09.2018 г., а отчетът е завършен на 14.12.2018 г.

Резултатите са изложени в три глави – първа глава покрива резултатите по дейност 1 и 2, вкл. анализ на проведената анкета с експерти от администрацията, индустрията и академичния сектор, втора глава представя резултатите по дейности 3, 4 и 5 за изследване на приложимостта на иновативни технологии като блокчейн и изкуствен интелект, а трета глава представя разработените алтернативи за развитие на организацията за кибер сигурност в държавната администрация на България и предлаганата Визия за реализация на предпочитания вариант с възможност за приложение на иновативни технологии.

Развитието на информационните и комуникационни технологии и дигитализацията като глобален феномен промениха характера на съвременните общества от „технологични“ в „информационни“ в една качествено нова, *информационна* ера. Държавата, бизнесът и гражданите разчитат на лесен достъп и надеждно функциониране на взаимосвързани комуникационни и информационни системи и технологии, и интернет средата или на новото киберпространство, в което вече живеем и се развиваме.

Българското общество като част от глобалното интернет семейство, се развива интензивно и уверено в цифровата и информационна ера. Дигиталните инфраструктури се превръщат в гръбнак или критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на модерна и иновативна икономика, прозрачно управление, на модерно и демократично гражданско общество.

Същевременно, нарастващата и необратима дигитална зависимост на основните функции и дейности на обществото поражда нови значими рискове и заплахи. Киберпространството носи нови уязвимости с непознат досега мащаб и потенциална сила на въздействие, които изискват повишаване на общата кибер култура и колективна киберсигурност на цялото общество, прилагане на активни мерки за предпазване от известните видове заплахи (от небрежност до умишлени действия, използване на технически и човешки слабости), както и подготовка за „неизвестните неизвестни“ и постигане на кибер устойчивост във всички сфери.

Целта на настоящото изследването е установяване на празноти в регулациите на дейностите по кибер сигурност и устойчивост в Република България, идентифициране на добри практики в Европейския съюз и НАТО и дефиниране на предложения за усъвършенстване на регулаторната рамка, политики и стратегии за гарантиране на сигурно и устойчиво функциониране на държавата, икономиката и обществото в кибер пространството.

Разработката на Препоръки за усъвършенстване на държавната политика в областта на кибер сигурността се базира на анализ на държавната политика в областта на кибер сигурността и обзор и анализ на регулаторните инструменти, политики и стратегии на НАТО и ЕС, които влияят на кибер сигурността на България. Дейност 1 е изпълнена от екип, ръководен от доц. д-р Велизар Шаламанов.

Фигура 1. Архитектура на системата / организацията за кибер сигурност

Изследването се базира на общият модел за анализ по базовата архитектура на системата за кибер сигурност (Фигура 1). Кибер сигурността се постига чрез успешни кибер операции на организацията за кибер сигурност. Самата организация/система се гради на базата на:

1) документи – с фокус на цели, процеси, организация:
   1.1) концепции;
   1.2) стратегии и пътни карти;
   1.3) закони;
   1.4) планове и програми, бюджети;
2) организации (в съответствие с документите):
   2.1) елементи в НАТО и ЕС, други международни организации с влияние по кибер сигурността;
   2.2) елементи на ниво Парламент, Правителство, Президентска институция;
   2.3) елементи по министерства и ведомства, местна власт;

2.4) елементи в бизнеса;
2.5) елементи в академичния сектор и неправителствен сектор;

3) системи (в съответствие с документите):
3.1) състояние на ИТ системите на държавната информация;
3.2) състояние на системите за кибер сигурност;
3.3) системна връзка на ДА с бизнеса и академичния сектор;
3.4) системна връзка на ДА с НАТО и ЕС;

4) ресурси (в съответствие с документите):
4.1) финансови ресурси за ИТ в администрацията;
4.2) финансови ресурси за кибер сигурност (вкл. мрежова и информационна сигурност) в ДА;
4.3) състояние на човешкия ресурс за ефективно и ефикасно управление на ИТ и кибер устойчивост, връзки с индустрията, академичния сектор НАТО и ЕС за помощ и ротация на персонал;
4.4) развитие на идеята за „кибер резерв";

5) капацитет за управление на промяната в сферата на ефективно, ефикасно и кибер устойчиво управление на информационните ресурси (в съответствие с документите);
6) ниво на международно сътрудничество, вкл. кибер дипломация (в съответствие с документите);
7) капацитет за демократичен контрол върху системата за кибер сигурност (в съответствие с документите).

Оценката на текущото състояние се извършва по метода SWOT и се определя на нивото на зрялост на системата за кибер сигурност в България по модела CMMI. На тази основа и в контекста на възможностите на рамката за кибер сигурност на НАТО и ЕС са разработени и препоръките за усъвършенстване.

Използваните методи са: изследване на документи, интервюта и анкети, участие в срещи със заинтересовани лица, системен анализ на събраните материали, консултиране с експерти, организационно проектиране на структури за ръководство и управление на кибер сигурността, участие в учения / симулации по кибер сигурност, провеждане на мозъчна атака, сравнение и оценка на варианти и синтез на рационален вариант (AHP метод – аналитичен йерархичен процес за вземане на решение чрез сравняване и избор на алтернативи) за детайлна разработка.

В **първа глава,** под общото ръководство на **доц. Велизар Шаламанов**, като ключов експерт „Анализ и проучване“, **първи раздел** започва с преглед на актуални политики, стратегии, закони и други актове, формиращи *държавната политика в областта на кибер сигурността и подготовка на анализ на състоянието* от **проф. д-р Тодор Тагарев** и **г-н Васил Ризов** с участие на други експерти от екипа по проекта**.** Резултатът е представен в секция „*Национална политика в областта на кибер сигурността*“ и приложения 1 и 2.

Следва преглед на актуални политики, стратегии и други актове (вкл. стандарти за информационна сигурност и кибер устойчивост, както и на модели на зрялост на организации, с приложимост в публичната администрация и е-Управление) на НАТО и ЕС, влияещи на ***държавната политика в областта на кибер сигурността и анализ на състоянието*** *(консултиран с представители на НАТО и ЕС)* от **проф. д.н. Янцислав Янакиев.** Резултатът е представен в секция „*Обзор и анализ на регулаторните инструменти, политики и стратегии на НАТО и ЕС, които влияят на киберсигурността на България*“.

На базата на анализа са разработени препоръки за усъвършенстване на ***държавната политика в областта на кибер сигурността от доц. д-р Велизар Шаламанов,*** представени в съответната секция „*Препоръки за усъвършенстване на държавната политика в областта на кибер сигурността*“.

Вторият раздел от първа глава е насочен към идентифициране на критични точки и перспективи в сферата на кибер сигурността на базата на направения анализ с цел представяне на ясна визия за подобряване на кибер сигурността на публичния сектор в България.

Предложена е система от мерки за повишаване капацитета на структури и звена в държавната администрация на България по въпроси, свързани с киберсигурността от **д-р Георги Шарков.**

Представени са резултатите от проучване (анкета и кръгла маса) на възможности за изграждане на продуктивна връзка и взаимодействие между центрове за научни и приложни изследвания, водещи софтуерни и ИКТ фирми и публичния сектор в България от **доц. д-р Димитрина Полимирова.** В тази си част изследването акцентира върху идентифициране на основни академични звена по кибер сигурност в България и ИКТ фирми с активно присъствие на пазара за решения / услуги по кибер сигурност. Анализира се дискусията на кръглата маса по взаимодействие между академични звена, индустрия и публичния сектор в сферата на кибер сигурността и определяне на критични точки / перспективи с визия за подобряване на взаимодействието между

академични звена, индустрия и публичния сектор в сферата на кибер сигурността.

В общите рамки на изследването, представени в първа глава, са представени и възможности за използване на различни механизми за подкрепа за стимулиране на международно сътрудничество във връзка с приоритетно развитие на цифровата икономика и намирането на иновативни решения за дейността на държавата и публичния сектор.

В секция „Система от мерки за повишаване капацитета на структури и звена в държавната администрация на България по въпроси свързани с кибер сигурността“ на базата на проведеното изследване и консултирането му с група представители от администрацията, индустрията и академичната общност на кръглата маса от 15.11.2018 г. по кибер сигурност с администрацията и привличане на индустрия и академични звена **доц. д-р Велизар Шаламанов** предлага препоръки за усъвършенстване на съществуващата система на базата на рамката от НАТО и ЕС и на известни добри практики и целят да подготвят алтернативи на текущото състояние на организацията за кибер сигурност и оценката им за изработване на дългосрочна визия за промяна.

Съществуващата организация за е-Управление и кибер сигурност се базира основно на Закона за е-Управление и Закона за Кибер сигурност.

Във **втора глава** под общото ръководство на **доц. д-р Николай Стоянов**, като ключов експерт „Кибер сигурност и иновативни технологии“ е направен анализ на възможностите за използване на иновативни технологии (като блокчейн, изкуствен интелект и чатботове) в публичния сектор и в работата на държавната администрация.

В **първи раздел** на тази глава е направен общ преглед на основните елементи на блокчейн технологията и са описани основните видове блокчейн технологии. Посочени са основни елементи и характеристики на блокчейн технологията. В анализа на всяка иновативна технология се включват и въпросите, които имат отношение към сигурността – аспекти и направления, в които трябва да се разглежда и оценява сигурността на блокчейна, разгледани в секция „Сигурност“ на този раздел от тази глава. В край на този раздел е предложен подход за изчисляване на ползите и разходите от внедряване на тази технология в държавната администрация.

Във **втори раздел** на тази глава е направен преглед и анализ на световните тенденции и добри практики при внедряване на блокчейн технологията в държавната администрация и публичния сектор на Естония и Канада. На базата на този анализ са идентифицирани основните направления за приложение на тази технология в държавната администрация в България. Разгледани са и възможности за внедряване и

поддържане на публични регистри в България на основата на блокчейн технологията.

Екипът, участвал в разработването на първи и втори раздел от тази глава, е: **доц. д-р Николай Стоянов, доц. д-р Димитрина Полимирова, доц. д-р Красимира Иванова** и **Явор Папазов**.

Трети раздел от тази глава и разработен от **д-р Георги Шарков** и има за цел да систематизира съвременното състояние на изследванията и практическите възможностите, добрите практики и перспективите за използване на методите и средствата на ИИ за предоставяне на услуги и обслужване на потребители, основно за сектора на публичните услуги и администрация. В допълнение са разгледани и аспектите на използване на системи с изкуствен интелект (ИИ) в областта на киберсигурността (и по-общо – на сигурността и отбраната). Представени са основните групи етични, правни и социални аспекти на използването на ИИ, както и насоките за развитие на политики и стратегии в условията на развитие на цифровото общество и единен цифров пазар в ЕС. Дадени са и редица примери за използване на системи с ИИ в различни сфери услуги и дейности свързани с критични ресурси или „съществени услуги“.

В **трета глава** под общото ръководство на **доц. д-р Велизар Шаламанов**, се обобщават резултатите от изследването (включително на изводите от оценката на разработените от **проф. д-р Тодор Тагарев и г-н Васил Ризов** алтернативни модели за развитие на системата за кибер сигурност и използване на иновативни технологии в България), за да се дефинира *Визия за бъдещето – очаквани резултати на всички нива, от внедряването на иновативни решения в дейността на държавната администрация и публичния сектор.*

Първият раздел в трета глава – „Среда за кибер сигурност в България“ е насочен към дефиниране на средата за кибер сигурност за България в контекста на членство в НАТО и ЕС в следващите 3-5 години (вкл. стандартите, оперативната съвместимост и системите за споделяне на информация и съвместна бърза реакция). Тя е разработена от **д-р Георги Шарков** и покрива:

- основни рискове и заплахи за кибер сигурността в НАТО и ЕС със специфични измерения за България;
- стандарти за оперативната съвместимост и кибер сигурност / устойчивост в България и НАТО/ЕС;
- системи за споделяне на информация и съвместна бърза реакция в България и в рамките на НАТО и ЕС – провеждане на учения по кибер устойчивост.

Вторият раздел в трета глава представя алтернативни модели за развитие на системата за кибер сигурност и използване на иновативни технологии в България от **проф. д-р Тодор Тагарев** и **г-н Васил Ризов**:

- основни алтернативни решения за организация на националната система за кибер сигурност;
- основни критерии за оценка и избор на предпочитан вариант;
- анализ на оценките на експерти и изводи за развитие на организацията за кибер сигурност.

Оценката на разработените алтернативи е извършена чрез консултации с подбрани експерти от администрацията, индустрията и академичния сектор по анализ на алтернативите и развитие на Визия за бъдещето в сферата на кибер устойчивостта с отчитане на очакваните резултати на всички нива, от внедряването на иновативни решения в дейността на държавната администрация и публичния сектор. Интервютата са проведени **проф. Тодор Тагарев и г-н Васил Ризов** и е в контекста на създадената експертна мрежа с провеждане на кръглата маса през ноември, като детайлното представяне на резултатите е извън обхвата на настоящето изследване и е част от дисертационния труд на г-н Ризов.

Резултатите от началната оценка са представени в **раздел** „*Ранжиране на алтернативните модели за развитие на системата за кибер сигурност и използване на иновативни технологии*“. Отчитайки основата цел за избор на алтернатива (ефективно, ефикасно и кибер устойчиво управление на ИТ ресурсите в интерес на е-Управлението при минимална цена), очакваните резултати на всички нива от внедряването на иновативни решения в дейността на държавната и публичния сектор и приетите основни критерии за оценка на алтернативите изследването се фокусира върху описание на избраната алтернатива като визия за ефективно, ефикасно и кибер устойчиво управление на ИТ за е-Управление с отчитане на препоръките на консултираните експерти.

Последният раздел интегрира резултатите от цялото изследване с отчитане на изводите от всички дейности по проекта, за да очертае Визия за бъдещето в сферата на кибер устойчивостта: очаквани резултати на всички нива, от внедряването на иновативни решения в дейността на държавната и публичния сектор с фокус върху:

- **Модел на взаимодействие** между ПА, академичен и бизнес сектори за ефективност, ефикасност и кибер устойчивост на ИТ системите / организациите.
- **Модел на международно взаимодействие** за ефективност, ефикасност и кибер устойчивост на ИТ системите / организациите в публичния сектор на България.

- **Изисквания към Национална научна програма** „Ефективност, ефикасност и кибер устойчивост на ИТ системи / организации“.
- **Изисквания към сертификационна програма** за ИТ лидери и административни ръководители за Главни Информационни мениджъри / Мениджъри на кибер устойчивостта „Ефективност, ефикасност и кибер устойчивост на ИТ системи / организации“.
- **Роля на Регламент на ЕК и Съвета за създаване на Европейски център** за промишлени, технологични и изследователски експерти познания в областта на киберсигурността и Мрежа от национални координационни центрове в контекста на проекта по Х2020 за създаване на Европейска мрежа от центрове на компетентност с хъб за иновации и операции в Брюксел.

Този раздел е разработен от **доц. д-р Велизар Шаламанов, а валидацията на цялостното изследване бе организирана от доц. д-р Димитрина Полимирова** на работна среща на 10.12.2018 г. с представители на ИПА, ДАЕУ, ДАНС, МО, МВР (задочно със секретаря на Съвета за сигурност на МС) – основните институции по Закона за кибер сигурност.

ГЛАВА ПЪРВА

АНАЛИЗ НА ДЪРЖАВНАТА ПОЛИТИКА И ВИЗИЯ ЗА ПОДОБРЯВАНЕ НА КИБЕР СИГУРНОСТТА НА ПУБЛИЧНИЯ СЕКТОР В БЪЛГАРИЯ

АНАЛИЗ НА ДЪРЖАВНАТА ПОЛИТИКА В ОБЛАСТТА НА КИБЕР СИГУРНОСТТА. ОБЗОР И АНАЛИЗ НА РЕГУЛАТОРНИТЕ ИНСТРУМЕНТИ, ПОЛИТИКИ И СТРАТЕГИИ НА НАТО И ЕС, КОИТО ВЛИЯЯТ НА КИБЕР СИГУРНОСТТА В БЪЛГАРИЯ

НАЦИОНАЛНА ПОЛИТИКА В ОБЛАСТТА НА КИБЕР СИГУРНОСТТА

Първият раздел от доклада представя резултати от преглед на нормативните актове, формиращи основата на държавната политика в областта на кибер сигурността – както тези, които имат за основен предмет сигурността в кибер пространството, в т. ч. дейности и проекти по кибер отбрана и по противодействие на кибер престъпността, така и тези, които макар и с по-широк обхват, съдържат в себе си норми, определящи кое е дължимото поведение при осъществяване на дейности в кибер домейна.

Изследването **не** включва преглед на нормативните документи, регламентиращи сигурността на комуникационни и информационни системи за обработка на класифицирана информация по смисъла на раздел V, глава шеста от Закона за защита на класифицираната информация, както и нормативните документи, регламентиращи управлението и контрола на мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция „Национална сигурност“, Държавна агенция „Разузнаване“, Държавна агенция „Технически операции" и Националната служба за охрана, несвързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи.

В основата на това изследване е анализът на основните документи, изграждащи системата от норми за поведение при дейности за постигане на кибер сигурност. **Този анализ се извършва по няколко основни показателя**:

- действащи норми и норми в процес на приемане от компетентните органи;
- натрупана до момента практика;
- ресурсно осигуряване на дейностите.

В **обхвата** на прегледа са включени:

- **Националната стратегия за киберсигурност „*Киберустойчива България 2020*”**, приета от Министерски съвет на Република България на 13 юли 2016 г.;

- Актуализирана стратегия за национална сигурност на Република България, приета с Решение на Народното събрание от 14 март 2018 г.;
- Закон за управление и функциониране на системата за защита на националната сигурност, в сила от 01.11.2015 г.;
- Правилник за дейността, структурата и организацията на Държавна агенция "*Електронно управление*", приет с постановление № 274 от 28 октомври 2016 г.;
- **Закон за киберсигурност**, приет от Народното събрание на 31 октомври 2018 г.

Влияние върху формирането на политиката за кибер сигурност имат и приложими стандарти[2] и директиви. По отношение на кибер сигурността приложим е стандартът БДС EN ISO/IEC 27001:2017 „*Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията*" и Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза.

Терминология. Обхват на понятието *кибер сигурност*

В изследването на различните документи, формиращи рамката на държавната политика в областта на кибер сигурността, са използвани определенията, дадени в тях за основните термини и понятия.

Националната стратегия за кибер сигурност „Киберустойчива България 2020" от 2016 г.[3] е първият документ, изразяващ колективния ангажимент и отговорност на всички заинтересовани страни, и волята на ръководството на Република България да осигури модерна рамка и стабилна среда за развитие на националната система за кибер сигурност и постигане на отворено, безопасно и сигурно кибер пространство.

Стратегията определя модела и механизмите за координация на стратегическо, политическо, оперативно и техническо ниво, както и принципите за създаване на ефективна платформа за споделяне на информация и колективен отговор на заплахи за кибер сигурността. Набелязани са цели и мерки в девет основни направления, както и широко прилагане на различни форми на публично-частни партньорства.

---

2 „Технически стандарт" е правило по смисъла на чл. 2, параграф 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно Европейска стандартизация.

3 Национална стратегия за кибер сигурност „Киберустойчива България 2020", приета от Министерски съвет на Република България на 13 юли 2016 г.

Националната стратегия за кибер сигурност очертава етапите на развитие за израстване от базова информационна сигурност и кибер хигиена до зряло информационно общество, способно да устои на кибер и хибридни заплахи във всички сфери, постигано чрез провеждане на единна национална политика за кибер сигурност, в съответствие със стратегиите и политиките на Европейския съюз и НАТО. Стратегията набелязва цели и мерки за развитие в ***девет ключови области:***

1) Установяване и развитие на националната система за кибер сигурност и устойчивост.
2) Мрежова и информационна сигурност – фундамент на кибер устойчивостта.
3) Защита и устойчивост на дигитално зависимите критични инфраструктури.
4) Подобряване на взаимодействието и споделянето на информация между държава, бизнес и академичен сектор.
5) Развитие и подобряване на регулаторната рамка.
6) Засилване на противодействието на кибер престъпността.
7) Кибер отбрана и защита на националната сигурност.
8) Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността.
9) Международно взаимодействие – кибер дипломация и оперативно взаимодействие.

Стратегията предвижда изпълнението на целите и набелязаните мерки да бъдат развити в План с пътна карта съобразно набелязаните фази за развитие. За първи път тя предлага систематизирани определения за основните термини и понятия в областта на кибер сигурността. В същото време за някои от използваните термини са предложени повече от едно определение. На първо място това са определения на ***двете основни понятия*** в областта на кибер сигурността – *кибер пространство* и *кибер сигурност*.

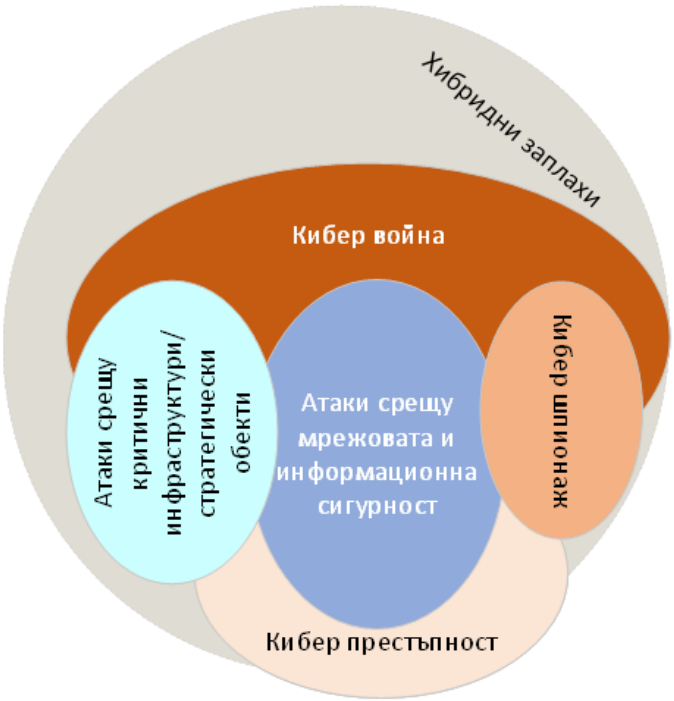
Дефинирани са критичните инфраструктури, представляващи особено важна част от националната икономика и общество и основна среда на дейностите по кибер сигурност.

Предложени са определения и на основните нежелани дейности/събития в кибер пространството, като: *кибер престъпление*, *кибер престъпност*, *кибер атака*, *кибер инцидент*, *кибер война*, както и *хибридна заплаха* и *хибриден модел на водене на война*.[4]

[4] Определенията на тези и други ключови термини са дадени в Приложение 1 и Приложение 2 към настоящия доклад.

Определени са също субектите и дейностите за противодействие на нежелани събития и гарантиране на нормално протичане на процесите в кибер пространството: *Computer Emergency Response Team (CERT)* и *кибер отбрана*.

Посочени са и определения на термини с общо приложение в областта на сигурността, като е посочено тяхното съдържание в контекста на Стратегията за кибер сигурност: *устойчивост, уязвимост, заплаха* и *риск.*



Фигура 2. Основни области на приложение на концепцията за кибер сигурност

Със *Закона за киберсигурност, приет на 31.10.2018 г.*[5] в българското законодателство се въвеждат изискванията на Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза.

До неговото приемане нямаше основен закон, който да урежда обществените отношения в областта на кибер сигурността. Материята беше

[5] Закон за киберсигурност, приет на 31 октомври 2018 г., Държавен вестник, бр. 94, 13.11.2018 г.

частично определена в други нормативни актове, като: Закона за електронното управление, Закона за управление и функциониране на системата за защита на националната сигурност, Закона за Държавна агенция „Национална сигурност“, Закона за министерството на вътрешните работи, Правилника за дейността, структурата и организацията на Държавна агенция „Електронно управление“, Наредбата за общите изисквания за мрежова и информационна сигурност и др.

Законът за киберсигурност урежда **основни въпроси** в областта на кибер сигурността, като:

- създаването на нови национални компетентни органи в областта – Национално единно звено за контакт, Националния координатор по киберсигурност, секторни Екипи за реакция при инциденти в киберсигурността (ЕРИКС), а създаването на Национален ЕРИКС се възлага на председателя на Държавна агенция „Електронно управление“;
- регламентира се управлението и организацията на националната система за киберсигурност;
- институционалната рамка в областта на кибер сигурността, превенцията и противодействието на кибер атаките;
- статута и функционирането на операторите на съществени услуги (ОСУ);
- статута и функционирането на доставчиците на цифрови услуги (ДЦУ).

Съществен принос на закона са легитимните определения на *двете основни понятия* в областта – *киберпространство и киберсигурност*.[6] В параграф 3 от Допълнителните разпоредби на закона се предлага систематизирано съдържанието на основните термини по смисъла на закона в областта на обществените отношения, които той регулира.

Предложените в закона правни дефиниции на основни дейности и понятия в кибер пространството обхващат един доста по-широк кръг от термини, като: „Онлайн място за търговия“, „Онлайн търсачка“, „Система за имена на домейни (Domain Name System – DNS)“, „Регистър на имена на домейни от първо ниво“, „Цифрова услуга“, „Цифрова инфраструктура“, „Компютърна услуга ‘в облак’“, „Съществени услуги“, „Технически стандарт“, „Спецификация“, „Точка за обмен в интернет“ и „Мрежа и информационна система“.

Специално внимание в *Закона за киберсигурност* е отделено на основните нежелани дейности/събития в кибер пространството и особено на *кибер инцидентите,* които са определени като *нежелани събития или*

6 Пълните определения са дадени в Приложение 2.

поредица от нежелани или неочаквани събития, свързани с кибер сигурността и са градирани по степента на негативно въздействие, което биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност, както в публичния сектор, така и върху бизнеса и предоставянето на услуги на гражданите. По този признак са дефинирани кибер инцидент със *среден*, *висок* или *значителен приоритет*, а като събития с най-високо ниво на вредни последици са отделени *мащабен кибер инцидент* и *инцидент със „значително увреждащо въздействие“.*[7] (Класификацията на инцидентите в кибер пространството се определя в зависимост от типа на атаката, по методика на Агенцията на Европейския съюз за мрежова и информационна сигурност, ENISA).[8]

Определени са също субектите и дейностите за противодействие на нежелани събития и гарантиране на нормално протичане на процесите в кибер пространството и са посочени органите, на които са възложени (или на които предстои да бъдат възложени) със закон или друг нормативен акт от съответния ред, отговорности за предоставяне на цифрови услуги и за осъществяване на дейности по гарантиране на сигурността в кибер пространството.

Съгласно приетия през 2015 г. *Закон за управление и функциониране на системата за защита на националната сигурност*, кибер сигурността е ключов елемент от националната сигурност на държавата – кибер пространството е специфична „виртуална“ територия без физически граници, в която също трябва да бъдат „гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите“.[9]

Стратегии, доктрини, процедури

Съгласно *Националната стратегия за киберсигурност „Киберустойчива България 2020”,* основната нормативна база за изграждане и функциониране на националната система за кибер сигурност е Законът за управление и функциониране на системата за защита на националната сигурност (ЗУФСЗНС, в сила от 01.11.2015 г.), както и международните ангажименти на Република България, поети с влезли в сила международни договори, по които Република България е страна в ЕС,

7 Пълните определения са дадени в Приложение 2.

8 Закон за киберсигурност, приет на 31 октомври 2018 г.

9 Закон за управление и функциониране на системата за защита на националната сигурност (в сила от 01.11.2015 г.)

НАТО, ООН и др. Определени аспекти са регламентирани и в други нормативни актове, (действащи към този момент) – Закон за електронните съобщения, Закон за електронното управление, Закон за Държавна агенция „Национална сигурност“, Закон за защита на класифицираната информация и наредбите към него, Закон за електронния документ и електронния подпис, и др.[10]

В *Закона за киберсигурност*, приет на 31 октомври 2018 г., е предвиден отделен раздел „Стратегии“. Там са посочени обхватът на *Националната стратегия за киберсигурност* и този на *Националната стратегия за мрежова и информационна сигурност* като стратегически рамки на държавната политика в съответните им предметни области.[11]

Предотвратяване и готовност за реагиране при заплахи за кибер сигурността

Със *Закона за киберсигурност* в ДАНС се създава Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху мрежовата и информационната сигурност на стратегическите обекти и дейности, от значение за националната сигурност и класифицираните мрежи, на който се възлага да поддържа готовност за координирана съвместна реакция в рамките на националната координационно-организационна мрежа за кибер сигурност при инциденти в мрежовата и информационната сигурност на стратегическите обекти, които са от значение за националната сигурност.[12]

Съгласно *Правилника за дейността, структурата и организацията на Държавна агенция „Електронно управление“,* развитието и изпълнението на функции на Национален център за действие при инциденти по отношение на информационната сигурност е възложено на Дирекция „Мрежова и информационна сигурност“. Дирекцията подпомага председателя на агенцията при провеждане на държавната политика в областта на мрежовата и информационната сигурност, като осъществява координация при изпълнението на политиките за мрежова и информационна сигурност, свързани с функционирането на електронното управление; изпълнява предвидените в Националната стратегия за киберсигурност функции относно координационно-информационната мрежа за кибер сигурност; анализира, координира и управлява инциденти,

10 Национална стратегия за киберсигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г.

11 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 7.

12 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 13.

уязвимости и данни, събрани при анализ на инциденти, свързани с кибер атаки.[13]

Реагиране на кибер атаки

Съгласно *Националната стратегия за киберсигурност „Киберустойчива България 2020”*, основната нормативна база за изграждане и функциониране на националната система за кибер сигурност е Законът за управление и функциониране на системата за защита на националната сигурност (ЗУФСЗНС, в сила от 01.11.2015 г.), както и международните ангажименти на Република България, поети с влезли в сила международни договори, по които Република България е страна в ЕС, НАТО, ООН и др. Определени аспекти са регламентирани и в други нормативни актове – Закон за електронните съобщения, Закон за електронното управление, Закон за Държавна агенция „Национална сигурност“, Закон за защита на класифицираната информация и наредбите към него, Закон за електронния документ и електронния подпис, и др.[14]

В *Закона за киберсигурност*, реагирането на кибер атаки е разпределено на няколко нива. Той предвижда в Държавна агенция „Национална сигурност” да се създаде Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху мрежовата и информационната сигурност на стратегическите обекти и дейности от значение за националната сигурност и класифицираните мрежи, на който се възлага да изпълнява както реактивни, така и проактивни дейности.[15]

В *Правилника за дейността, структурата и организацията на Държавна агенция „Електронно управление“* изпълнението на функции по анализ, координиране и управление на инциденти, уязвимости и данни, събрани при анализ на инциденти, свързани с кибер атаки, е възложено на Националния център за действие при инциденти по отношение на информационната сигурност, ситуиран в Дирекция „Мрежова и информационна сигурност“ и др.[16]

---

13 Правилник за дейността, структурата и организацията на Държавна агенция "Електронно управление", приет с постановление № 274 от 28 октомври 2016 г., чл. 21, ал. 2.

14 Национална стратегия за кибер сигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г.

15 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 13.

16 Правилник за дейността, структурата и организацията на Държавна агенция "Електронно управление", приет с постановление № 274 от 28 октомври 2016 г., чл. 21.

Организация на кибер сигурността

Функции и отговорности

Съгласно *Националната стратегия за киберсигурност „Киберустойчива България 2020”*, функциите и отговорностите по организацията на киберсигурността са разпределени между следните органи на държавна власт:

Народното събрание на Република България осигурява приемането на нормативните актове, свързани с кибер сигурността и осъществява парламентарен контрол за нейното състояние като част от контрола за управлението и функциониране на системата за защита на националната сигурност.

Президентът, в качеството му на Върховен главнокомандващ на въоръжените сили на Република България, получава цялостна информация за състоянието и развитието на националната система за кибер сигурност и устойчивост, а при въвеждане на „извънредно положение“, „военно положение“ или „положение на война“ ръководи дейностите по осигуряване на кибер устойчивост на държавното и военното управление.

Правителството на Република България определя политиката по кибер сигурност и развитието на кибер устойчивост, която се реализира от различни държавни институции, изпълняващи отделни функции в тази област. *Министерският съвет* осигурява политическата база за развитие, приема и периодично актуализира Националната стратегия за киберсигурност. За реализацията на утвърдената Стратегия МС приема план за изпълнение и следи за реализиране на приоритетите и целите и осигуряване на необходимите ресурси за изпълнение на заложените дейности.

Съветът по сигурността към Министерския съвет на Република България осъществява функции по развитие на способностите на системата за защита на националната сигурност за противодействие на заплахите, управление при кризи, осигуряването и защитата на информационната сигурност от посегателства. Съветът по сигурността при МС формулира позицията на Република България пред международни институции и организации по въпросите на кибер сигурността и решенията за управлението и функциониране на системата за защита на националната сигурност.[17]

[17] Национална стратегия за киберсигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г.

Със *Закона за киберсигурност* се поставят основите на структура от органи, на които се възлага изпълнението на дейностите по организацията, управлението и контрола на кибер сигурността, в т.ч. всички дейности и проекти по кибер отбрана и по противодействие на кибер престъпност, като са определени националните и специализираните компетентни органи в областта на кибер сигурността, както и техните правомощия и функции.[18]

Управлението и организацията на системата за кибер сигурност се осъществява от Министерския съвет, който създава и администрира Съвет по киберсигурност и приема с решение Национална стратегия за кибер сигурност и Национална стратегия за мрежова и информационна сигурност.[19]

В отделни текстове на закона са дефинирани функциите и отговорностите на основните субекти за осъществяване на дейности по гарантиране на сигурността в кибер пространството:

- Председателят на Държавна агенция „Електронно управление“ провежда държавната политика в областта на мрежовата и информационната сигурност, разработва и предлага проект на Национална стратегия за мрежова и информационна сигурност за утвърждаване от Министерския съвет.[20]
- Министърът на отбраната провежда държавната политика за защита и активно противодействие на кибер атаки и хибридни въздействия върху системите за управление на страната и въоръжените сили във военно положение, извънредно положение или положение на война (кибер отбрана); организира координацията и взаимодействието във връзка с изпълнението на поети ангажименти за колективна отбрана на споделеното кибер пространство с Организацията на Северноатлантическия договор (НАТО) и Европейския съюз (ЕС).[21]
- Началникът на отбраната организира поддържането на способности за кибер отбрана за защита на системите за управление на отбраната и въоръжените сили и възлага интегрирането на задачите по кибер отбрана като елемент от стратегическото планиране в плановете за изграждане на отбранителни способности и в плановете за операции на въоръжените сили.[22]

18 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 1.

19 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 5.

20 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 9.

21 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 10.

22 Пак там.

❖ Министърът на вътрешните работи провежда държавната политика в областта на противодействието на кибер престъпността.[23]

❖ Държавна агенция „Национална сигурност“ извършва дейности и осъществява контрол на информационната защита на стратегическите обекти и дейности от значение за националната сигурност. В ДАНС се създава Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху мрежовата и информационната сигурност на стратегическите обекти и дейности, от значение за националната сигурност и класифицираните мрежи, на който е възложено изпълнението както на реактивни, така и на проактивни дейности.[24]

В *Закона за киберсигурност* са разписани също функциите и отговорностите на националните компетентни органи по мрежова и информационна сигурност, които се създават с решение на Министерския съвет към административните органи в секторите, където такива не са създадени със специален закон:

❖ **Съвет по киберсигурност** е нещатен постоянен консултативен орган към Министерския съвет, който предлага на Министерския съвет Национална стратегия за киберсигурност и пътната карта за нейното изпълнение, а също така и за тяхната периодична актуализация;

❖ **Национален координатор по кибер сигурност**, който изпълнява функциите на секретар на Съвета по кибер сигурност и ръководи разработването и актуализирането на Националната стратегия за киберсигурност, плана за нейното реализиране; организира тяхното прилагане и осъществява мониторинг по отношение на тяхното изпълнение.

Ресурсно осигуряване

В съответствие с препоръките за прилагане на Стратегията за киберсигурност на ЕС и на директивата на Европейския парламент относно повишаване на сигурността на мрежите и информационните системи, и за осигуряване на високо общо ниво на МИС във всички сегменти на кибер пространството, *Националната стратегия за киберсигурност „Киберустойчива България 2020”* предвижда да бъдат предприети систематични мерки за *„Осигуряване на капацитет, техническа и организационна помощ за постигането на минималните изисквания за МИС от страна на Правителствения CERT и осигуряване на постоянна поддръжка (24/7), извършване на съответни периодични одити, както и*

[23] Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 11.

[24] Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 12.

периодичен контрол на състоянието от страна на специализираните звена за национална сигурност (ДАНС)“.[25]

Съгласно Закона за киберсигурност, „Националните компетентни органи трябва да разполагат с достатъчно технически, финансови и човешки ресурси, за да се гарантира, че са в състояние да изпълняват ефективно и ефикасно възложените им задачи в съответствие с този закон.“[26] Законът предвижда осъществяването на дейностите по него да бъдат в рамките на бюджетите за съответната календарна година на засегнатите държавни институции. Приета е хипотезата, че законът няма да доведе до необходимост от допълнителни финансови и други средства за прилагането на новата уредба.

Очаква се създаването на нов орган – Съвет по киберсигурност – като нещатен консултативен орган към Министерския съвет и определянето от министър-председателя на Национален координатор по киберсигурност да не доведе до допълнителни разходи, а функциите на Съвета по киберсигурност да не се дублират с функциите на вече съществуващи съвети или органи.

Предвижда се финансирането на административните структури, отговорни по законопроекта – Национални компетентни органи по сигурност на мрежите и информационните системи, които ще бъдат определени от Министерския съвет сред съществуващите администрации, Националното единно звено за контакт, създадените към определените Национални компетентни органи секторни Екипи за реакция при инциденти в компютърната сигурност, както и Национален екип за реакция при инциденти в компютърната сигурност към председателя на Държавна агенция "Електронно управление", да се осъществи за сметка и в рамките на утвърдените разходни тавани на съответните разпоредители с бюджет съгласно РМС № 654 от 30 октомври 2017 г. за одобряване на Актуализираната средносрочна бюджетна прогноза за периода 2018 – 2020 г.

Взаимодействие и координация

Голямото значение на въпросите по взаимодействието и координацията между публичните организации при осъществяване на дейности по поддържане на готовност, реагиране на инциденти и изграждане на способности е намерило отражение в съществения

[25] Национална стратегия за киберсигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г., Раздел „*Мерки за постигане на високо общо ниво на мрежова и информационна сигурност*“.

[26] Закон за киберсигурност, приет на 31 октомври 2018 г.

внимание, което е отделено на тези въпроси в разглежданите нормативни документи. И Стратегията и Закона за киберсигурност предвиждат създаването на национален кибер ситуационен център, който да координира оперативните дейности по поддържане на „национална кибер картина“, реагирането на кибер атаки и т.н., както и на механизъм, чрез който да се съгласуват дейности по развитие на способностите за киберсигурност.

Научно и технологично осигуряване на системата за кибер сигурност

Научни изследвания

В България няма обособена научно-изследователска организация, фокусирана върху проблемите на кибер сигурността. Съответни научни изследвания се извършват от институти на Българска академия на науките (основно в Института по математика и информатика /ИМИ/, Института по информационни и комуникационни технологии /ИИКТ/ и Националната лабораторията по компютърна вирусология /НЛКВ/), Института по отбрана към Министерството на отбраната, висши училища и в частност тези с традиционно силни факултети и департаменти по информатика, информационни технологии и компютърни мрежи, и някои специализирани звена, като Лабораторията по киберсигурност към София Тех Парк.

Изследователски проекти

Отделни изследвания се извършват на проектна основа и в зависимост от приоритетите и тематиката на финансиращата организация. В някои от тях успяват да се включат и български фирми.

В Таблица 1 са дадени международни изследователски проекти с българско участие от последните 10 години.

Проблемите на кибер сигурността нямат обособено място в програмите за създаване на центрове за върхови постижения и центрове за компетентност. Не са предвидени изследвания и разработване на съответни технологии в одобрените проекти.[27]

[27] Вж. http://sf.mon.bg/?go=news&p=detail&newsId=531.

Таблица 1 Идентифицирани изследователски проекти

Проект	Механизъм за финансиране	Продължителност	Участници от България
ECHO – European network of Cybersecurity centres and competence Hub for innovation and Operations, H2020 ICT 830943	H2020-SU-ICT-2018 – Establishing and operating a pilot for a Cybersecurity Competence Network	2019-2023	Институт по отбрана, ИИКТ, Европейски софтуерен институт – център Източна Европа, Телелинк
FORTIKA - Cyber Security Accelerator for trusted SMEs IT Ecosystems	H2020-EU.3.7.4. - Improve cyber security	2017-2020	Мотивиан ЕООД Немечек ЕООД
Courage – Cybercrime and cyberterrorism European Research Agenda	FP7-SECURITY	2014-2016	Международна академия за обучение по киберразследвания
SPEAR – Secure and Private Smart Grid	H2020-EU.3.7.4. - Improve cyber security	2018-2021	ТУ-София МВЕЦ Ленища ООД
ACDC – Advanced Cyber Defence Centre	CIP	2013-2015	Български пощи ЕАД
YAKSHA – Cybersecurity Awareness and Knowledge Systemic High-level Application	H2020-EU.2.1.1. - Industrial Leadership – ICT	2018-2020	Мотивиан ЕООД
FORWARD – Managing Emerging Threats in ICT Infrastructures	FP7-ICT	2008-2010	ИПОИ (сега ИИКТ)
VisiOn – Visual Privacy Management in User Centric Open Environments	H2020-EU.3.7. – Secure societies	2015-2017	Военномедицинска академия
TETRAMAX – Technology Transfer via Multinational Application Experiments	H2020-EU.2.1.1. - Industrial Leadership – ICT	2017-2021	АМГ Технолоджи ООД
SysSec – A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World	FP7-ICT	2010-2014	ИИКТ

Кибер сигурността като изследователски и практически проблем присъства по-ясно в националната научна програма „*Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността*“ с общ бюджет за периода 2018-2020 г. 3 450 000 лв. Макар и с широк спектър от цели и дейности, програмата предвижда изследвания по проблеми на информационната сигурност, в това число „сигурността на информационно-изчислителните ресурси и данни“, „сигурност на електронната инфраструктура за отворена наука“, използване на „големи данни“ за предпазване от кибер атаки и създаване на изследователски център за мониторинг и разработка на превантивни политики за информационна сигурност и реакция при инциденти. Към момента не е ясно в каква степен проблемите на кибер сигурността ще намерят място сред финансираните по програмата проекти.

Изследователски полигони (tesbeds)

Лаборатория по киберсигурност, София Тех Парк [28]

В Лабораторията по киберсигурност, която се изгражда от 2016 г. в Лабораторния комплекс на София Тех Парк, се разработват тестови и симулационни полигони, свързани с изследвания на уязвимости на системи за управление и индустриални системи в публичния и частния сектор, включително системи ICS/SCADA, многослойни атаки (комуникационно, мрежово, системно, приложно и човешко ниво), слабости в устойчивостта на организации със сложни системи (Systems-of-Systems), изучаване и симулиране на атаки към слабости в IoT, PLC и други индустриални и домашни „умни“ системи. Разработен е специализиран учебен полигон за курсове и обучения свързани с технологии за дизайн и разработване на софтуерни системи – secure coding / security by design, прилагани в различни платформи – Linux, PHP, Java Script, C, C++, мобилни платформи. Симулационните установки се използват и за организиране на състезания CTF (Capture-the-Flag) и червен-син екип (симулиране на атаки и защита), както и за практически упражнения на курсове в областта киберсигурност и устойчивост от факултетите по математика и информатика на Софийски университет, Нов Български Университет, Пловдивски университет и други.

Лабораторията за киберсигурност в София Тех Парк се изгражда със съдействието на „Европейски софтуерен институт – център Източна Европа“ (http://esicenter.bg/) и Cyber Resilience Lab (https://cyreslab.org/) към него, в партньорство с Института по софтуерно инженерство и централния CERT на университета Карнеги Мелън (САЩ). Тестовите и симулационни установки се използват за над 10 професионални курса в областта на кибер

[28] Вж. http://sofiatech.bg/en/about/tin/laboratory-complex/cybersecurity/.

сигурността, както и за лицензирани обучения по модела CERT-RMM (Resilience Management Model) от CERT на Software Engineering Institute, университета Карнеги Мелън, САЩ (https://www.sei.cmu.edu/about/divisions/cert/).

Институт по отбрана

Институтът по отбрана към Министерството на отбраната разполага с компютърна лаборатория за тестване, експериментиране и обучение на базата на технологиите за виртуализация. Лабораторията е изградена и функционира с цел подкрепа на всички изследователски и експериментални дейности в областта на кибер сигурността, включително сътрудничеството в областта на научните изследвания, разработването, тестването и сертифицирането на отбранителните продукти в рамките на НАТО, ЕС, както и на двустранна основа с партньори и в национален контекст. Лабораторията е с капацитет от 896 GB RAM, 168 ядра и 54 TB дисково пространство.

Сертификация за кибер сигурност на продукти и услуги

В национална нормативна уредба е развит въпроса за сигурността на автоматизираните информационни системи (АИС) или мрежи по отношение на класифицираната информация и включваща в условията за сигурност компютърната, комуникационната, криптографската, физическата и персоналната сигурност, сигурността на самата информация на всякакъв електронен носител, както и защитата от паразитни електромагнитни излъчвания.[29]

Не е известно обаче да са въведени единни изисквания и процедури за проверка на вграждани продукти, елементи, системен софтуер и приложения от гледна точка на кибер сигурността, които потенциално биха могли да допринесат за уязвимост на изградените информационни системи и мрежи.[30]

Хората в кибер сигурността

Хората, със своите знания, умения и контакти, са основен капитал за всяка една организация. За да се гарантира високо равнище на кибер

[29] Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, приета с ПМС № 99 от 10.05.2003 г., обн. ДВ. бр.46 от 20 Май 2003 г., изм. ДВ. бр.44 от 9 Май 2008 г.

[30] Вж. например Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg Businessweek*, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

сигурност е необходимо да има ясно разбиране за необходимите компетенции и ефективни начини за придобиването им.

Към настоящия момент няма изградена цялостна система за определяне на необходими компетенции със съответните образователни и квалификационни изисквания, съответни акредитирани програми, лицензирани центрове за обучение и механизми за сертификация. В известна степен тази сериозна слабост на системата за кибер сигурност в администрацията се компенсира с инициативата на голям брой висши училища, изследователски звена и бизнес организации, но това не е решение на проблема.

Образование за кибер сигурност

Към момента, в Република България **не** съществуват единни образователни изисквания по кибер сигурност. Основната част от висшето образование за придобиване на образователно-квалификационна степен „Бакалавър“ или „Професионален бакалавър“, свързано с проблематиката на кибер сигурността, се осъществява в професионалните направления „Математика“, „Информатика и компютърни науки“, „Комуникационна и компютърна техника“. В два идентифицирани случая (вж. по-долу), висши училища обучават по специалност „кибер сигурност“ на ниво бакалавър.

През последните години се наблюдава бум на магистърските програми по кибер сигурност. Някои от тях са по изброените професионални направление, докато други, в зависимост от получената акредитация, осъществяват обучение в професионални направления „Икономика“ (с фокус върху мениджмънт на кибер сигурността), „Национална сигурност“ и „Военно дело“.

Информацията в този раздел е от официални сайтове на висши училища и университети, обучаващи студенти по специалност „Кибер сигурност“ или аналогична.

Бакалавърски програми

Висше училище по телекомуникации и пощи

Специалност „Киберсигурност на високите технологии“

Професионално направление 5.3. „Комуникационна и компютърна техника”

Образователно-квалификационна степен „Професионален бакалавър“

Програмата съчетава изучаването на комуникационни мрежи и технологии и правните и етични въпроси в областта на компютърната сигурност.

Университет по библиотекознание и информационни технологии

Бакалавърска програма „Информационна сигурност“, факултет „Информационни науки“

„Изучават се фундаментални и специализирани дисциплини като линейна алгебра и аналитична геометрия, математически анализ, системен анализ, информационен мениджмънт, основи на компютърните системи, теоретични основи на информатиката, програмиране, информационни системи, компютърни мрежи и комуникации, методологични основи на информационната сигурност, криптография и криптология, защита на информацията в компютрите и мрежите, информационна сигурност в Интернет, защита на класифицирана информация, защита на интелектуалната собственост, нормативно-правни основи на информационната сигурност, риск мениджмънт, бизнес психология.“[31]

Магистърски програми

Нов Български Университет

Магистърска програма „Киберсигурност“[32] в професионално направление „Национална сигурност“

Изучават се основи на сигурността, сигурност на автоматизираните информационни системи, криптографска защита на приложенията в компютърните мрежи, сигурност и защита на информацията в компютърни системи, програмиране на специализирани системи.

Варненски свободен университет „Черноризец Храбър“

Магистърска програма „Киберсигурност“[33] в професионално направление „Информатика и компютърни науки“

Програмата е създадена с цел да подготви професионалисти в областта на информационната сигурност, управлението на сигурността, престъпленията в киберпространството и тестването на защитите.

31 Вж. https://www.unibit.bg/learning-activity/bachelor/bachelor-specialties#IS.

32 Вж. https://ecatalog.nbu.bg/.

33 Вж. http://ksp.vfu.bg/magistar/specialnosti/78.

Висше военноморско училище „Н.Й. Вапцаров“

Магистърска програма „Киберсигурност“[34] в професионално направление „Информатика и компютърни науки“

Изучават се въпросите на противодействието на хакерски атаки, компрометиращи различни компютърни мрежи и системи.

Военна академия „Г.С. Раковски“

Магистърска програма „Киберсигурност“[35] в професионално направление „Национална сигурност“

Целта е придобиване на специализирани знания умения за решаване на проблеми на изследването, нововъведенията и приложението на комуникационните и информационните системи и технологии, развиване на способности и усъвършенстване на необходими навици и умения в отговор на повишените изисквания към кибер сигурността и адекватни реакции на заплахите в кибер пространството, включваща формулиране на заплахи, оценка на риска, определяне на средства за кибер защита и организация на мероприятията по защита на информацията и личните данни в КИС в единна система, работа с техника и технологии за предоставяне на услуги

Висше училище по застраховане и финанси

Магистърска програма „Киберсигурност и стратегически мениджмънт“ в Пловдив, Индийски институт по хардуерни технологии (http://iiht.bg/)[36] в професионална област „Икономика“

Целта е студентите да могат да направят критичен анализ на дадена ИТ инфраструктура, с цел откриване на слаби места, позволяващи злоумишлен достъп до тази структура.

Университет по библиотекознание и информационни технологии

Магистърска програма „Информационна сигурност“ в професионално направление „Информатика и компютърни науки“

Целта е да подготви „специалисти, които да анализират, диагностицират, оценяват и провеждат активни мероприятия или анализи за нарушения в кибер пространството, както и мерки за тяхното предотвратяване“.[37]

34 Вж. http://www.naval-acad.bg/education/msc/cybersecurity-msc.

35 Вж. http://rnda.armf.bg/.

36 Вж. https://financebg.com/

37 Вж. https://drive.google.com/file/d/0B-7I4wu_HMCHT0Y0ek9iNjlzck0/view

Бургаски свободен университет

Магистърска програма „Информационна сигурност“ в професионално направление „Информатика и компютърни науки“

Програмата „надгражда базовите знания на студентите в областта на приложния и системния софтуер, на системните и мрежовите технологии, както и проектирането и разработването на локални и разпределени системи, работещи в Интранет и Интернет среда.“[38]

Ресурсно осигуряване

Изследователският екип не разполага с информация каква част от обучението по кибер сигурност се финансира от държавата чрез т.н. „държавна поръчка“ и каква част е изцяло за сметка на студентите.

Междинни изводи: Към момента няма утвърдени единни (национални) образователни изисквания в областта на кибер сигурността. Университети и висши училища проявяват инициатива с желание да отговорят на нарастващите потребности, но в много случаи програми и специалности под едно и също заглавие се предлагат в рамките на съществено различаващи се научни и професионални области. Това налага изготвяне на национални изисквания за знанията и уменията в сферата на кибер сигурността за нуждите на администрацията, синхронизирани с развитието в НАТО и ЕС.

Квалификация за кибер сигурност

Към момента не съществуват изисквания за професионална квалификация по въпроси на кибер сигурността. В актуалния списък на професиите за професионално образование и обучение фигурират професионални направления „Компютърни науки“ (професии Програмист, Системен програмист и Приложен програмист), „Приложна информатика“, „Сигурност“ и „Военно дело и отбрана“.[39]

При търсене в базата данни от курсове, предлагани от лицензирани Центрове за професионално обучение, не се откриват курсове по кибер или информационна сигурност. От тук може да се направи извод, че за получаване на професионална квалификация в областта на кибер сигурността се разчита изцяло на висшите училища.

[38] Вж. https://www.bfu.bg/bg/magistarski-programi/tsentar-po-informatika-i-tehnicheski-nauki/informatsionna-sigurnost

[39] Вж. https://www.navet.government.bg/bg/aktualen-spisak-na-profesiite-za-poo/

Частично изключение правят курсове, изградени около продукти на определена фирма и сертифицирани от нея,[40] както и курсовете, провеждани в Лабораторията по киберсигурност към София Тех Парк.[41]

Учения за кибер сигурност

Съгласно *Закона за киберсигурност,* Националният координатор по киберсигурност следва да координира организираните от национални компетентни органи общи и частични учения в областта на кибер сигурността или учения от хибриден характер,[42] а функцията да координира, организира и провежда учения и тренировки в областта на мрежовата и информационната сигурност в международен и национален формат е възложена на *Председателя на Държавна агенция „Електронно управление“*.[43]

Съответно с *Правилника за дейността, структурата и организацията на Държавна агенция "Електронно управление*", на Дирекция „Мрежова и информационна сигурност“ в агенцията е възложено участието в процесите на планиране, подготовка и провеждане на международни и национални учения в областта на мрежовата и информационната сигурност. [44]

Настоящият раздел на доклада ще представи възможния обхват на ученията в сферата на кибер сигурността и опита в Република България до момента.

Регулярното провеждане на учения, посветени на кибер сигурността или с хибридни сценарии, отчитащи въздействието на кибер атаки, е незаменим инструмент за развитие и валидиране на индивидуални и групови умения, както и за проверка на процедури и технически възможности за междуведомствено и международно взаимодействие.

Все още няма общоприета класификация на ученията в областта на кибер сигурността. MITRE предлага класификация с три типа учения [45]:

- **“Table-top” (или „щабни“) учения**, целящи да се определи капацитета на персонала да отговори на инцидент или да взаимодейства, да се валидират процедури, да се наблюдава и

40 Вж. например https://cisco.uni-sofia.bg/bg/content/courses.

41 Вж. съответния раздел по-горе.

42 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 8.

43 Закон за киберсигурност, приет на 31 октомври 2018 г., чл. 9.

44 Правилник за дейността, структурата и организацията на Държавна агенция "Електронно управление", приет с постановление № 274 от 28 октомври 2016 г., чл. 21.

45 Jason Kick, *Cyber Exercise Playbook*, Report MP 140714 (Wiesbaden, Germany: MITRE Corporation, 2014).

опише процеса на откриване, отговор и възстановяване от симулирани събития;

- "**Full Live", или „живи" учения**, насочени към подготовка на организацията и професионалния състав чрез реални събития и сценарии;
- **„Хибридни" учения**, целящи да подготвят организацията, като валидират процедури и определят способността да се открие, реагира на симулирано събитие и възстанови работоспособността.

Испанският институт за изследвания по кибер сигурност INCIBE конкретизира и развива тази класификация в „Таксономия на кибер ученията",[46] като отличава:

- учения с цел **придобиване и поддържане на умения** (drills), групово сработване, разработване и тестване на нови политики и процедури;
- **функционални учения** за валидиране и оценяване на индивидуални умения и тестване на планове, политики, процедури и персонал на базата на комплексни и реални проблеми, изискващи бърз и ефективен отговор в стресова обстановка и при ограничено време;
- **пълномащабни учения**, с фокус върху прилагането и анализа на планове, политики, процедури и споразумения за сътрудничество.

Освен това, таксономията отличава ученията според броя на участващите държави, модалностите (аналогични на класификацията на MITRE), броя на засегнатите сектори и други параметри.

Според наличната информация, "Киберзима 2011″ (декември 2011 г.) се счита за първото учение по кибер сигурност в България.[47] Целта на учението е служители на Министерството на транспорта, информационните технологии и съобщенията (МТИТС) и изпълнителните агенции към него да се справят в реално време с хакерски атаки срещу сървърите и системите на ведомството. Тествани са конкретни мерки и процедури в случай на инцидент в областта на кибер сигурността.

През май 2014 г. Националната агенция за приходите провежда учение „Кибер НАП 2014" с цел да усъвършенства уменията на експерти от

[46] Elena García Díez, Daniel Fírvida Pereira, Marco A. Lozano Merino, Héctor R. Suárez, and Darío Beneitez Juan, Cyber Exercises Taxonomy (Spanish National Cybersecurity Institute, March 2015), https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/incibe_cyberexercises_taxonomy.pdf

[47] Irena Nikolova, "Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector," *Information & Security: An International Journal* 38 (2017): 79-92.

агенцията за защита на комуникационно-информационната инфраструктура от кибер атаки и реакция на пробиви в информационната инфраструктура.[48]

През октомври 2016 г. МТИТС провежда ново учение „на оперативно ниво“ с участници от министерството и подчинените му структури с основна цел проверка на стандартните оперативни процедури за реагиране при кибер инцидент в организацията и взаимодействието между отделни нейни структури.[49]

Ученията *Cyber Europe* представляват симулации на мащабни кибер инциденти, ескалиращи в кибер кризи на равнище ЕС. Ученията дават възможност за анализиране на високотехнологични кибер инциденти и за справяне със сложни ситуации, свързани с непрекъснатостта на дейността и управлението на кризи. ENISA вече организира четири общоевропейски кибер учения — през 2010 г., 2012 г., 2014 г. и 2016 г.

На 6 и 7 юни 2018 г. CERT България към Държавната агенция „Електронно управление“ взе участие в най-сложното досега международно учение по киберсигурност в ЕС, организирано от Агенцията на ЕС за мрежова и информационна сигурност ENISA – *„Cyber Europe 2018“*. Повече от 900 специалисти от държавите членки на ЕС работиха по повече от 23 000 симулирани инциденти в областта на кибер сигурността.

NATO Cyber Coalition Exercise

Ежегодно Институтът по отбрана „Проф. Цветан Лазаров“ е домакин на българският екип, участващ в учението на НАТО Cyber Coalition. В учението се тестват и обучават екипи за кибер сигурност от целия Алианс в способността им да защитават националните мрежите и мрежите на НАТО. Cyber Coalition включва около 700 участници от съюзниците, партньорите, индустрията и академичните среди. Целта на учението е да се подобри координацията и сътрудничеството между НАТО и съюзниците, да се укрепи способността за защита на кибер пространството на Алианса и да се водят военни операции в кибер пространството. Също така се тестват процедурите на НАТО и националните процедури за обмен на информация, ситуационна осведоменост в кибер пространството и вземане на решения.

„Кибер игри“

Ежегодно Институтът по отбрана съвместно с Лабораторията по киберсигурност към София Тех Парк провежда национално състезание по кибер сигурност „Кибер игрите“.[50] Целта на състезанието е да се стимулират

[48] Ibid.

[49] Ibid.

[50] За подробности вж. https://www.thecybergames.net/bg/za-kiber-igrite

и насърчат заниманията, свързани с кибер сигурността, и да се предостави възможност на любителите на предизвикателствата в тази област.

Разгледаните по-горе учения вече са проведени. Изследователският колектив разполага с информация, че през 2019 г. се предвижда България да участва в ежегодните учения по кибер сигурност на НАТО и на ЕС, както и че се планира провеждането поне на две национални учения, в които да се тестват капацитета за защита на критични инфраструктури и механизмите за публично-частно взаимодействие.

Междинни изводи: В страната има натрупан опит от участие в (и в по-малка степен – за организация на) учения по кибер сигурност, но все още обхвата на тези учения е твърде тесен. До момента на практика не се използват мулти-секторни сценарии, не се тества междуведомственото взаимодействие, а апробирането на механизми за международно взаимодействие е все още ограничено. Тази слабост частично се компенсира от участието в учения на НАТО и ЕС, но е наложително изработването на национална програма за кибер учения в администрацията на общинско, областно и национално ниво по сценарии, покриващи хоризонтално взаимодействие между институциите.

Демократичен контрол в сферата на кибер сигурността

Съгласно Закона за електронното управление (ЗЕУ),[51] чл. 60 (1) на председателя на Държавната агенция "Електронно управление" се възлага да упражнява контрол за спазване на изискванията за мрежова и информационна сигурност и оперативна съвместимост. В чл. 7в на Закона са определени съответни правомощия да *„издава методически указания и координира изпълнението на политиките за мрежова и информационна сигурност*“, *„подпомага разработването и утвърждава проектни предложения, координира и контролира изпълнението на проектите за електронно управление, информационни и комуникационни технологии в администрациите, финансирани със средства от държавния бюджет, от структурните и инвестиционните фондове на Европейския съюз и от други източници*“, *„както и удостоверява съответствието на информационните системи с изискванията за оперативна съвместимост, мрежова и информационна сигурност и осъществява контрол върху администрациите за спазване на тези изисквания,…*“.

[51] Закон за електронното управление, обн. ДВ, бр.46 от 12 юни 2007 г., в сила от 13.06.2008 г., изм. … изм. ДВ, бр. 88 от 23 октомври 2018 г.

Освен това, ЗЕУ предвижда контрол в рамките на бюджетния процес (чл. 7г), осъществяван от председателя на ДАЕУ, който съгласува предварително предложения от всички административни органи за „разходите в областта на електронното управление и за използваните от тях информационни и комуникационни технологии“. ЗЕУ въвежда и изисквания за прозрачност, напр. задължения на ДАЕУ за регулярно публикуване на обществена информация в машинно четим отворен формат (чл. 7п).

Ежегодно, председателят на ДАЕУ внася в Министерски съвет „отчет за състоянието и годишен план за развитието и обновяването на информационните ресурси в администрацията и информационните ресурси на Единната електронна съобщителна мрежа на държавната администрация и за нуждите на националната сигурност“, като и двата документа се публикуват на интернет страницата на агенцията.

Наредбата за общите изисквания за мрежова и информационна сигурност [52] (Загл. изм. – ДВ, бр. 5 от 2017 г., в сила от 1.03.2017 г.) доразвива механизмите за контрол от страна на председателя на ДАЕУ.

Новоприетият закон за кибер сигурност определя изискванията към доставчици на административни и обществени услуги, предоставяни по електронен път, като изключва комуникационните и информационните системи за обработка на класифицирана информация.

Законът създава Съвет по киберсигурността като консултативен и координиращ орган към Министерския съвет по въпросите на киберсигурността, със заместник министър-председател като председател на Съвета и осем министри, т.е. политически лица, сред членовете му.

От гледна точка на отчетността, Законът предвижда ежегодно предоставяне на информация от Съвета по киберсигурност на Съвета по сигурността към Министерския съвет относно състоянието на сигурността в кибер пространството, която се включва в проекта на годишен доклад за състоянието на националната сигурност. Този доклад се приема от Министерския съвет и се внася в Народното събрание, като по този начин се предвижда възможност за регулярен парламентарен контрол на състоянието на кибер сигурността.

Контрол на кибер сигурността от страна на Министерския съвет, чрез Съвета по сигурността, са предвидени и в Националната стратегия за киберсигурност.[53] Стратегията предвижда функции на Народното събрание, Президента и правителството на Република България. В частност, Народното събрание да осигурява приемането на нормативните актове,

[52] Наредба за общите изисквания за мрежова и информационна сигурност (Загл. изм. – ДВ, бр. 5 от 2017 г., в сила от 01.03.2017 г.)л

[53] Приета от Министерски съвет на Република България на 13 юли 2016 г.

свързани с кибер сигурността и да осъществява парламентарен контрол за нейното състояние в рамките на контрола за управлението и функциониране на системата за защита на националната сигурност.[54]

Предстои възможностите за парламентарен контрол да се използват пълноценно. До момента е известен един случай на отправено парламентарно питане от ноември 2015 г. (относно изготвянето на стратегия за киберсигурност), на което е предоставен писмен отговор.

ОБЗОР И АНАЛИЗ НА РЕГУЛАТОРНИТЕ ИНСТРУМЕНТИ, ПОЛИТИКИ И СТРАТЕГИИ НА НАТО И ЕС, КОИТО ВЛИЯЯТ НА КИБЕР СИГУРНОСТТА НА БЪЛГАРИЯ

Развитие на политиката за кибер отбрана в НАТО и влияние върху България

В този раздел са представени основните стъпки в еволюцията на политиката на НАТО в областта на кибер отбраната.

Преди повече от 10 години, през 2007 г. и съответно 2008 г. НАТО за първи път разработва и приема два документа в областта на кибер отбраната (NATO Cyber Defense Policy, 20 December 2007 и NATO Cyber Defense Concept, 13 March 2008).

Три години по-късно, на срещата на върха в Лисабон през 2010 г. е взето решение Северно Атлантическият съвет да разработи цялостна политика на НАТО в областта на кибер отбраната и да подготви План за действие за нейното прилагане. В изпълнение на взетото решение, през 2011 г. министрите на отбраната на НАТО одобряват Политика на НАТО за кибер отбрана, която определя визия и план за действие с цел гарантиране на координирани действия на Алианса в контекста на бързо развиващата се стратегическа среда за сигурност.[55]

Същността на политика на НАТО за кибер отбрана включва:

- интегриране на кибер защитата в процесите на планиране на Алианса, за да се изпълняват пълноценно основните задачи на НАТО за колективна отбрана и управление при кризи;

[54] Национална стратегия за киберсигурност „Кибер устойчива България 2020," т. 4.1.1.

[55] Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 Nov. 2010, Press Release (2010) 155, Issued on 20 Nov. 2010, p. 11.

- съсредоточаване върху превенцията, гарантиране на устойчивостта и защитата на критичните кибер инфраструктури на НАТО и на съюзниците;
- създаване и поддържане на стабилни способности за кибер отбрана и централизирана защитата на мрежите на НАТО;
- разработване на минимални изисквания за кибер защита на националните мрежи, които са от критично значение за изпълнението на основните задачи на НАТО;
- осигуряване на съдействие на съюзниците за постигане на минимално ниво на кибер защита и намаляване на уязвимостта на националните критични инфраструктури;
- ангажиране с партньори, международни организации, частния сектор и академичните среди[56].

На срещата на върха в Чикаго през май 2012 г. лидерите на страните-членки на Алианса отново потвърждават своя ангажимент за подобряване на кибер отбраната, като включват всички мрежи на НАТО под централизирана защита и осъществяват поредица от действия за развитие на способностите на НАТО в отговор на компютърни инциденти (NATO Computer Incident Response Capability - NCIRC)[57]. В изпълнение на приетите решения, през същата година кибер отбраната става неотменна част от процеса на отбранително планиране в НАТО.

През февруари 2014 г. министрите на отбраната на НАТО вземат решение да се разработи нова, подобрена политика в областта на кибер отбраната, която по-късно е одобрена на срещата на високо равнище в Уелс през 2014 г. Освен това по време на срещата на върха на НАТО в Уелс, съюзниците приемат, че международното право се прилага в кибер пространството и че въздействието на кибер атаките може да бъде толкова опасно за нашите общества, колкото една конвенционална атака. Поради тази причина те могат да предизвикат реакция съгласно чл. 5 от Северноатлантическия договор. В резултат на това, кибер отбраната е призната като част от основната задача на НАТО за колективна отбрана. Решение за задействане на чл. 5 ще се взема за всеки отделен случай от Северно Атлантическия Съвет. Основен акцент е поставен също на изграждането на капацитет и способности за кибер отбрана на страните-членки на Алианса, интегрирането на кибер отбраната в операциите на НАТО и в процеса на отбранително планиране, както и на необходимостта от повишаване на обмена на информация и постигане на подобрена

56 NATO (2011). Defending the Networks: The NATO Policy on Cyber Defence.

57 Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, 20 May. 2012, Press Release (2012) 062, Issued on 20 May 2012, pp. 12-13.

ситуационна осведоменост между съюзниците. Вземат се важни решения също и по отношение на засилване на партньорствата с Европейския съюз и отделни страни-партньори, както и с индустрията. Не на последно място е посочена потребността от подобряване на образованието и обучението в областта на кибер отбраната в Алианса.[58]

На срещата на върха в Варшава през 2016 г. се вземат важни решения, които по-нататък развиват и усъвършенстват политиката на НАТО в областта на кибер отбраната. На първо място държавните и правителствените ръководители потвърждават, че кибер отбраната е част от основната задача на НАТО за колективна отбрана и че съюзниците могат да разчитат на колективна отбрана в отговор на значителна кибер атака, еквивалентна на въоръжено нападение. Освен това киберпространството е дефинирано като домейн на бойното пространство, наред с въздуха, морето и сушата.[59]

В приета по време на срещата Cyber Defence Pledge се посочва, че съюзниците потвърждават поетите национални отговорности съгласно чл. 3 от Вашингтонския договор и в областта на кибер отбраната. Те заявяват готовност да работят за изпълнение на приетата по време на срещата на високо равнище в Уелс подобрена политика в областта на кибер отбраната. Наред с това се потвърждава ролята на сътрудничеството между НАТО и ЕС в гарантиране сигурността в кибер пространството. Изграждането и развитието на националните способности за кибер отбрана се определят като приоритет. Друг основен акцент в документа е подобряване на капацитета и осведомеността на всички заинтересовани страни, както и засилване на сътрудничеството и обмена на информация между тях. Не на последно място се отделя специално внимание на ролята на образователните институции в Алианса за подобряване на образованието и обучението в областта на кибер отбраната.[60]

На срещата на върха в Брюксел през 2018 г.[61] държавните и правителствени лидери на държавите в Алианса потвърждават, че НАТО ще продължи да се адаптира към развиващия се спектър от кибер заплахи, които се осъществяват от държавни и недържавни участници.

58 Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 Sep. 2014, Press Release (2014) 120, Issued on 05 Sep. 2014, pp. 15-16; NATO Policy on Cyber Defence, endorsed by Allied Defence Ministers in June 2014.

59 Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, 09 Jul. 2016, Press Release (2016) 100 Issued on 09 Jul. 2016, pp. 15-16.

60 Cyber Defence Pledge 08 Jul. 2016, Press Release (2016) 124 Issued on 08 Jul. 2016.

61 Brussels Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 11-12 July 2018, Press Release (2018)074, accessed on 2.11.2018.

Препотвърждава се разбирането, че кибер отбраната е част от основната задача на НАТО за колективна отбрана. Затова НАТО трябва да може да работи така ефективно в кибер пространството, както във въздуха, на сушата и в морето за укрепване цялостната възпираща и защитна сила на Алианса. Кибер пространството се разглежда като домейн на операциите. За първи път се посочва, че, за да изпълни отбранителната си задача НАТО, ще прилага и използва пълната гама от способности, включително в кибер пространството, за да възпира, защитава и противодейства на целия спектър от кибер заплахи, включително тези, провеждани като част от хибридна кампания.

Друг важен момент, който се посочва за първи път в подобен документ е, че за установяването и противодействието на злонамерени действия в кибер пространството ще се търси координиран отговор, за да се повиши себестойността на една кибер атака и така да се засили възпиращия потенциал на Алианса. На следващо място ръководителите на държавите и правителствата решават да се създаде нов Център за операции в кибер пространството (Cyber Operations Centre), като част от командната структура на НАТО. Центърът трябва да осигури ситуационна осведоменост и координация на операциите на НАТО в киберпространството. Съюзниците също така приемат, че НАТО може да използва националните способности на отделните държави-членки на Алианса в киберпространство за своите мисии и операции.

В следващите редове се представят и анализират основни компоненти на изграждането и развитието на способности на НАТО за кибер отбрана.

В Алианса се налага разбирането, че кибер отбраната е комплексен феномен и затова се полагат усилия по целия спектър от компонентите на способностите (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Interoperability (DOTMLPFI).

За да се подобри ситуационната осведоменост по отношение на кибер заплахите в Алианса, през 2015 г. е разработен актуализиран Меморандум за разбирателство относно кибер отбраната (Memorandum of Understanding on Cyber Defence)[62]. Този меморандум се сключва между НАТО и националните органи за кибер защита на всяка от държавите-членки на Алианса. В него се дефинират условията за обмен на информация между съюзниците и възможностите за оказване на помощ с цел подобряване на способностите за предотвратяване на кибер инциденти,

62 Signing of Memorandum of Understanding on Cyber Defence, available on: https://www.nato.int/cps/ie/natohq/photos_136551.htm, accessed on 15.10.2018.

както и способностите за реагиране и гарантиране на устойчивост на информационните мрежи.

Сред най-важните участници при създаване и укрепване на способностите на НАТО за кибер отбраната е Агенцията за комуникации и информация (NATO Communications and Information Agency – NCIA), създадена през 2012 г. като част от реформата на агенциите на Алианса. Нейното предназначение е да подкрепя операциите на НАТО, да свързва информационните и комуникационни системи на НАТО и да защитава мрежите на Алианса.[63]

На следващо място е важно да се посочи изграденият и действащ център на НАТО за реагиране при компютърни инциденти (NCIRC), който е част от NCIA и е базиран в Съюзното командване по операциите (SHAPE), гр. Монс. Той е предназначен да подкрепя процеса за ранно откриване, предотвратяване, реакция и възстановяване след инциденти, свързани с кибер отбраната в Алианса.[64] Освен техническия център, NCIRC има и информационно-координационен елемент в Международния секретариат (Emerging Security Challenges Division).

Не на последно място следва да се посочи създаденият Център за управление на сложни кризисни операции (CCOMC) в Съюзното командване по операциите, който има елементи за управление, свързани с кибер заплахи.

По отношение на компонента на способностите „доктрина“ в НАТО се работи по няколко направления. На първо място е по отношение на възприетото вече разбиране, че кибер пространството е домейн за провеждане на съвременни военни операции. Следователно действията в този домейн, също следва да бъдат обект на доктринално и нормативно преосмисляне. Военният комитет на НАТО вече е одобрил таксономия на операциите в кибер пространството. Работи се по създаване на съвместна съюзна публикация (Allied Joint Publication) 3.20, касаеща провеждането на операции в кибер пространството. Тя е в процес на съгласуване от страните-членки на Алианса. На второ място, употребата на сила в кибер пространството също следва да бъде регламентирана. Затова, по препоръка на Съюзното командване по операциите, Военният комитет преразглежда условията за употреба на сила (Rules of engagement), които ще отразяват и при действия в кибер пространството.

В структурно отношение, НАТО започна изграждането на органи за кибер отбрана. От лятото на 2018 г. в Съюзното командване по

63 https://www.ncia.nato.int/Pages/homepage.aspx, acessed on 15.10.2018.

64 https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx, accessed on 15.10.2018.

трансформацията действат командни структури по кибер отбрана. Начални способности е постигнал и Центърът за операции в кибер пространството.[65]

За гарантиране на кибер отбраната хората са също толкова важни, както и технологиите. Затова основен акцент е подобряване на състоянието на образованието, обучението и ученията.

В областта на образованието, изследванията, ученията и тренировките по кибер сигурност водеща роля играе Центърът на НАТО за върхови постижения и сътрудничество в кибер пространството (NATO Cooperative Cyber Defence Centre of Excellence – CCD CoE) в Талин, Естония. Той е мултидисциплинарен и многонационален център, акредитиран от Командването по трансформацията на НАТО за провеждане на научни изследвания, образование, обучение, консултации и извличане на поуки от практиката в областта на кибер отбраната.[66]

Друг важен център за подготовка на персонал от държавите-членки на Алианса и от държави партньори, свързана с експлоатацията и поддръжката на комуникационните и информационните системи на НАТО е Училището за комуникации и информационни системи (NCISS) на НАТО в Латина, Италия.[67] С решението за преместването му в Ореаш, край Лисабон (Португалия) в мандата на училището се включва кибер отбраната и то ще се преобразува в Академия за комуникация, информация и кибер отбрана (NCI Academy), също част от NCIA.

Обучението по кибер сигурност на тактическо и оперативно ниво се извършва от Училището на НАТО в Оберамергау (NSS), Германия. Обучението там е свързано с поддръжката на операциите на Алианса, развитието на стратегията, политиката, доктрината и процедурите.[68]

Обучението на стратегическо ниво, формирането на стратегическото мислене по политико-военните въпроси, включително в областта на кибер отбраната се осъществява от Колежа по отбраната на НАТО (NDC) в Рим, Италия.[69]

Накратко, заслужават специално внимание две инициативи по отношение на засилването на способностите на НАТО в областта на кибер отбраната, които ще бъдат реалност в съвсем близко бъдеще. На първо място това е създаването на Академията за комуникации и информация на НАТО в Португалия, която ще започне да функционира през 2019 г. и ще допринася за образованието и обучението на специалисти от НАТО и

65 Progress Report on NATO Cyber Defence, 2018.

66 https://ccdcoe.org/, accessed on 15.10.2018.

67 https://www.nciss.nato.int/, accessed on 15.10.2018.

68 http://www.natoschool.nato.int/, accessed on 15.10.2018.

69 http://www.ndc.nato.int/, accessed on 15.10.2018.

държавите партньори. На второ място е създаването на Център за операции в кибер пространството, съгласно решенията на срещата на върха в Брюксел от тази година.

Според някои високопоставени служители на НАТО, Алиансът трябва да постигне пълни оперативни способности в областта на кибер отбраната до 2023 г.[70]

Наред с посоченото до тук, е важно да се отбележат дейностите в областта на кибер отбраната в рамките на Организацията за наука и технологии на НАТО (NATO STO).[71] Централно място имат изследванията в рамките на различните изследователски групи и STO Tech watch cards, които покриват широк кръг от теми (Blockchain and Distributed Ledger Technologies, Cyber Resilience, Modelling and Simulation S&T: Critical enabler for Cyber Defence, Cyber Security Science and Engineering 2.0, Cyber monitoring and detection capability for military systems, Predictive Analysis of Adversarial Cyber Operations, Military Strategic Level Decision Making within a (future) framework of Cyber Resilience, Enabling Technical Considerations for a NATO-Common Space Domain Operating Picture, Cyber Effects in Campaign and Mission Simulations, Cyber Symbology, Human Systems Integration Approach to Cyber Security и др.).

Кибер отбраната е интегрирана в инициативата на НАТО за интелигентна отбрана. Проектите в кибер защита по тази линия досега включват Платформата за разпространение на информация за зловреден софтуер (MISP), Проектът за многонационално развитие на способностите за мобилна отбрана (MN CD2) и Проектът за многонационално образование и обучение в кибер отбраната (MN CDE& T).

Като **обобщение** може да се каже, че НАТО помага на съюзниците да засилят кибер отбраната си чрез:

- **дефиниране на кибер отбраната като част от основната задача на НАТО** – колективната отбраната, възможност за задействане на чл. 3 и чл. 5 от Вашингтонския договор при наличие на кибер заплаха и включване на кибер пространството като домейн на бойното пространство;
- **реализиране на политиката за пълно интегриране на кибер отбрана** с висока степен на приоритетност в процеса на отбранително планиране на НАТО;

70 Quatation of Antonio Missiroli, NATO assistant secretary general for emerging security challenges. “Nato’s full operational capability in terms of cyber security is expected by 2023,” in panel discussion on the future of NATO’s cyber policy at the 2018 European Cybersecurity Forum in Krakow, https://www.computerweekly.com/, accessed on 22.10.2018.

71 https://www.sto.nato.int/publications/Pages/default.aspx, accessed on 22.10.2018.

- **разработване на минимални изисквания** за тези национални информационни системи, които са от решаващо значение за осъществяването на основните задачи на НАТО;
- разработване на цели за съюзниците за изграждане на общ подход към техните способности за кибер отбрана;
- **споделяне на информация за заплахи в реално време** чрез специализирана платформа за обмен на информация за зловреден софтуер, както и добри практики в отговор на кибер заплахи;
- **поддържане на екипи за кибер защита**, които могат да бъдат изпратени, за да подпомогнат съюзниците при справянето с кибер предизвикателства;
- подобряване на възможностите за ранно предупреждение, ситуационна осведоменост и анализ;
- **предоставяне на възможност за повишаване на образованието и обучението** в учебни институции на Алианса, както и в многонационални учения. В това отношение NCIA е подготвила класификация на курсовете и квалификациите в областта на кибер отбраната. Този документ може да послужи като основа за взаимното признаване на квалификациите в областта на кибер отбраната, придобити в различни страни-членки на НАТО и различни институции;
- предоставяне на възможност за използване на експертизата и подкрепата на NATO Cooperative Cyber Defence Centre of Excellence;
- предоставяне на възможност за включване в многонационални изследователски групи в рамките на Организацията за наука и технологии на НАТО.

Много съществен елемент от развитието на политиката и практиките в областта на кибер отбраната в НАТО е стартираното сътрудничество с индустрията (NATO Industry Cyber Partnership) по време на срещата в Уелс (2014 г.), както и изграждане на иновационен хъб по кибер сигурност в Хага (в рамките на NCIA). Ежегодният симпозиум по кибер сигурност (октомври, Монс, Белгия) е най-големият форум по темата за страните от НАТО.

Развитие на политиката за кибер сигурност в ЕС и влияние върху България

Цялостната дейност по формиране и реализиране на политиките в областта на кибер сигурността и кибер отбраната в рамките на Европейския съюз (ЕС) и съответните действия за тяхното изпълнение следва да се

разглеждат в контекста на **Стратегията на Европейския съюз за киберсигурност** от 2013 г.[72] **и Заключенията на Съвета**.[73] Това са двата ключови документа, които дефинират основните принципи, стратегически приоритети, цели на Съюза и средствата за тяхното постигане в контекста на Общата политика за сигурност и отбрана (ОПСО) и отношенията с НАТО.

В Стратегията категорично е посочено, че основните ценности на ЕС се прилагат с еднаква сила както във физическия свят, така и в цифровия свят. Същите закони и норми, които се прилагат в други области от ежедневието, се прилагат и в киберпространството. Освен това всяко споделяне на информация за целите на кибер сигурността, когато могат да бъдат застрашени личните данни, следва да съответства на законодателството на ЕС за защита на данните и да отчита изцяло правата на физическите лица в тази област.

Стратегията дефинира следните три основни принципа на сигурността в кибер пространството:

Първо, осигуряване на свободен и равен достъп на всички до интернет. Ограниченият или липсващият достъп до интернет и „цифровата неграмотност“ се разглеждат като неравнопоставеност за гражданите, като се има предвид в каква степен дигитализацията обхваща обществото. В този смисъл всеки човек трябва да има свободен достъп до интернет.

Второ, гарантиране на демократично и ефикасно управление на множество заинтересовани страни в настоящия модел на управление на интернет, като фактор за кибер сигурността.

Трето, съвместна, споделена отговорност за гарантиране на сигурността в кибер пространството на всички заинтересовани страни, независимо дали са публични органи, представители на частния сектор или отделни граждани. Всички те трябва да приемат тази отговорност и, ако е необходимо, да осигурят координиран отговор за гарантиране на кибер сигурността.

Основните стратегически приоритети и действия са следите:

На **първо място** е **поддържането на кибер устойчивост на национално ниво**. В това отношение Стратегията е придружена от предложение за законодателни промени (Директива за мрежова и

72 European commission, Joint communication to the European Parliament, the Council, the European economic and social committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013.

73 COUNCIL OF THE EUROPEAN UNION, Draft Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available from: http://register.consilium.europa.eu/, accessed on 5.11.2018.

информационна сигурност) с цел да се установят общи минимални изисквания за мрежова и информационна сигурност (МИС) на национално равнище. Тези изисквания следва да задължат държавите-членки:

- да определят национални компетентни органи за МИС;
- да създадат добре функциониращ Национален център за действие при инциденти в информационната сигурност (CERT); и
- да приемат национална стратегия за киберсигурност и национален план за сътрудничество в областта на МИС.

Изграждането на капацитет и координацията в областта на киберсигурността се отнасят и до институциите на ЕС. През 2011 г. е създаден екип за реагиране срещу кибер инциденти с трансгранично измерение, отговарящ за сигурността на информационните системи на институциите, агенциите и органите на ЕС (CERT-EU), който започва да работи постоянно през 2012 г. [74]

Важни инструменти за поддържане на кибер устойчивост са European Public-Private Partnership for Resilience (EP3R)[75], Connecting Europe Facility (CEF)[76] и многонационалните учения на ниво ЕС като Cyber Europe 2018.[77]

Важна задача, която Стратегията поставя е повишаване на ситуационната осведоменост на крайните потребители, което е от изключителна важност за защита на информационните системи и мрежи и е обща отговорност на всички заинтересовани страни. Не на последно място в Стратегията се поставя акцент на повишаване на националните усилия в областта на образованието и обучението по кибер сигурност, чрез въвеждане на обучение в училищата със срок до 2014 г., обучение на студенти по компютърни науки; и основно обучение на персонала, работещ в публичната администрация.

Вторият стратегически **приоритет** е драстично намаляване на кибер престъпността.

Акцентът в тази област е върху създаване и прилагане на силно и ефективно законодателство за борба с кибер престъпността. В това отношение се препоръчва да бъдат подкрепени държавите-членки да идентифицират слабите места и пропуските и да засилят способността си да разследват и да се борят с кибер престъпността. Основната цел е да се постигне подобрена оперативна способност за борба с кибер

[74] https://cert.europa.eu/cert/plainedition/en/cert_privacy.html, accesed on 5.11.2018.

[75] https://www.enisa.europa.eu/news/enisa-news/conclusion-for-the-european-public-private-partnership-ppp-for-resilience-scheme, accesed on 5.11.2018.

[76] https://ec.europa.eu/inea/en/connecting-europe-facility, accesed on 5.11.2018.

[77] https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2018, accesed on 5.11.2018.

престъпността. Разчита се на Европейския център за кибер престъпления[78] към Европол, като ключова институция в борбата с кибер престъпността, като и на Евроюст[79] и на Европейския полицейски колеж.[80]

Третият стратегически **приоритет** в свързан с **разработване на политика и способности за кибер отбрана в контекста на Общата политика за сигурност и отбрана на ЕС**. Стратегията предвижда да се направи оценка на оперативните изисквания на ЕС в областта на кибер сигурността и да се насърчи развитието на способности, които да обхващат всички им аспекти включително доктрината, ръководството, организацията, персонала, обучението, технологиите, инфраструктурата, логистиката и оперативната съвместимост. Освен това се планира разработване на Рамка на ЕС за политика в областта на кибер отбраната за защита на мрежите и информационните системи в мисиите и операциите по линия на ОПСО. На следващо място, в Стратегията е предвидено насърчаване на диалога и координацията между гражданските и военните участници в рамките на ЕС – със специален акцент върху обмена на добри практики, обмена на информация и ранното предупреждение, реакцията при инциденти, оценката на риска, повишаването на осведомеността и установяването на кибер сигурността като приоритет. Не на последно място, се предвижда осигуряване на диалог с международни партньори, включително с НАТО, други международни организации и многонационални центрове за върхови постижения, за да се осигурят ефективни отбранителни способности, да се определят областите на сътрудничество и да се избегне дублирането на усилия.

Четвъртият приоритет в Стратегията е свързан с **осигуряване на промишлени и технологични ресурси за кибер сигурността**. Тук акцентът е поставен върху насърчаване на единния пазар на ЕС за продуктите, свързани с кибер сигурността, стимулиране на разработването и приемането на единни стандарти за сигурност, технически норми и принципи на сигурност. Освен това се обръща специално внимание на насърчаване на инвестициите в научноизследователска и развойна дейност и на иновациите. В това отношение полезен инструмент е Програмата на ЕС „Хоризонт 2020“ за насърчаване на ранното включване на промишлеността и на академичните среди в разработването и предлагането на координирани решения, както и Програмата „Хоризонт Европа“[81] —

78 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, accesed on 5.11.2018.

79 https://europa.eu/european-union/about-eu/agencies/eurojust_bg, accesed on 5.11.2018.

80 https://www.europol.europa.eu/agreements/european-police-college-cepol, accesed on 5.11.2018.

81 COM/2018/435 Предложение за Регламент на Европейския парламент и на Съвета за създаване на Рамковата програма за научни изследвания и иновации „Хоризонт Европа“ и за определяне на нейните правила за участие и разпространение на резултатите.

следващата рамкова програма на ЕС за научни изследвания и иновации, която също поставя кибер сигурността сред своите приоритети.

Петият приоритет в Стратегията е свързан със **създаване и прилагане съгласувана международна политика на Европейския съюз в киберпространството**, за да се насърчават основни ценности на ЕС като достойнство, свобода, демокрация, равенство, върховенство на закона и зачитане на основните права на човека. Приоритет е включването на въпросите на сигурността в кибер пространството във външните отношения на ЕС и в Общата външна политика и политиката на сигурност.

В заключение в Стратегията се подчертава, че централизираният подход на ниво ЕС не е най-доброто решение за гарантиране на киберсигурността. **Дейностите трябва да се организират и координират между три основни стълба**:

1) националните органи за мрежова и информационна сигурност;
2) правоприлагащите институции; и
3) министерствата на отбраната.

Проблем е обаче, че те действат в различни нормативни рамки.

Ключовият фактор за успех е добрата координация. Затова държавите-членки следва да разполагат вече или в резултат на приетата стратегия да изградят структури за осигуряване на кибер устойчивост и противодействие на кибер престъпността. Те трябва да достигнат необходимото ниво на способност за справяне с инциденти в кибер пространството. В това отношение е необходимо да се насърчава обмена на информация между националните институции и частния сектор, за да се установят национални планове за сътрудничество в областта на МИС, които да бъдат активирани в случай на кибер инциденти.

В Стратегията се посочват редицата участници на ниво ЕС, които са ангажирани с киберсигурността. По-специално това са Европейската агенция за мрежова сигурност (ENISA), Европейският център за кибер престъпления (EC3) към Европол и Европейската агенция по отбрана (EDA).

В международен план Комисията, Върховният представител за външната политика и политиката за сигурност на Съюза и държавите-членки участват в политически диалог с международни партньори и с международни организации като Съвета на Европа, ОССЕ, НАТО и ООН.

Подобно на активирането на Чл. 5 от Вашингтонския договор, в Стратегията се предвижда колективен отговор и подкрепа от ЕС в случай на голям кибер инцидент или атака спрямо страна-членка на ЕС. Посочено е, че в такъв случай ще бъдат активирани механизмите за ранно предупреждение, а при необходимост и управлението при кризи или други процедури. Особено сериозен инцидент или атака в кибер пространството

би могъл да представлява достатъчно основание за държава-членка на Съюза да се позове на клаузата за солидарност на ЕС (чл. 222) или клаузата за взаимна отбрана (чл. 47.2) от Договора за Европейския съюз.

Важно е да се посочи, че Стратегията за кибер сигурност на ЕС е одобрена от Съвета и е придружена от Директива (ЕС) 2016/1148 от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза[82], като част от Плана за действие на Европейската комисия за гарантиране на свободен и достъпен за всички интернет[83].

Тази директива е първият нормативен документ в областта на кибер сигурността, който покрива целия ЕС. Тя има за цел:

1) изграждане на устойчивост чрез усъвършенстване на националния капацитет за кибер сигурност;
2) насърчаване на по-доброто сътрудничество между държавите-членки; и
3) въвеждане на изискване към икономическите субекти във важни сектори на икономиката като енергетика, транспорт, банки, инфраструктури на финансовите пазари, доставчици на здравни услуги, вода и цифрова инфраструктура и др. да въведат ефективни практики за управление на риска и да докладват на националните органи за сериозните инциденти.

По отношение на специфичните регулаторни области, Директивата е разделена на три основни стълба. На първо място, тя има за цел да установи минимални нива на национални способности (определяне на компетентните национални органи, които да следят прилагането на НИС; създаване на Computer Emergency Response Teams (CERT); приемане на стратегии за МИС). На второ място, тя създава мрежа за сътрудничество между компетентните органи на държавите-членки. Предвижда се да бъде създадена сигурна система за обмен на информация, която да обединява системата за ранно предупреждение за рискове и инциденти и да гарантира координирани отговори. Трето, Директивата изисква субектите, които попадат в приложното поле, да прилагат най-съвременните мерки за сигурност, които гарантират ниво на сигурност, съответстващо на риска. Една от най-важните промени, въведени от Директивата, е изискването за докладване на инциденти на централния орган, ако тези инциденти могат значително да повлияят на непрекъснатостта на услугите. Уведомлението

82 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (*OJ L 194, 19.7.2016, p. 1).*

83 European Commission, EU Cybersecurity plan to protect open internet and online freedom and opportunity, Brussels, 7 February 2013.

трябва да бъде направено без неоправдано забавяне (24-72 часа) след откриването на нарушението.

Друг важен документ на ЕС по отношение на политиката за киберсигурност е Рамката за съвместен дипломатически отговор на Съюза по отношение на злонамерени действия в киберпространството.[84]

Този документ представлява система от мерки в кибер дипломацията, която страните-членки на ЕС могат да предприемат в отговор на злонамерени действия в кибер пространството. Понятието кибер дипломация („cyber diplomacy“) се въвежда първи път с Решение на Съвета през 2015 г.[85]

ЕС отново потвърждава ангажимента си за разрешаване на международните спорове в кибер пространството с мирни средства. Освен това се посочва, че всички дипломатически усилия на ЕС следва приоритетно да бъдат насочени към насърчаване на сигурността и стабилността в кибер пространството чрез засилено международно сътрудничество и намаляване на риска от погрешно възприемане, ескалация и конфликт, които могат да възникнат в резултат на кибер инциденти.

ЕС подчертава, че ясното демонстриране на вероятните последици от съвместния дипломатически отговор на Съюза за такива злонамерени дейности оказва влияние върху поведението на потенциални агресори в кибер пространството, като по този начин се засилва сигурността на Съюза и на неговите държави-членки.

По-нататъшно развитие на политиката за кибер сигурност на ЕС може да се проследи в Съвместното съобщение на Европейската комисия до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“.[86] Документът е одобрен от Съвета[87] и е към него е разработен Първият план за действие за изпълнение на приетите решения.[88]

84 Council of the European Union, Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017.

85 Council of the European Union, Council Conclusions on Cyber Diplomacy, available from: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf, accessd on 5.11.2018.

86 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final

87 Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - Council conclusions (20 November 2017).

88 Council of the European Union, Action Plan for implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 12 December 2017

Няколко момента заслужават **внимание** в този документ.

Първо, разширяването на мандата и засилването на ролята на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), като ключов фактор за укрепването на устойчивостта на ЕС за реагиране на кибер атаки. В това отношение се предвижда сериозна реформа, включително даване на постоянен мандат за агенцията и превръщането ѝ в агенция за кибер сигурност на ЕС.

Второ, Европейската комисия оценява като основен проблем липсата на схеми за сертифициране за кибер сигурност, признати в целия Съюз. Затова се предлага да се създаде Европейска рамка за сертифициране за кибер сигурност.

Трето, пълно прилагане на Директивата за сигурността на мрежите и информационните системи, най-късно до май 2018 г.

Четвърто, **постигане на кибер устойчивост чрез бързо реагиране при извънредни ситуации**. Предвижда се аспектите на кибер сигурността да бъдат включени в съществуващите механизми на ЕС за управление при кризи. За бърза и ефективна реакция се разчита също и на механизъм за бърз обмен на информация между всички най-важни участници на национално и европейско равнище.

Пето, изграждане на мрежа за компетентност в сферата на кибер сигурността с Европейски център за изследвания и компетентност в тази област през 2018 г. Тези структури ще насърчават развитието и внедряването на технологии за кибер сигурност и ще допълват действията за изграждане на капацитет на равнище ЕС и на национално равнище.

През септември 2018 г. е прието Предложение за Регламент на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на кибер сигурността и Мрежа от национални координационни центрове[89]. Центърът за експертни познания ще улеснява и подпомага координирането на работата на мрежата и ще подпомага експертната общност в сферата на киберсигурността, насочвайки развитието в областта на технологиите за кибер сигурност и улеснявайки достъпа до събрания по този начин експертен опит. По-специално, Центърът за експертни познания ще постига това чрез изпълнението на съответните части на програмите „Цифрова Европа“ и „Хоризонт Европа“ чрез отпускане на безвъзмездни средства.

89 ПРЕДЛОЖЕНИЕ ЗА РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове SWD/2018/404 final.

Шесто, **насърчаване на „кибер хигиената“ и общата осведоменост в областта на киберсигурността**. В документа се посочва, че около 95 % от инцидентите са станали възможни поради „някакъв вид човешка грешка, съзнателна или несъзнателна“. Това е показателно за силната роля на човешкия фактор в кибер сигурността. Това означава, че личното поведение, поведението в корпоративен план и това на публичната администрация трябва да се променят, за да се гарантира, че всеки човек разбира опасността и разполага с необходимите средства и умения бързо да открива атаки и активно да се защити от тях. Нужно е хората да си създадат навици за „кибер хигиена“, а бизнесът и организациите да приемат подходящи програми за кибер сигурност, основани на рисковете, и периодично да ги актуализират, за да отразяват развиващата се ситуация на рискове.

Седмо, създаване на ефективна система на ЕС за кибер възпиране, която включва:

- установяване на лицата, действащи злонамерено;
- подобряване на ответните мерки по правоприлагане;
- подобряване на публично-частното партньорство срещу кибер престъпността;
- засилване на политическия отговор; и
- изграждане на възможности за възпиране чрез отбранителния капацитет на държавите-членки.

Осмо, **укрепване на международното сътрудничество в сферата на киберсигурността**, като се надгради постигнатото и се задълбочава сътрудничеството с НАТО в областта на киберсигурността, противодействието на хибридните заплахи и в отбраната, както предвижда съвместната декларация от 8 юли 2016 г. Приоритетите включват насърчаване на оперативната съвместимост чрез ясни изисквания и стандарти, засилване на сътрудничеството при обучение и учения, хармонизиране на изискванията за обучение. Освен това, ЕС и НАТО ще развиват също и сътрудничеството в научните изследвания и иновации за кибер отбрана и ще развиват съществуващото техническо споразумение за обмен на информация относно киберсигурността между техните съответни органи по кибер сигурност.

По отношение на координираните общи действия на ЕС в отговор на мащабни инциденти в областта на кибер сигурността и кризи, внимание заслужават **Препоръката на Европейската комисия към Съвета на ЕС и предложената Схема за координирана реакция при мащабни**

трансгранични инциденти и кризи в кибер сигурността.[90] В документа се посочва, че инцидентът, свързан със сигурността на кибер пространството, може да се разглежда като криза на равнището на Съюза, когато прекъсването, причинено от инцидента, е твърде мащабно, за да може дадена държава-членка да се справи сама или когато се засягат две или повече държави-членки с толкова широко обхватно въздействие от техническо или политическо значение, че той изисква навременна координация и реакция на политическо равнище от Съюза.

В документа са посочени и са описани задълженията на ключовите участници в реагирането при кризи, свързани с кибер сигурността на равнище Съюз. Това са мрежата от екипи за реагиране при инциденти по компютърна сигурност, както и съответните агенции и органи, а именно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), Европейският център за кибер престъпления в Европол, Центърът за анализ на разузнавателните служби на ЕС (INTCEN), Дирекция „Разузнаване“ на Военния комитет на ЕС (EUMS INT) и Ситуационният център (Sitroom), CERT-EU и Координационният център за спешно реагиране в Европейската комисия.

Накрая препоръката на Европейската комисия включа подходи за усъвършенстване на взаимодействието между съответните отговорни структури в държавите-членки и тези в Съюза на политико-стратегическо, оперативно и техническо ниво.

В хода на обзора на основните стратегически и регулативни документи на ЕС за кибер сигурността, специално внимание следва да се отдели на **Регламента на Европейския парламент и на Съвета относно ENISA, „Агенцията на ЕС за киберсигурността“** или т.нар. **„Закон за киберсигурността**“.[91] Регламентът се основава на два основни стълба. Първо той установява целите, задачите и организационните аспекти на Агенцията на ЕС за кибер сигурност (ENISA). Второ – създава рамката на Европейски схеми за сертифициране на киберсигурността в рамките на Съюза.

По отношение на ENISA, Регламентът дава постоянен мандат за Агенцията, за да се позволи ефективна и ефикасна подкрепа за държавите-членки, институциите на ЕС и други заинтересовани страни с оглед гарантиране на сигурно кибер пространство. На първо място ENISA ще има за задача активно да допринася за разработването на политика в областта

90 COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, Official Journal of the European Union, L 239/36, 19.9.2017.

91 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM/2017/0477 final - 2017/0225 (COD).

на мрежовата и информационната сигурност, както и за други политически инициативи, свързани с кибер сигурността в различни сектори (енергетика, транспорт, финанси и др.) На следващо място ENISA ще допринася за подобряването на възможностите и експертните познания на публичните органи на ЕС и на националните органи, включително по отношение на реакцията при инциденти и надзора върху регулаторните мерки, свързани с киберсигурността. Трето, Агенцията ще има отговорности по отношение на обмена на знания и информация, като се превърне в информационен център на ЕС. Това би означавало насърчаването и споделянето на добрите практики и инициативи в целия ЕС чрез обединяване на информация за киберсигурността, произтичаща от ЕС и националните институции, агенции и органи. На четвърто място ENISA ще изпълнява редица функции, свързани с пазара (стандартизация, сертифициране по отношение на киберсигурността). На следващо място ENISA ще има отговорности и по отношение на научните изследвания и иновации, като допринася със своя експертен опит, консултира европейските и националните органи относно определянето на приоритети в научноизследователската и развойна дейност, включително в контекста на публично-частно партньорство в киберсигурността. Не на последно място, Агенцията ще подпомага оперативното сътрудничество при управление при кризи на базата на укрепване на съществуващите превантивни оперативни способности и по-специално повишаване ефективността на общоевропейските учения по кибер сигурност (Cyber Europe). ENISA също така ще играе роля при определяне на препоръката на Комисията към държавите-членки за координиран отговор в случай на мащабни трансгранични инциденти в областта на кибер сигурността.

По отношение на втория стълб на Регламента, Европейската рамка за сертифициране на кибер сигурността за продукти и услуги в областта на ИКТ, ще се предоставят няколко предимства за гражданите и бизнеса. На първо място се създават схеми за сертифициране на кибер сигурността за конкретни продукти или услуги в целия ЕС на “едно гише“. На второ място, Рамката утвърждава предимството на европейските схеми за сертифициране на киберсигурността по отношение на националните такива. Съгласно правилото на чл. 49, приемането на европейска схема за сертифициране на кибер сигурността ще замени съществуващите паралелни национални схеми за същите продукти или услуги в областта на ИКТ на дадено ниво на сигурност. На трето място, Регламентът ще подкрепи и улесни разработването на европейска политика в областта на киберсигурността чрез хармонизиране на условията и съществените изисквания за сертифициране на кибер сигурността на продукти и услуги в областта на ИКТ в ЕС.

Основният документ на ЕС, който дефинира целите, принципите и подходите в кибер отбраната в рамките на Съюза е **EU Cyber Defence Policy Framework**.[92] В този документ са представени виждания за улесняване на сътрудничеството с частния сектор в областта на развитието на способностите за кибер отбрана. Освен това тук се обръща специално внимание на укрепването на научноизследователската и технологичната дейност и Европейската отбранителна технологична и индустриална база (EDTIB). Не на последно място политическата рамка осигурява съгласуваност между усилията на ЕС и НАТО в кибер отбраната и предлага области за сътрудничество между тях.

Подобно на НАТО, и в ЕС тече дискусия за дефиниране на кибер пространството като пети домейн на военните операции, еднакво критичен за прилагането на Общата политика за сигурност и отбрана на Европейския съюз, както сушата, морето, въздуха и космоса.

Приоритет за ЕС е да се осигури непрекъсната оценка на уязвимостта на информационните инфраструктури и гарантиране устойчивостта на мрежите при операциите по линия на ОПСО. Акцентът е поставен както върху подобряването на защитата на комуникационните мрежи на структурите, така и върху развитието на способностите на кибер отбрана на държавите-членки. Развитието на способностите и технологиите за кибер отбрана трябва да обхваща всички аспекти на развитието им, включително доктрината, лидерството, организацията, персонала, обучението, технологиите, инфраструктурата, логистиката и оперативната съвместимост.

За постигане на тези цели ще се използва Плана за развитие на способностите, за да се подобри степента на сближаване в планирането на изискванията за кибер отбраната на държавите-членки на стратегическо ниво. Предвижда се също подкрепа за настоящи и бъдещи проекти за обединяване и споделяне в областта на кибер отбраната. Освен това ще се разработи стандартен набор от цели и изисквания, определящи минималното равнище на кибер сигурност и доверие, което държавите-членки трябва да постигнат, като използват съществуващия опит в ЕС. За това ще спомогне насърчаването на споделянето на информация за кибер заплахи в реално време между държавите-членки и съответните структури на ниво ЕС. На следващо място се предвижда засилване на доброволното сътрудничество между военните CERT на държавите-членки с цел подобряване на предотвратяването и справянето с инциденти. Не на последно място се предвижда разработването на обучение по кибер отбрана с оглед на сертифицирането на бойните групи в ЕС.

92 Council of the European Union, EU Cyber Defence Policy Framework, Brussels, 18 November 2014.

EU Cyber Defence Policy Framework предвижда Европейската агенция за мрежова и информационна сигурност (ENISA), Европейският център за борба с кибер престъпността към Европол (EC3) заедно с други компетентни агенции на ЕС, както и държавите-членки се насърчават в рамките на ОПСО да засилят сътрудничеството си в следните области:

- **разработване на общи профили за компетентност в областта на кибер сигурността и кибер отбраната**, основаващи се на добрите международни практики, използвани от институциите на ЕС, като се вземат предвид и стандартите за сертифициране в частния сектор;
- **развитие и адаптиране** на организационните и техническите стандарти в кибер сигурността и защитата на публичния сектор за използване в сектора на отбраната и сигурността;
- **разработване на работещ механизъм за обмен на добри практики** относно ученията, обучението и други области на евентуална цивилно-военна синергия;
- **увеличаване на възможностите на ЕС** в областта на превенцията, разследването и съдебната медицина и засиленото им използване в развитието на способностите на кибер отбраната.

На следващо място анализираният документ предвижда конкретни дейности за улесняване на гражданско-военното сътрудничество в развитието на способностите за кибер отбрана и укрепване на Европейската отбранителна технологична и индустриална база. В това отношение ще се търси синергия на усилията в областта на научните изследвания и технологиите във военния сектор с граждански програми за научноизследователска и развойна дейност като „Хоризонт 2020“ и „Хоризонт Европа“;

Освен това Европейската служба за външни дейности ще определи приоритети за обучение по линия на ОПСО заедно с EDA, Европейския колеж по сигурност и отбрана и държавите-членки. Предвижда се обучение и образование в рамките на ОПСО за различни аудитории, включително персонал, участващ в мисии и операции по линия на ОПСО. Акцент се поставя върху необходимостта от установяването на стандартите за обучение и сертифицирането за кибер отбрана. В това отношение се предвижда установяване на взаимодействие с други заинтересовани страни, като ENISA, Европол, Европейската група за обучение и образование в областта на кибер престъпленията (ECTEG), Европейския полицейски колеж (CEPOL), както и с Центъра на НАТО за върхови постижения в сътрудничество в кибернетичното пространство в Естония.

Не на последно място EU Cyber Defence Policy Framework предвижда развитие на допълнително сътрудничество в областта на кибер отбраната между ЕС и НАТО в области като:

- обмен на добри практики при управление при кризи, както и във военни операции и граждански мисии;
- разработване на изискванията за способности в кибер отбрана;
- разработване на концепции за обучение и образование в областта на кибер отбраната и ученията; и
- сътрудничеството между органите на CERT-EC и съответната структура на НАТО – NCIRC с цел подобряване на осведомеността относно ситуацията, обмен на информация, механизми за ранно предупреждение и предвиждане на заплахи, които биха могли да засегнат двете организации.

С приетата от **Европейския парламент (ЕП) Резолюция 2018/2004 (INI) относно кибер отбраната** през юни 2018 г.[93] се актуализират и препотвърждават редица постановки от цитираните по-горе стратегически и нормативни документи на ниво ЕС и се призовават държавите-членки на Съюза да работят в тясно сътрудничество, за да се противопоставят на нарастващите кибер и хибридни предизвикателства и атаки.

Кибер отбраната остава основна компетентност на държавите-членки, потвърждава резолюцията на ЕП, но все пак ЕС има водеща роля в осигуряването на платформа за сътрудничество в рамките на Съюза и ще координира усилията в трансатлантическата архитектура за сигурност, за да се избегнат пропуски и неефективност, които съпътстват много традиционни усилия в областта на отбраната.

Кибер и хибридните предизвикателства, заплахи и атаки се извеждат на преден план и се посочва, че те представляват сериозна заплаха за сигурността, отбраната, стабилността и конкурентоспособността на ЕС, неговите държави-членки и неговите граждани.

За пръв път в документ от подобен характер се посочват потенциалните източници на кибер и хибридни заплахи. Това са различни държавни участници като Русия, Китай и Северна Корея, както и недържавни участници (включително организирани престъпни групи), мотивирани, наети или спонсорирани от държави, агенции за сигурност или частни компании, които вече са участвали в злонамерени дейности в кибер пространството за постигане на политически, икономически или свързани със сигурността цели. Тези действия включват атаки срещу критична инфраструктура, кибер шпионаж и масово наблюдение на гражданите на

93 European Parliament, 2014-2019, REPORT on cyber defence (2018/2004(INI)), European Commission, Bruselss, 25.5.2018.

ЕС, подпомагане на кампании за дезинформация и разпространение на злонамерен софтуер (например Wannacry и NotPetya) и др.

В това отношение заслужават внимание също заключенията на Съвета, където се посочва, че ЕС изразява сериозната си загриженост относно повишената способност и готовност на трети държави и недържавни участници да преследват своите цели чрез предприемане на зловредни дейности в кибер пространството и ще продължи да засилва своите възможности за справяне с кибер заплахите. ЕС признава, че взаимосвързаните и сложният характер на кибер пространството изисква съвместни усилия от страна на правителствата, частния сектор, гражданското общество, техническата общност, потребителите и академичните среди за справяне с предизвикателствата, пред които са изправени, и призовава тези заинтересовани страни да признаят и поемат своите специфични отговорности за поддържането на открито, свободно, сигурно и стабилно кибер пространство.[94]

В Резолюция 2018/2004 ясно се посочва, че кибер защитата включва както военни, така и граждански измерения и, че границата между гражданската и военната намеса в кибернетичното пространство все повече се размива.

ЕП препотвърждава клаузата за взаимна защита, член 42, параграф 7 от Договора за ЕС, която предвижда взаимно задължение за помощ и подкрепа чрез всички сили и средства в случай на въоръжена агресия срещу територията на държава-членка на Съюза. Клаузата за солидарност, член 222 от Договора за ЕС, допълва клаузата за взаимна защита, като предвижда, че държавите от ЕС са длъжни да действат съвместно, когато държава от ЕС е станала жертва на терористична атака или природно или причинено от човека бедствие. Няма изрично посочен текст, който насочва към прилагане на чл. 47.2 и чл. 222 в случай на кибер атака с особено големи мащаби.

Заключението на ЕП по отношение на многобройните инциденти в кибер пространството е, че те се дължат на липсата на гъвкавост и устойчивост на инфраструктурата на частните и публичните мрежи, поради слабо защитени или неосигурени бази данни и поради други недостатъци в критичната информационна инфраструктура. Ясно е посочено, че само малка част от държавите-членки поемат отговорността за защитата на съответните им мрежови и информационни системи и свързаните с тях данни, което обяснява пълната липса на инвестиции в обучение и

[94] Council of the European Union, Council conclusions on malicious cyber activities – approval, Brussels, 16 April 2018, http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf, accesed on 5.11.2018.

съвременните технологии за сигурност, както и разработването на подходящи политики и насоки за киберсигурност.

В същото време в документа се посочва, че кибер възпирането и отбраната на въоръжените сили на Европа и критичната инфраструктура са изключително важни в дебатите относно модернизацията на отбраната, общите усилия на Европа в областта на отбраната, бъдещото развитие на въоръжените сили и техните операции, както и за стратегическата автономия на Европейския съюз.

Освен това като проблем, който се нуждае от допълнително внимание е посочен фактът, че кибер командванията в различните държави-членки на Съюза се различават в своите офанзивни и отбранителни мандати. Освен това целите, задачите, организацията на другите национални структури за кибер отбрана на държавите-членки варират в широк смисъл и често остават разпокъсани. В същото време кибер отбрана и възпирането са дейности, които най-добре могат да бъдат решени съвместно на Европейско равнище и в сътрудничество между партньорите и съюзниците. Затова ЕП идентифицира наличие на спешна необходимост от засилване на възможностите на ЕС в областта на кибер защитата.

Специално внимание в Резолюцията е отделено на засилване на ситуационната осведоменост, разкриването на злонамерен софтуер и обмена на информация чрез използване на съществуващи проекти като Malware Information Sharing Platform (MISP)[95] и Multi-Agent System For Advanced Persistent Threat Detection (MASFAD).[96]

По отношение на необходимостта от изграждане на капацитет и обучение в областта на кибер защита, се посочва, че те са значителни и се увеличават и най-ефективно могат да се осъществят съвместно на равнище ЕС и НАТО. Важно е също да се използват по-пълноценно възможностите за обучение, които предлага European Security and Defence College (ESDC). В момента Колежът предлага специализирани курсове като „Cyber defence and security for senior decision makers“, „Understanding the Civil-Military Dimension of Cyberattacks“, „EU facing "Hybrid Threats" and Challenges“, „Cyber ETEE conference“, „Challenges of EU Cyber Security“, както и докторска програма по „Cyber, new technologies and security in the CSDP context“.[97]

Не на последно място в Резолюцията се подчертава, че кибер защита трябва да бъде надлежно разгледана и да бъде неотменен елемент на всички етапи от процеса на планиране на мисиите и операциите по линия на ОПСО.

---

[95] https://www.misp-project.org/, accessed on 5.11.2018.

[96] http://www.sic.rma.ac.be/research/RUAI/proj363.html, accessed on 5.11.2018.

97 Source: https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/4369, accessed on 28.10.2018.

В заключение, Резолюция 2018/2004 (INI) на Европейския парламент представя в обобщен вид най-важните политики и практически стъпки, които следва да се предприемат на ниво ЕС за гарантиране на кибер отбраната на Съюза.

На **първо място** е **необходимостта от развитие на способностите за кибер защита и възпиране**. В това отношение се подчертава, че една обща политика в областта на кибер защитата и изграждането на значителна способност за защита на кибер пространството следва да съставляват основни елементи в развитието на Европейския отбранителен съюз. Освен това се припомня, че кибер отбраната има както военно, така и гражданско измерение и затова е необходим интегриран политически подход и тясно сътрудничество между военни и цивилни заинтересовани страни.

На следващо място ЕП призовава за **последователно развитие на капацитет за кибер защита** във всички институции и органи на ЕС, както и в държавите-членки и за осигуряване на необходимите политически и практически решения за преодоляване на оставащите политически, законодателни и организационни пречки пред сътрудничеството в кибер отбраната. Редовният и засилен обмен и сътрудничество между съответните заинтересовани страни в кибер защитата на равнище ЕС и на национално равнище е изключително важен.

По-нататък в документа се посочва категорично, че в рамките на нововъзникващия Европейски отбранителен съюз **изграждането на капацитет за кибер отбрана на държавите-членки трябва да бъде на преден план** и, доколкото е възможно, да бъде **интегриран от самото начало**, за да се гарантира максимална ефикасност.

Не на последно място ЕП признава, че **притежаването на собствени способности за кибер отбрана е в основата на национална стратегия за сигурност** на редица държави-членки и, че това е съществена част от националния им суверенитет. Наред с това се подчертава, че поради естеството на кибер пространството без граници, мащабът на знанията, необходими за действително ефективен отговор, който гарантира стратегическата автономия на ЕС в кибер пространство, е извън обсега на всяка отделна държава-членка и поради това се налага, засилено и координирано действие от страна на всички държави-членки на равнище ЕС.

На **второ място** са **политиките и действията за осигуряване на кибер защита на мисиите и операциите на Съюза по линия на ОПСО**. В Резолюцията ясно се подчертава, че кибер защитата следва да се разглежда като основна задача в мисиите и операциите по линия на ОПСО и, че тя следва да бъде включена във всички процеси на отбранително планиране.

На **трето място** са **политиките и действията в областта на образованието и обучението в кибер отбраната**. Резолюцията отбелязва, че един ефективно организиран и интегриран процес на образованието и обучението по кибер сигурност в ЕС би намалил значително заплахите и призовава Съюза и държавите-членки да засилят своето сътрудничество в областта на образованието, обучението, ученията и оценяването им (ETEE). В това отношение се подкрепя военната програма "Еразъм" и други общи инициативи за обучение и обмен между страните-членки. Добър пример е също създаването в рамките на Европейския колеж за сигурност и отбрана на платформата за образование, обучение и оценка на кибер отбраната. На следващо място се посочва, че устойчивостта на кибер пространство изисква безупречна „кибер хигиена“ и затова ЕП призовава всички заинтересовани страни от публичния и частния сектор да провеждат редовни обучения в тази посока. На последно място ЕП препоръчва обменът на опит и извличането на поуки от практиката да бъдат засилени между въоръжените сили, полицейските сили и другите държавни органи на държавите-членки, активно ангажирани в борбата срещу кибер заплахи.

Четвъртата група препоръки по отношение на необходимите политики и практически действия в областта на кибер отбраната засяга **сътрудничество между ЕС и НАТО**. Отново се заявява, че на основата на общите си ценности и стратегически интереси, ЕС и НАТО имат специална отговорност и капацитет да се справят по-ефективно с нарастващите предизвикателства, свързани с кибер сигурността и кибер отбраната, и в тясно сътрудничество, като търсят възможни допълнения и се избягва дублирането на дейности. Необходимо е да продължи обмена на концепции за интегриране на изискванията и стандартите за кибер отбрана в планирането и провеждането на мисии и операции с цел насърчаване на оперативната съвместимост.

Като добра практика е посочено споразумението между CERT-EU и Центъра на НАТО за реагиране при компютърни инциденти (NCIRC). Накрая ЕП призовава Комисията да разработи пътна карта за осъществяване на координиран подход към Европейската кибер защита, включително актуализиране на Рамката на политиката на ЕС в областта на кибер отбраната.

Изисквания, произтичащи от приетата политика за кибер сигурност и кибер отбрана в НАТО и ЕС към развитие на организацията за кибер сигурност в България

Прегледът на регулаторните инструменти, политики и стратегии за киберсигурност и кибер отбрана на НАТО и ЕС в предходните два раздела

на тази глава дава възможност да се систематизират **основните изисквания към развитие на организацията за кибер сигурност в България**. Те могат да се обединят в няколко групи.

Първата група обединява изискванията към изграждане на национални способности за кибер сигурност и принос към кибер сигурността и кибер отбраната на Съюзно ниво.

Както е посочено в Резолюция 2018/2004 (INI) на ЕП, кибер отбраната остава основна компетентност на държавата, което поставя сериозни изисквания към изграждането и поддържането на целия спектър от компонентите на способностите (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities, Interoperability (DOTMLPFI). Затова изграждането и развитието на националните способности за кибер отбрана и осигуряването на оперативна съвместимост със съюзниците следва да се определят като приоритет на отбранителната политика на страната.

В същото време и НАТО и ЕС оценяват съществуващите национални способности на повечето от съюзниците като недостатъчни и фрагментирани, за да осигурят високо ниво на МИС на съюзно ниво. Това се отнася в пълна сила и за България и е фактор, който води до затруднения при осъществяването на взаимодействие със съюзниците и намалява възможностите за координиран отговор в случай на кибер атаки. Затова следва да се има предвид препоръката на ЕП за спешна необходимост от засилване на способностите на ЕС в областта на кибер защитата и дефиниране на минимални нива на национални способности.

Необходимо е да се направи преглед на съществуващите национални способности за кибер сигурност и кибер отбрана и да се идентифицират евентуални пропуски в нормативната база и организационни пречки пред сътрудничеството на национално и съюзно ниво.

Необходимо е също да се направи преглед и актуализиране на необходимите стратегии, пътни карти, доктрини и процедури и да се прецени доколко те са адекватни на актуалните рискове и заплахи в кибер пространството и доколко създават условия за сътрудничество между всички заинтересовани страни на национално и съюзно ниво.

На следващо място специално внимание заслужава развитието на системата на отбранителното планиране, за да се реализира политиката за пълно интегриране на кибер отбраната като приоритет в процеса на планиране и да се осигури непрекъсната оценка на уязвимостта на информационните инфраструктури и гарантиране устойчивостта на мрежите и при мисиите и операциите на НАТО и ЕС. Важно е също така при планирането да се изпълни изискването за интегриран подход и тясно

сътрудничество между военни и цивилни заинтересовани страни в кибер отбраната.

Сериозни предизвикателства пред отбранителното планиране поставят решенията на НАТО, а именно че кибер отбраната е неотменна част от основната задача на Алианса за колективна отбрана, включването на киберпространството като домейн на бойното пространство и създаването на Център за кибер операции. Много въпроси чакат отговор: Как България ще допринесе за реализиране на кибер възпиране на потенциални агресори в кибер пространството? Как на практика ще се задейства при необходимост чл. 5 от Северноатлантическия договор в случай на мащабна кибер атака? Как ще се реализира нашето участие и какъв ще бъде българският принос към Центъра за операции на НАТО в кибер пространството?

На следващо място България следва да създаде и поддържа структура за осигуряване на кибер устойчивост. Дали това ще бъде Кибер командване или друга национална структура и коя институция в страната трябва да има водеща роля, това трябва да покаже прегледа. При всички случаи е необходима интегрирана национална междуведомствена структура с участие на бизнеса, академичните среди и неправителствения сектор, която да осигури интегриран подход към кибер сигурността.

Не на последно място е важно да се прецени как България ще допринася за периодично актуализиране на Рамката на политиката на ЕС в областта на кибер отбраната. В това отношение от съществено значение са заключенията и препоръките в последния доклад за напредъка в изпълнението на политиката, където се препоръчва Европейската служба за външни дейности и Европейската агенция за отбрана, съвместно с Европейската комисия, и на основата на приноса на страните-членки, да се предприемат действия за актуализиране на документа до средата на 2018 г.[98]

Втората група обединява изискванията към актуализиране на нормативната база за кибер сигурността и кибер отбраната. И НАТО и ЕС приемат, че международното право се прилага в кибер пространството. Дейностите в кибер сигурността и кибер отбраната трябва да се организират и координират между три основни стълба:

1) националните органи за мрежова и информационна сигурност;
2) правоприлагащите институции; и
3) министерствата на отбраната.

[98] Council of the European Union, Annual Report on the Implementation of the Cyber Defence Policy Framework, available from, http://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf, accessed on 5.11.2018.

Те обаче в момента действат в различни нормативни рамки и това определено е проблем, който заслужава внимание. С приемането от Народното събрание на Закона за кибер сигурност, беше постигнат сериозен напредък в това отношение, но реалната работа за подобряване на координацията и взаимодействието между институциите на държавата и останалите заинтересовани страни в киберсигурността тепърва предстои.

Третата група обединява изискванията към организацията на киберсигурността в България. Ключовата дума тук е осигуряване на взаимодействие и координация между всички заинтересовани страни. Имаме определени проблеми в междуинституционалното сътрудничество, както и в публично-частно партньорство и обмена на информация между националните институции и частния сектор, за да се установят национални планове за сътрудничество в областта на МИС за подобряване на стандартите за сигурност и обмен на информация и насърчаване на интегриран подход към кибер сигурността. Реализирането на този подход ще доведе до по-добри възможности за реагиране при кибер инциденти и обединяване на ресурси.

По отношение на организацията на кибер сигурността у нас е важно да се оцени до каква степен е изпълнено изискването на Директивата за сигурността на мрежите и информационните системи за нейното пълно прилагане, което е с вече изтекъл срок - май 2018 г.

На следващо място заслужава внимание подготвеността на страната за изпълнение на предложения Регламент на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на кибер сигурността и Мрежа от национални координационни центрове, когато се създадат. Как ще изградим национален координационен център, как ще мобилизираме експертната общност в сферата на кибер сигурността и какъв ще бъде Българският принос към Европейския център?

Четвъртата група обединява изискванията към хората в киберсигурността. И НАТО и ЕС вече са осъзнали, че за гарантиране на кибер сигурността и кибер отбраната хората са също толкова важни, както и технологиите. Затова се отделя специално внимание на сътрудничеството в сферата на образованието, обучението, ученията и тяхната оценка (EETE), както и на хармонизиране на изискванията към този процес. В това отношение са необходими сериозни националните усилия в областта на образованието и обучението по кибер сигурност, чрез въвеждане на обучение в училищата, обучение на студенти по ИКТ и основно обучение на персонала, работещ в публичната администрация.

Важно е да се акцентира на повишаване на общата осведоменост и „кибер хигиена“ на персонала на базата на идентифицирани в рамките на

двата съюза общи профили за компетентност в областта на кибер сигурността и кибер отбраната, основаващи се на добрите международни практики.

Необходимо е да се възползваме по-активно от възможностите за обучение, които предоставят образователните институции на ЕС и НАТО: Центърът за върхови постижения и сътрудничество в областта на кибернетичното пространство на НАТО, Училището на НАТО в Оберамергау, Германия; Колежа на НАТО в Рим, Италия, Академията за комуникации и информация на НАТО и Европейския колеж по сигурност и отбрана.

Добре би било да се използват възможностите също на разработените в рамките на Проектите „Интелигентна отбрана“ на НАТО в кибер защита платформа за разпространение на информация за зловреден софтуер (MISP) многонационално образование и обучение в кибернетичната отбрана (MN CD E & T) и на ЕС Malware Information Sharing Platform (MISP) и Multi-Agent System For Advanced persistent threat Detection (MASFAD).

Петата група обединява изискванията към процеса на Сертификация за кибер сигурност. Както се вижда от направения преглед на регулаторните механизми в ЕС, Европейската комисия оценява като основен проблем липсата на схеми за сертифициране за кибер сигурност, признати в целия Съюз. Затова е важно България да участва активно в процеса на прилагане на Европейската рамка за сертифициране за киберсигурност.

Последната, но не по значение **група** изисквания, произтичащи от направения преглед на регулаторните механизми и стратегически документи в НАТО и ЕС, **е свързана с научноизследователската и развойна дейност.** Една от недостатъчно използваните възможности е активното включване в многонационални изследователски групи в рамките на Организацията за наука и технологии на НАТО. За целта обаче България, и в частност Министерството на отбраната, следва да преоцени политиката в областта на научните изследвания и развойната дейност и да създаде специална програма, чрез която на проектен принцип да се финансират разработки с важно значение в областта на кибер сигурността и кибер отбраната. Добре би било при формулиране на перспективни теми за изследвания в областта на кибер отбраната да се следват и формулираните от Европейската агенция по отбраната EDA CAPTECHs[99],

[99] https://www.eda.europa.eu/what-we-do/activities/activities-search/captech-components, accessed on 28.10.2018.

както и ежегодно актуализираните приоритети на Организацията за наука и технологии на НАТО[100].

Освен това следва по-активно да се използват механизмите на Програмата на ЕС „Хоризонт 2020“ и следващата рамкова програма за научни изследвания и иновации „Хоризонт Европа“, която ще се изпълнява след 2021 г. Основа на участие на България, обаче, в международни изследователски, образователни, индустриални програми е съществуването на добре финансирани и управлявани национални програми за изследване и обучение, както и наличие на система от национални учения.

ПРЕПОРЪКИ ЗА УСЪВЪРШЕНСТВАНЕ НА ДЪРЖАВНАТА ПОЛИТИКА В ОБЛАСТТА НА КИБЕР СИГУРНОСТТА

Усъвършенстване на основните процеси за постигане на кибер сигурност

От първостепенна важност е изграждането на ефективен модел за ръководство на **консолидирана мрежа** от звена в сферата на кибер сигурността (администрация, академична общност, индустрия) в контекста на организацията за е-Управление (Фигура 3). Консолидацията е важна както в рамките на администрацията, индустрията и академичния сектор (вкл. НПО и други граждански организации), така и между тези групи на базата на съвет за консултации и координация, както и съвет за вземане на решения, вкл. ресурсни.

Консолидацията е възможна на базата на добра карта на звената с компетентности по кибер сигурност (и е-Управление) от една страна, а от друга оценка на въздействието / моделиране на основните документи за изграждане на пълно и непротиворечиво **описание на процесите**, идентифициране на органите/организациите и създаване на RACI (responsible, accountable, coordinated, informed) матрица. На базата на началната консолидация на звената и изчистване на процесите може да се създаде „As-Is“ архитектура, на базата на която да почне разработване на алтернативи за последваща рационализация и оптимизация.

Съществено за сферата на кибер сигурността е да се постигне **разграничаване и синхронизация на организациите за кибер сигурност** в публичната администрация, сектора за сигурност, индустрията и академичния сектор, както и механизмите за институционализиране на

[100] https://scienceconnect.sto.nato.int/apps/10716, accessed on 28.10.2018.

взаимодействието в ЕС и НАТО, сътрудничеството в регионален и глобален план.

Фигура 3. Организация за е-Управление/КС в Публичната администрация

В сферата на ДА / публичната администрация се изисква синхронизация на работата на **Съвета за е-Управление и Съвета за кибер сигурност** за постигане на **единен подход за ефективно, ефикасно и кибер устойчиво управление на ИТ/информационните ресурси** в контекста на утвърждаване на ролите на Главен информационен мениджър (ГИМ) и Мениджър по киберсигурността (МКС).

Работата на тези съвети позволява да се създаде организация за ефективно, ефикасно и кибер устойчиво управление на ИТ /

информационните ресурси (ИР) за е-Управление в ДА / ПА, като се федерират сегменти за:

- формиране на политика и контрол;
- ресурсно управление в сферата на е-Управление и кибер сигурност;
- изпълнение на политиката;
- придобиване на способности;
- предоставяне на услуги на база на придобити способности;
- провеждане на научно и научно-приложни изследвания;
- образование и подготовка на персонала, вкл. съвместно с изследванията – организиране на демонстрации и учения.

Необходими промени в организацията за кибер сигурност и управлението на информационните ресурси

Промените в организацията могат да се планират едва след добра карта (оперативна архитектура) и оценка на сега действащата система за създаване на алтернативи при отчитане на различните оси на действие:

- вземане на решения, вкл. ресурсни;
- координация на различните оси на действие;
- научни изследвания;
- придобиване на способности и услуги (аутсорсване);
- обучение – индивидуално и групово;
- оперирane на способностите / операции, услуги;
- одит и контрол.

Изследването по първия раздел от тази глава дава добра картина и с препоръките от втория раздел от тази глава, както и резултатите от трета глава се разработват и оценяват алтернативи по **цел – максимално ефективно, ефикасно и кибер устойчиво управление на информационните ресурси с висока степен на гъвкавост / адаптивност и принос към свързани дейности**. Допълнителни критериите могат да са:

- приемливост за гражданите;
- приложимост в български условия;
- наличие на подготвен персонал;
- достъпност на необходимите технологии;
- време за промяна;
- цена на прехода;
- степен на риск от прекъсване на ИТ поддръжката.

В този контекст препоръките за промени са представени във Визията в трета глава от този документ.

Развитие на критични технически системи по кибер сигурност

Критичните елементи за кибер сигурност са преди всичко свързани със степента на „управляемост“ на мрежите – колко мрежи, ниво на централизация на управлението им, степен на консолидация на кибер значимата информация между различните мрежи, вкл. наличие на добри „кибер сензори“, ефективност на събираната и изобразявана „обща кибер картина“, използване на Изкуствен интелект / Машинно обучение за ситуационна осведоменост и вземане на решение, способност за бързо обменяне на критична информация и други, които по-детайлно ще се изследват по дейности 3, 4 и 5, а резултатите ще се интегрират във Визията по дейност 6.

Основната препоръка тук е, че критичните технически системи за кибер сигурност се изграждат (вграждат) в основните елементи на инфраструктурата и приложенията, са част от интензификация на обучението на кибер специалисти и в най-голяма степен (поради естеството на кибер пространството – глобално, бързо променящо се) са системи базирани на модели за работа в реално време с голям обем от данни с използване на Изкуствен интелект.

Подобряване на ресурсното осигуряване на организацията за кибер сигурност

Ресурсното осигуряване може да се оцени само в контекста на анализ на ресурсите за ИТ като цяло и в частност на базата на оценка на риска от пропадане на ИТ системите. Ресурсите се оптимизират в контекста на холистичен подход към ефективност, ефикасност и кибер устойчивост на управлението на ИР.

Най-ценния и най-скъпия ресурс си остават хората и именно затова централно място заема управлението на човешките ресурси. В този контекст като минимум е необходима институционализация на **национална програма за обучение и сертификация** на персонала по кибер сигурност (вкл. система от учения, създаване на “кибер резерв„) – интеграция в организацията за ETEE / EAB.Cyber на ЕС и NCI Academy на НАТО.

Обучението обаче е само част от управление на човешките ресурс – необходима е добра система за подбор, развитие / ротация, задържане на персонала в тази област, създаване на механизми за „кибер резерв“, както и ползване на екипи за бързо реагиране от партньорски организации.

Използването на консултанти и аутсорсване на дейности към индустрията от ПА е част от управление на човешките ресурси.

Много важен инструмент е ротиране на хора между организацията за кибер сигурност и структури на НАТО (например NCIA) и ЕС (например ENISA, ELISA, новия Център на компетентност).

Усъвършенстване на капацитета за управление на промяната за подобряване на устойчивостта и нарастване на нивото на зрялост

Промяната винаги изисква ясна визия, резултат от изследвания – от приложни и организационни аспекти на кибер сигурността до специфични технологични разработки. В този смисъл институционализацията на национална **научна програма** за ефективно, ефикасно и кибер устойчиво управление на ИТ/ИР с фокус върху приложението в академичния сектор и синхронизация с Цифрова Европа и Хоризонт Европа на ЕС чрез изграждане на **национална мрежа от центрове** и интеграция в мрежата от центрове / лаборатории на ЕС е важна препоръка за усъвършенстване на организацията за кибер сигурност.

Важна препоръка е за участие на България в Европейски център за промишлени, технологични и изследователски експертни познания в областта на кибер сигурността. Паралелно с това се налага относително бързо (и във връзка с национална научна програма) да се номинира **национален координационен център** по регламента на ЕС за Европейски център за промишлени, технологични и изследователски експертни познания в областта на кибер сигурността и Мрежа от национални координационни центрове

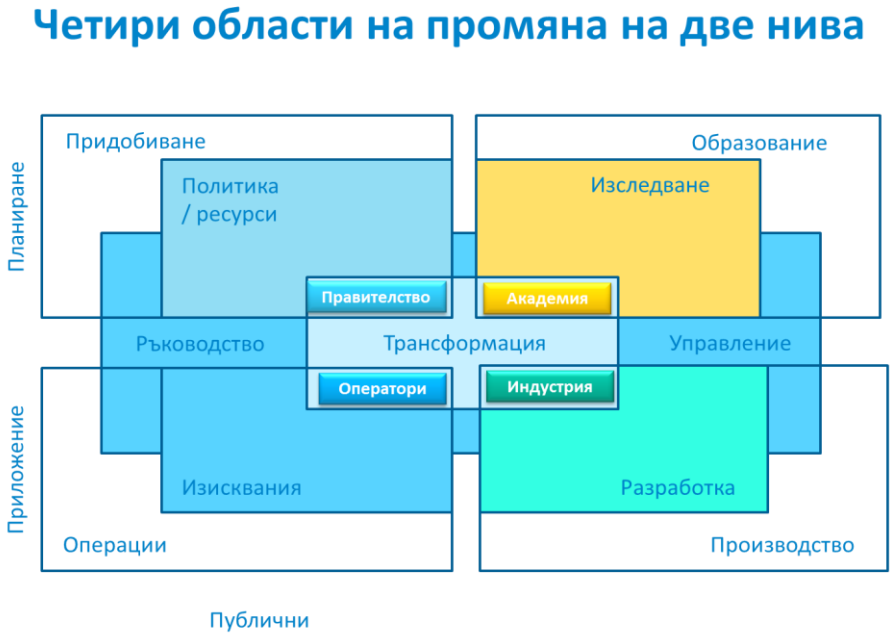
Изграждане на **Национален и академичен CERT** по утвърдените добри практики в ЕС и НАТО в координация с центровете за управление на мрежите на администрацията и академичната общност.

Оказване на помощ от Националния и академичния CERT за изграждане на **секторни CERT** и тестване на началната организация с **национално кибер учение** още през 2019 г.

Трансформационната промяна изисква синхронизирани действия и в 4-те квадранта от Фигура 4 на две нива. Четирите квадранта са съответно с по две нива на ангажиране в единна спирала:

- правителство с две нива:
  - формиране на политика;
  - придобиване на способности;
- оператор на системата:
  - определяне на изисквания;
  - опериране на придобитата способност;

- академичен сектор;
  - изследвания по кибер сигурност по формиране на политика, определяне на способности и разработка на решения;
  - обучение (индивидуално и групово) на персонала за опериране на способности;
- индустрия:
  - разработка на индустриални решения за оперативните изисквания;
  - производство на оборудване и приложения за способности, придобивани от правителството.



Фигура 4. Измерения на промяната в организацията за е-Управление и кибер сигурност

За поддържане на процеса на промяна в организацията за кибер сигурност е необходимо да се създаде и развива среда за консултации, експерименти, учения и подкрепа на трансформацията по модела на Фигура 5.

Представители на четирите квадранта на Фигура 4 след предварителна подготовка, работят като екип за промяна в средата от Фигура 5 по разработване на алтернативи, оценката им, избор на предпочитана алтернатива и стратегическо планиране на нейното

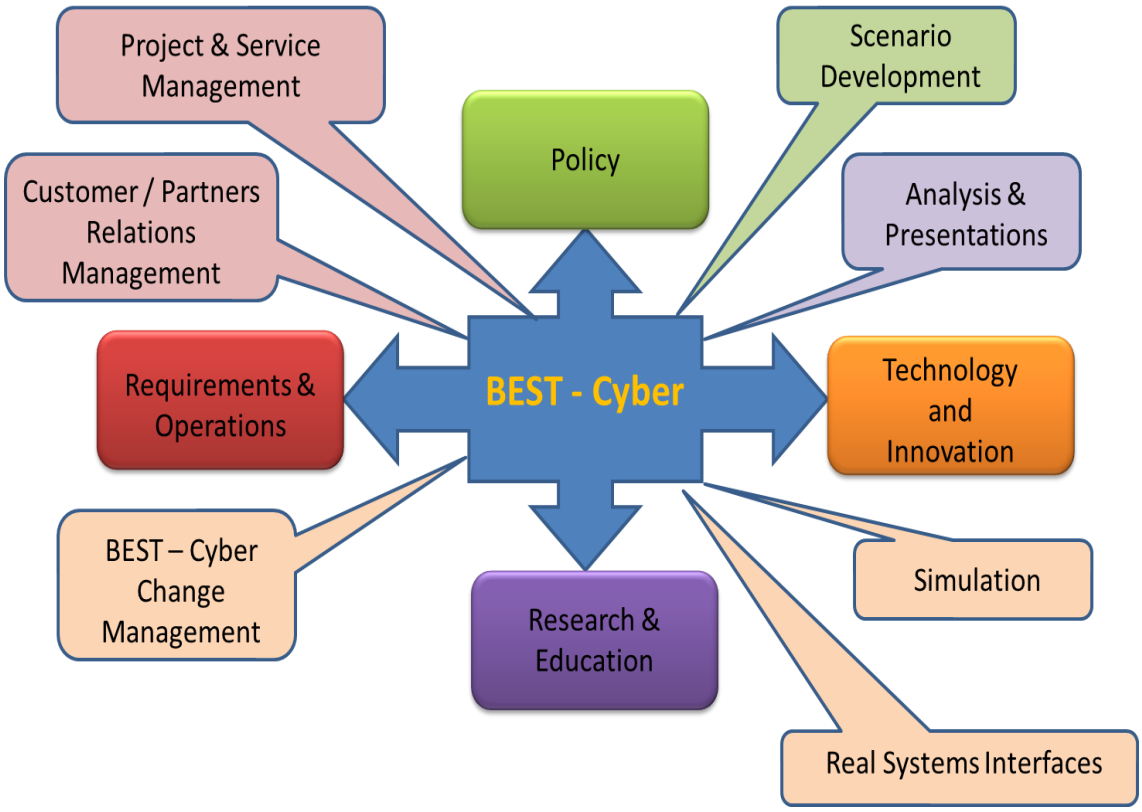
реализиране с фокус върху плана за промяна в началните етапи на стратегическия план.

Средата поддържа работа по метода PEST за анализ на средата, както и по метода SWOT за оценка на алтернативите. Самите алтернативи се създават на базата на архитектурния подход, а избора на подходяща алтернатива става по модела на аналитичен йерархичен процес за вземане на решение (AHP метод).

Стратегическото планиране се извършва по метода на Балансирана система от показатели (BSc) и стратегически инициативи, управлявани като портфолио от проекти. Планирането и управлението на промяната става по метода ADKAR (Awareness, Desire, Knowledge, Ability, Reinforcement).

Средата BEST-Cyber е базирана на опита на Lighthouse (Център за иновации на компанията Локхийд Мартин) в Съфолк, Вирджиния (САЩ) за намиране на решения на сложни мултидисциплинарни проблеми между множество организации – такъв е и проблемът с кибер сигурността. Средата е изградена в ИИКТ-БАН на базата на опита от провеждането на редица учения и проекти по стратегическо планиране с министерства в България, както и по проекти с НАТО (SfP 981149) и ЕС (EUTACOM SEE 2006). Като инфраструктура се използва СЦОСА (център за съвместно обучение, симулации и анализ – JTSAC) с адаптация към проблемите на кибер сигурността по модела за промяна, изложен по-горе. Този модел е ползван през 2004 година за анализ и оптимизация на системата за гражданска защита в България по проект с ПКЗНБАК.

Препоръката е този модел е приложена по Дейност 6 за изработване на визия за организацията по кибер сигурност в България на базата на анализа в Дейност 1, 2, 3, 4 и 5.



Фигура 5. Среда BEST (Basic Environment for Simulation and Training) за подпомагане на трансформацията на организацията за кибер сигурност

Развитие на международното сътрудничество за подобряване на капацитета на организацията за кибер сигурност

Повишаване на зрелостта на системата за кибер сигурност в България и изпълнението на изискванията от членството в НАТО и ЕС при използване на добри практики и солидарна помощ от тези организации е обща препоръка за усъвършенстване на системата за кибер сигурност. Тя може да се реализира чрез конкретни стъпки:

- самооценка и съвместна оценка с НАТО и ЕС на състоянието на системата за кибер сигурност;
- активно използване на решения, утвърдили се в НАТО и ЕС – CERT-EU, NCIRC в сътрудничество с агенции на НАТО и ЕС;
- активна ротация на българи в структури по кибер сигурност на НАТО и ЕС;

- участие в многонационални кибер проекти в НАТО и ЕС – и изследователски и индустриални, включително за развитие на способности за НАТО и ЕС с общо финансиране;
- федериране на наши структури в мрежи на НАТО и ЕС;
- участие в платформата за образование, подготовка, експериментиране и учения по кибер сигурност на ЕС;
- засилено участие в мрежата на ЕС от центрове на компетентност по кибер сигурност и др.

В тази област основното изследване е по Дейност 2.

Осигуряване на прозрачност, отчетност и интегритет на организацията за кибер сигурност

Създаването на роля ГИМ и МКС в ДА със съответните съвети на ГИМ по нива (използване на сега съществуващите Съвет за е-Управление и Съвет по киберсигурност) има за цел да се институционализира процеса на планиране на ИТ ресурсите и тези за кибер сигурност. Така установеният процес е основа за създаване на механизъм за прозрачност, отчетност и постигане на интегритет чрез демократичен контрол. Институционализацията включва прозрачен процес на стратегическо планиране, оперативно управление, ключови индикатори за ефективност и ефикасност, за кибер устойчивост, на базата на които да се оценява работата в тази област. Отвореността на тези процеси създава и възможности на гражданите, НПО да са ангажирани, а участието и приносът на индустрията и академичния сектор да се оптимизира.

ИДЕНТИФИЦИРАНЕ НА КРИТИЧНИ ТОЧКИ И ПЕРСПЕКТИВИ. ПРЕДСТАВЯНЕ НА ЯСНА ВИЗИЯ ЗА ПОДОБРЯВАНЕ НА КИБЕР СИГУРНОСТТА НА ПУБЛИЧНИЯ СЕКТОР В БЪЛГАРИЯ

СИСТЕМА ОТ МЕРКИ ЗА ПОВИШАВАНЕ КАПАЦИТЕТА НА СТРУКТУРИ И ЗВЕНА В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ НА БЪЛГАРИЯ ПО ВЪПРОСИ СВЪРЗАНИ С КИБЕР СИГУРНОСТТА

Този раздел няма за цел да предложи цялостна програма за развитие на способности за кибер сигурност (или кибер отбрана) за организациите от публичния сектор. Ще се ограничим в предлагането на групи от конкретни мерки, които са от т.нар. ниво на „бързи успехи“ и се справят с някои ясно идентифицирани слабости (на организациите). Ще подчертаем, че мерки от този тип, макар и в случая „животоспасяващи“ по характера си, следва да бъдат разглеждани задължително в **контекста на визията и политиките** за развитие на организацията, както и на план за постигането им, за да не останат само „епизодични“ инициативи.

Предлагаме мерките да бъдат систематизирани и групирани според **нивото на амбиция** и **нивото на рискове (заплахите)**, с които си поставяме за цел да се справим.

Ще отбележим, че **управлението на рисковете** (от оперативен характер) зависи от:

- възможностите и средствата за **идентифициране и оценката (aware)** на слабости, заплахи и възможни начини и източници на въздействие (вектори на заплахите);
- възможностите и средствата да се **забелязват (detect)** своевременно инциденти или зловредни въздействия, както и методи и средства за **оценка на въздействие им (impact assessment)**, при това в динамика;
- способности (човешки, организационни, технически) за реакция и справяне с инцидентите **(react/respond)**, както и за възстановяване **(recover)**.

Според посочените два аспекта (ниво на амбиция, и видове рискове/заплахи) в Националната стратегия за киберсигурност (2016г.) са определени и трите основни **нива на зрялост** в кибер пространството на организации, държава и общество, определени в Стратегията като **информационна сигурност, кибер сигурност и кибер устойчивост.** Ще е

използваме тези нива за структуриране на приоритетните мерки, които адресират ясно изразени рискове (част от тях проявени и на практика)[101]:

❖ Базово **ниво на зрялост („оцеляване“) - „информационна сигурност“** – рискове от типа *„известни известни“* - защита и предпазване на информационните активи и комуникационна инфраструктура от известни слабости, заплахи и пробиви, свързани с основната „триада“ на информационната сигурност (или рискове и мерки, свързани с постигане на „кибер хигиената“).

➢ **Мерки** (повечето са в духа на очакваните по Наредбата за прилагане на Закона за киберсигурност/Директивата за МИС, но препоръчваме паралелно и с приоритет някои базови мерки с непосредствен бърз ефект, включително и **„запушване“ на критични слабости**):

- стартиране на кампания „кибер хигиена“ в публичната администрация - инвентаризация на основните информационни и технически ресурси (спрямо установени изисквания за киберсигурност) - сканиране на системите и мрежи със специализирани софтуери (вкл. и open-source) - **отстраняване на основни критични уязвимости** (от типа Top 10 по OWASP, за уеб системи; основните изисквания на ISO 2700x)
- преглед за лицензирани и поддържани от производителите софтуерни и хардуерни системи, „изключване“ на неподдържаните
- сканиране на сигурността и достъпността на уеб сайтовете и уеб-базирани системи и услуги на правителството и държавната администрация (вкл. на интернет свързани системи), възможен аутсорсинг, консултации с бизнес и академични организации
- инсталиране на основни IDS/IPS (Intrusion Detection System / Intrusion Prevention System)
- въвеждане (осъвременяване) на основни процедури за действия при кибер инциденти (SOP) – тестване и „оживяване“ с учения/упражнения
- интензифициране на кампания за публична информираност за разкрити киберпрестъпления (и кибер инциденти с голям мащаб)
- развитие на човешки капацитет – групи за бързо реагиране (възможно е смесени с индустрия, академия)

[101] Национална стратегия за киберсигурност „Киберустойчива България 2020“ , 2016г. – www.cyberBG.eu

- преглед на възможностите за бърз трансфер към публичния сектор на добрите практики и доказани модели от индустрията, пилотно внедряване на съвременни инструменти и платформи (работещо „демо“) по инициатива и с ресурси на индустрията (основа за публично-частно партньорство „в действие“)

❖ Второ ниво на зрялост „кибер сигурност“ („уравляемо“) - рискове, свързани с комплексни заплахи („неизвестни известни“), включително и „скрити“ въздействия, зловредни действия от типа APT (Advanced Persistent Threats), както и кампании срещу репутацията на организации и личности, дезинформация, пробиви в КИН в особено големи мащаби. Действия:

- разширена „инвентаризация“ - системно прилагане на принципа КИН за всички активи в дигиталната екосистема - *информация, технологии, хора, съоръжения (и „външни зависимости“)*
- внедряване на интегрирани системи (или поне една система от типа (advanced)SIEM, с възможност за комбиниране на данни от различни канали и агрегиране на анализа за формиране на „кибер картина“ (на ниво организация)
- разширяване на стандартните оперативни процедури (SOP) – от действия при кибер инциденти към действия при „инциденти от хибриден характер“
- изграждане на Център за оперативна сигурност (SOC – Security Operations Center) - разширение на екипите за реагиране при кибер инциденти (възможен аутсорсинг на дейността, при въведени изисквания и критерии за „доверие“)
- определяне на максимални срокове за възстановяване на нормалното функциониране на системите.

❖ Зряло ниво **„кибер устойчивост“** („дефинирано“) – готовност за справяне с „неизвестни неизвестни“ - неочаквани (нови) заплахи в киберпространството, динамично променящи се рискове и комплексни въздействия с непредсказуеми последствия, които изискват гъвкавост и устойчивост на системите, организацията и процесите, и съответни стандарти при разработването и внедряването им.

- **Мерки** (критични, които би следвало да се **предприемат сега**, тъй като са свързани с бъдещи системи и способности, по-детайлен списък е набелязан в Стратегията и Закона КС):
  - въвеждане на принципите и изискванията за устойчивост към развитието на системите и при дизайна на нови такива, прилагане на модела „дизайн за сигурност“
  - въвеждане на единна система и унифицирани критерии за оценка на кибер рисковете по цялата верига на оперативната

обвързаност, и преглед на цялостната архитектура и изисквания за оперативна съвместимост на системите и услугите от гледна точка на тяхната кибер защита и устойчивост

- непрекъснато подобряване на изискванията за осигуряване на еднакво ниво на кибер сигурност и устойчивост при декларираното равнопоставено използване в системата на електронното управление на „класически“, „виртуализирани“, „облачни“, „мобилни“ и други нови технологии

Човешки капацитет

Относно идентифицираните огромни дефицити по отношение на наличие и квалификация на кадри и специалисти по киберсигурност (за нуждите на публичната администрация) – в други раздели на доклада са предложени и разработени подробни мерки и план за развитие. Тук ще подчертаем критичната важност на базови ресурси за стартиране на неотложните мерки, както и препоръчителното използване на основни механизми за публично-частно партньорство и взаимодействие с академичните ресурси и индустрията.

Важно е и бързо да се постигне съгласие за основната рамка, и да стартира „Национална програма за обучение и сертификация по кибер сигурност в публичната администрация“. Провежданите досега и планирани учения (общи с НАТО и ЕС, както и национални, секторни) са изключително полезни, но те могат само да подпомогнат консолидирането на фрагментирания капацитет. За изграждането на капацитет е необходима системна учебна програма, която включва интензивни практически курсове (както технически, така и за управление на действията), идентифициране и дефиниране на профили за техническите и ръководни кадри. Съществен стимул е стандартизирането на обучението и сертификацията на специалистите по световно признати стандарти и схеми за компетентности.

За развитието на модели на взаимодействие и изграждане на поделен капацитет е важно изучаването и прилагането на опита в НАТО, ЕС (и напредналите държави – Германия, Франция, Нидерландия, Великобритания), както и на САЩ, Израел и други световни лидери. Практически за изграждането на общ и работещ капацитет ще спомогнат различни форми за изграждане на „кибер резерв“ – по модела на други държави от НАТО и ЕС, например Естония, както и заложената в Закона за КС механизъм в Министерство на отбраната.

Механизъм за взаимодействие и развитие на капацитет предоставя и участието на България в Европейското „договорно“ публично-частно партньорство ECSO (European Cyber Security Organization)[102] .

Кибер хигиена – пилотно изследване

В рамките на настоящото изследване бе извършен и пилотен преглед на уеб сайтовете (и системи) на публичната администрация (правителство и ведомства, както и местна администрация – общини, области). Целта е да се придобие ясна представа за състоянието на известните уязвимости (представени като „критични“ по-горе в група 1) – „известни известни“, т.е. публично известни и видими, използваеми и без високо ниво на компетентност). За целта беше използвано разработеното в Лаборатория по киберсигурност в София Тех Парк, по методика на ЕСИ Център Източна Европа, техническо средство „Кибер Карта на България“[103]. Изследвана е само публично достъпната информация (т.е. без използване на деструктивни или проактивни средства), която е агрегирана и анононимизирана в справката.

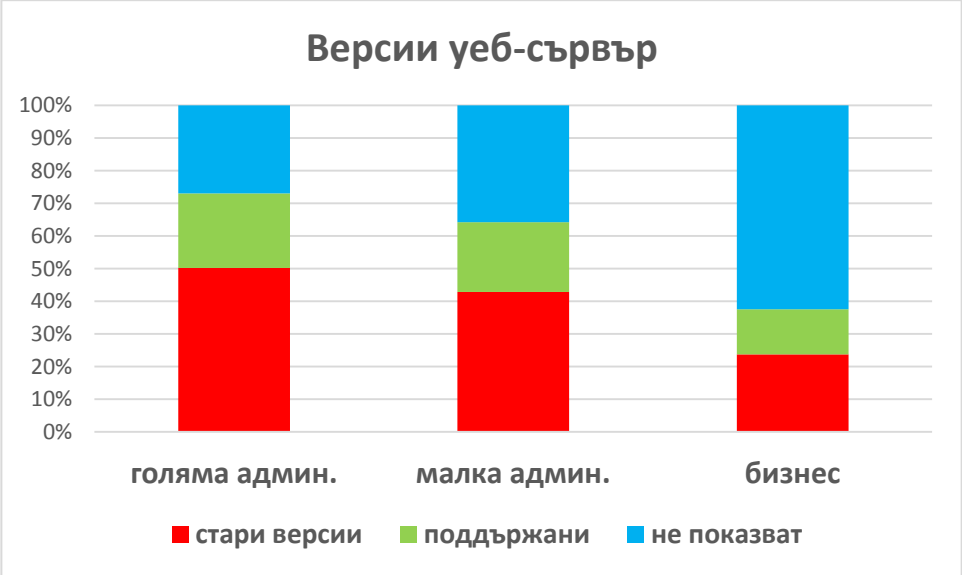
Справката е направена върху следните групи изследвани сървъри, поддържащи уеб-интерфейс (всички са на домейни, регистрирани в **„.bg”**):

- Група **„малка админ.“** – интернет сайтове (сървъри) на централна администрация (министерства, централни ведомства) – 28 бр.
- Група **„голяма админ.“** – разширена група, добавени са и сайтове на местна администрация – общо 197 бр.
- Група **„бизнес“** – случайна извадка от бизнес организации (индустрия, НПО) – 202 бр.

Представяме обобщените резултатите в **два вида сканирания**:

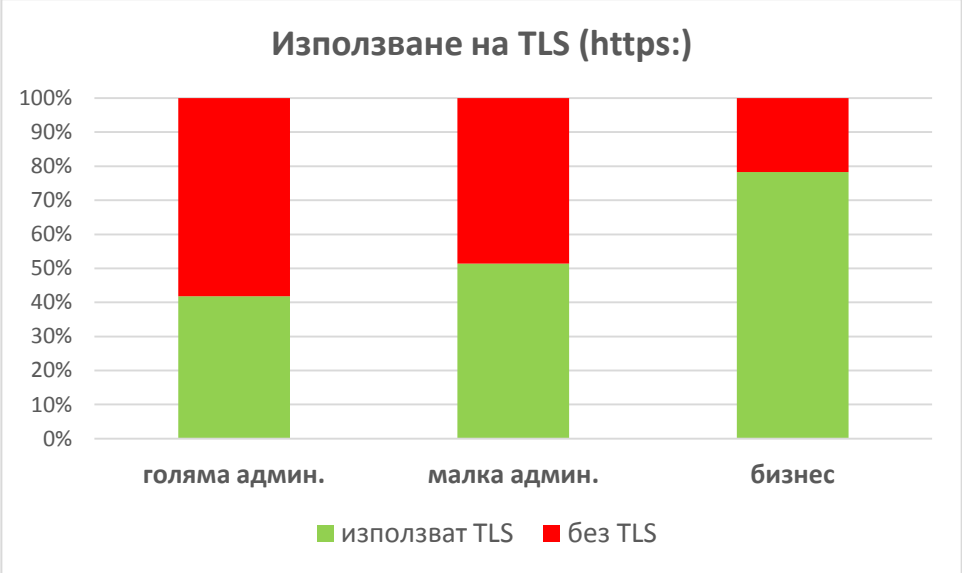
Тест 1: Версии на използваните уеб-сървъри (Фигура 6) с обобщена оценка за тяхната уязвимост – поддържани версии (по официална информация Microsoft-IIS, Apache, nginx и др.), стари (неподдържани), „не показват“ – без публична индикация (това се приема за „добра“ хигиена, т.е. те са „добри“)

[102] https://ecs-org.eu/
[103] http://sofiatech.bg/about/tin/лабораторен-комплекс/cybersecurity/



Фигура 6. Версии на уеб-сървъри (обобщени)

Тест 2: Използване на TLS (т.е. поддържане на https:), на Фигура 7. Не са отчетени версиите на TLS/SSL (от които също има уязвими).



Фигура 7. Използване на защитена връзка https: (TLS)

Общ извод от представените обобщени резултати е, че заплахата от елементарни атаки, използващи публично известни уязвимости на стари, неподдържани версии на уеб-сървърите, както и на незащитена връзка към

сайтовете на публичната администрация е голяма. Наблюдава се известно повишаване на нивото в централната администрация, но сравнението с бизнес сайтовете е очевидно (макар и нивото на използване на неподдържани софтуери е също тревожно).

Препоръчителните мерки не изискват някакви особени технически и административни умения, и са предмет на бързи и отговорни действия. Представената картина е обобщена, и е с цел да покаже сериозността на заплахата.

Използваните средства и методи („Кибер карта България“ на Лабораторията по киберсигурност в СТП) позволяват по-детайлни анализи, допълнителни параметри, уязвимости, мерки, както и последващи тестове (известни като pen-tests). Възможни са и анализи на различни групи, както и от посочени от потребителя групи домейни и сайтове, както и допълнителен анализ за характерни (хронични) слабости за определена група или клъстер, и препоръчвани на съответни комплекс от мерки и програми за подобрение.

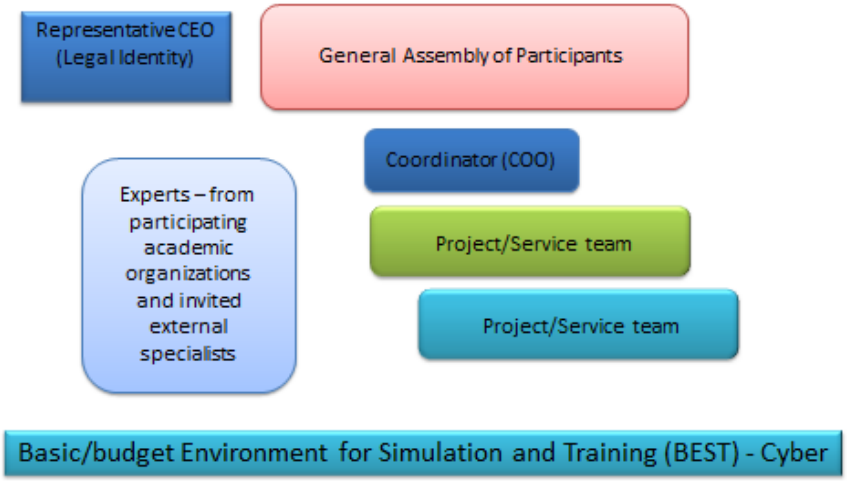
Перспективи пред организацията за киберсигурност в публичния сектор

Започвайки със Съвета по кибер сигурност и неговия секретариат и надолу в структурите на ДА, индустрията, академичния сектор е необходимо да се развие мрежа от минимално необходимите, но с достатъчен капацитет звена за гарантиране на кибер устойчивост.

Освен Съвета по кибер сигурност на най-високо ниво е ключова ролята на Национален координатор по кибер сигурност.

В академичен план е важно да се създаде Национален координационен център за изследвания и обучение по кибер сигурност в съответствие с регламента на ЕС. Това може да бъде съчетано със създаване на Национална научна програма за „Ефективност, ефикасност и кибер устойчивост на ИТ системи /организации“.

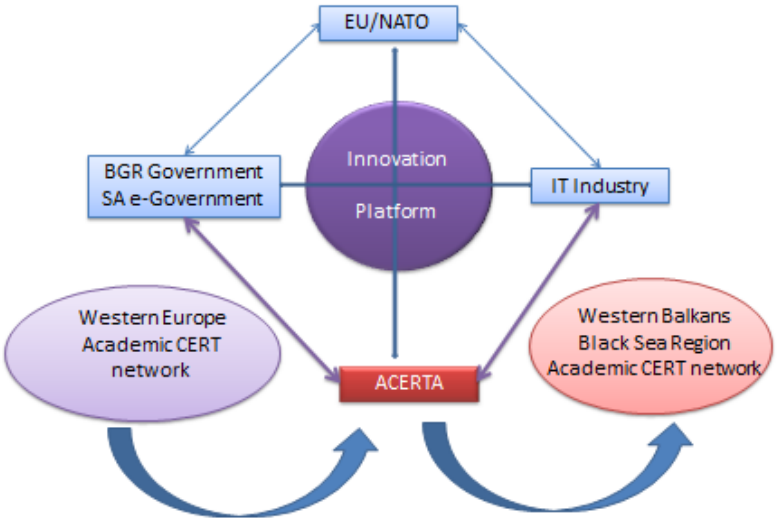
В този смисъл общата архитектура на академична кибер организация (Фигура 8) определя основните компоненти – Общо събрание и Представител, заедно с Координатор и множество екипи по проекти или услуги, които са формирани от експерти на всички академични звена, участващи в организацията (представени в общото събрание). Основа е инфраструктурата – кибер полигон, базова среда за симулации и обучение.



Фигура 8. Академична кибер организация (ACRETA)

Взаимодействие между центрове за научни и приложни изследвания, водещи софтуерни и ИКТ фирми и публичния сектор в България по въпроси на кибер сигурността

Партньорството между ДА, индустрия и академичен сектор на базата на компетентности е критичен фактор за висока степен на кибер устойчивост.

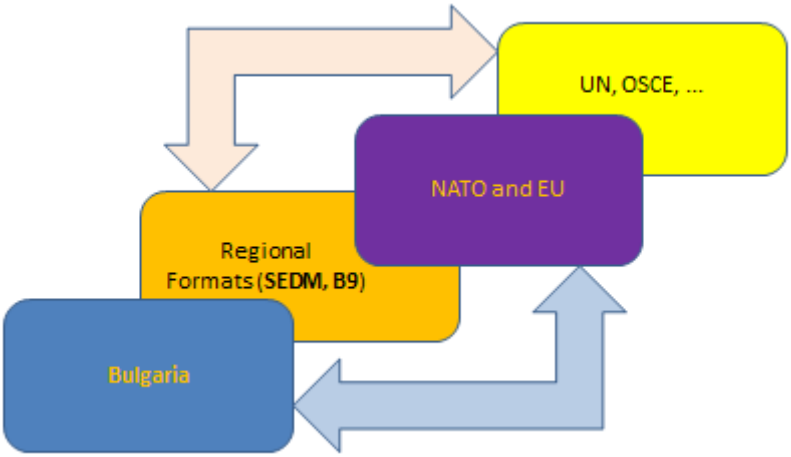


Фигура 9. Модел за (хоризонтално) взаимодействие между академичната кибер организация (ACERTA), администрацията и ИТ индустрията в контекста на ЕС и НАТО

Хоризонталното взаимодействие между ДА, академична организация (ACERTA) и индустрията в контекста на рамката, определена и с наше участие в НАТО и ЕС, е отразено на Фигура 9. Именно академичната организация позволява в най-голяма степен да се организира трансфериране на знание и добри практики от Западна Европа към Западните Балкани и Черноморския регион през ACERTA.

Стимулиране на международно сътрудничество във връзка с приоритетно развитие на цифровата икономика и намирането на иновативни решения за дейността на държавата и публичния сектор

Вертикалното взаимодействие между организацията за кибер сигурност в България със структурите в НАТО и ЕС от една страна (разглеждана за нас като вътрешно съюзна) и с глобалните / евразийски структури, а от там и в регионален план – Източна Европа (Западни Балкани, Черноморие) е показано на Фигура 10.



Фигура 10. Модел за (вертикално) взаимодействие между националните кибер звена, ЕС и НАТО в контекста на глобални (пан-европейски) и регионални формати за сигурност в Източна Европа

ВИЗИЯ ЗА ПОДОБРЯВАНЕ НА КИБЕРСИГУРНОСТТА В ПУБЛИЧНИЯ СЕКТОР

Развитието на визията, представена в трета глава, стъпва на оценка на текущото състояние и отговор на следните въпроси:

1) Какви са основните теми за иницииране на национална програма за изследване по кибер сигурност?
   - Модели за ръководство и управление на ИТ системи / организации;
   - Управление на ресурсите за кибер сигурност и управление на риска;
   - Използване на ИИ в системите за кибер сигурност и в частност оценка и предлагане на решения по кибер сигурността;
   - Модели за разработка на сигурен софтуер и неговото сертифициране;
   - Сензори за следене на състоянието на ИТ системите;
   - Изобразяване на „кибер ситуацията“ – обща картина на кибер пространството;
   - Сигурно споделяне на информация по обща картина на кибер пространството;
   - Интеграция на технологии за демонстрации, експериментиране и учения по кибер сигурност (кибер полигони).
2) Какви са основните въпроси за една концепция за развитие на човешкия потенциал в сферата на кибер сигурността?
3) Развитие на програма за обучение на експерти по кибер сигурност:
   - Модел за сертификация на персонала;
   - Модел за развитие и задържане на персонала, вкл. в доброволни структури (кибер резерв);
   - Модел на заплащане на специалистите по кибер сигурност.
4) Кои са ключовите въпроси за създаване на модел за взаимодействие между администрация, бизнес и академичен сектор в оперативното поддържане на електронното управление?
   - Институционализиране на ГИМ и Главен мениджър по кибер сигурност;
   - Създаване на консултативни съвети и съвети за вземане на решения по кибер сигурност;
   - Създаване на мрежа за обмен на информация и за ротиране на експерти.

5) Какви са важните инструменти на международно сътрудничество по кибер сигурност, основно в ЕС и НАТО, но и в региона?
   - Участие в многонационални проекти на НАТО и използване на VNC в кибер сигурността;
   - Институционализиране на Кибер координационен център за изследвания и технологии по регламента на ЕС, участие в Центъра за компетентност на ЕС;
   - Създаване на мрежа от центрове на компетентност в България за включване чрез Х2020 / Х-Е в мрежата на ЕС.

Отговори на тези въпроси се консултираха по време на кръглата маса от 15.11.2018 г. за осигуряване на идеи по развитие на алтернативи за организацията за кибер сигурност в България, които са дефинирани, оценени и използвани като основа за предложение на Визия по организиране на кибер сигурността у нас (трета глава от този документ).

РЕЗУЛТАТИ ОТ ОНЛАЙН ИЗСЛЕДВАНЕТО С ЕКСПЕРТИ ПО КИБЕР СИГУРНОСТ

Направено бе експертно изследване, имащо за цел да се придобие и обобщи максимално широк кръг информация по въпроси, свързани с предизвикателствата пред гарантиране на кибер сигурността в България.

Резултатите от изследването следва да подпомогнат процеса на формулиране на изводи и препоръки за усъвършенстване на нормативната база, капацитета на институциите, набирането, развитието и задържането на кадрите и използване на нови технологии от блокчейн до изкуствен интелект и не на последно място финансирането на тази сфера, нивото на сътрудничество в страната и в рамките на НАТО и ЕС, степента на прозрачност и отчетност за реален демократичен контрол на системата.

Поставените в изследването въпроси касаят трите сектора – държавна администрация, академичен сектор и бизнес сектор – като участници в оперативната поддръжка на електронното управление в България, чиято консолидираност е изискване за постигане на кибер устойчива България.

За целта бе създаден въпросник, който бе изпратен до **369 държавни администрации**, **121 академични организации** и **95 бизнес организации**. Въпросникът няма задължителен характер за попълване. Въпреки това към

момента на съставянето на този доклад активност са проявили 92 участника от трите сектора (Фигура 11).

Фигура 11. Описание на извадката

Въпросникът съдържа 50 въпроса, които са обединени в 5 основни групи (Фигура 12), касаещи:

1) състояние и развитие на човешкия потенциал;
2) текущо състояние на оборудването и ресурсите;
3) управление и политики;
4) взаимодействие между трите основни сектора: държава, академия и индустрия;
5) иновативни технологии.

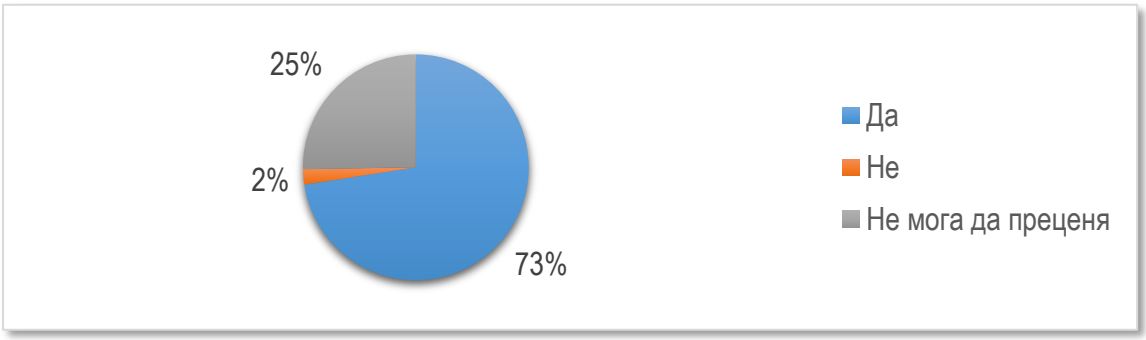
Фигура 12. Групи въпроси, включени в онлайн въпросника

Заеманите длъжности на анкетираните могат да се обособят в три основни групи: ръководна, експертна и изследователска като 85% от тях имат **ниво на експертиза** по отношение на въпросите, свързани с кибер сигурността, достатъчно за нуждите на организация, добро и високо. Те смятат, че само 15% от персонала, отговарящ за кибер сигурността, има ниско ниво на експертиза в тази област.

Следва представяне на избрани въпроси от проучването, които имат по-категорично изразени отговори.

ГРУПА 1: Състояние и развитие на човешкия ресурс

Смятате ли, че са необходими промяна и развитие в набирането, обучението, подготовката на кадрите, задържането им и извличането на поуки от практиката в областта на кибер сигурността в България?



В огромното си мнозинство експертите смятат, че са необходими промени в набирането, обучението, подготовката на кадрите, задържането им и извличането на поуки от практиката в областта на кибер сигурността. Конкретните предложения:

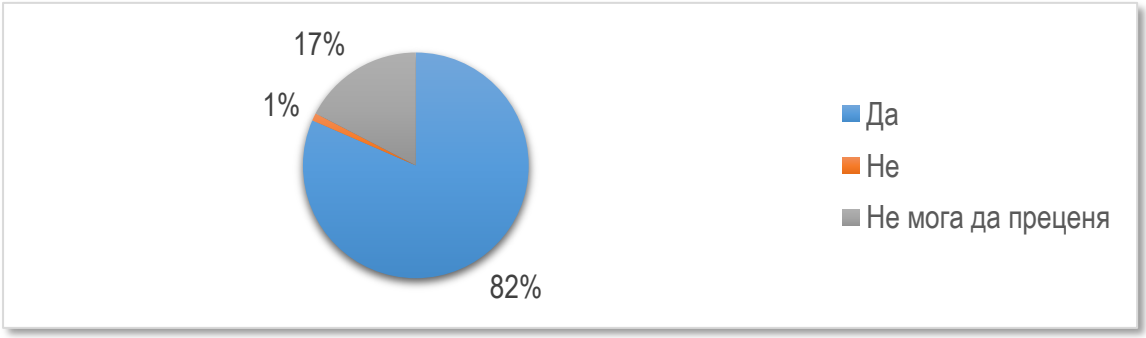
- Трябва да завършват сертификации за това, а и да има такава специалност в техническите висши учебни заведения;
- Кадрите трябва да се набират според конкретната задача, а не да бъдат „швейцарски ножчета“;
- Модно е да се преподава киберсигурност от хора, които никога не са работили в тази област. Няма ясно дефинирани способности, които се изграждат. Обучението е неосигурено с технологии и платформи. Лекциите, които се заимстват от западни и източни източници не са осигурени с възможност за практическа работа и проверка. Инвестициите меко казано не постигат своята цел, което говори за неправилното им насочване;
- Създаване на специализирани звена за обучение и „на място“;

- Фокус върху обучението и задържането на кадрите.

Освен това, в поредица от въпроси експертите бяха помолени да посочат дали са необходими промени в нормативната база, стратегиите, концепциите, доктрините и организацията на системата за кибер сигурност. В повечето случаи малко над половината от изследваните лица посочват, че такива промени са необходими. Освен това те дават конкретни предложения какво да се промени. Ето някои примери:

- Процедури за взаимодействие между организации;
- Ясни правила за публично-частно партньорство;
- Доктринални въпроси за взаимодействие в рамките на НАТО и ЕС;
- Процедури за действие при различни сценарии. Процедура за преглед и актуализация на стратегията;
- Трябва да има ясно определени лица, екипи и отговорности. Да им се поставят цели. При непостигане на целите - да има промени в екипите. По този начин за сравнително кратък период ще формират работещи екипи и държавната администрация ще се освободи от неработещи структури и псевдо експерти.

Смятате ли, че е необходимо да се отдели специално внимание на ролята на човешкия фактор в областта на кибер сигурността в България?



Отново огромното мнозинство от експертите подчертават ключовата роля на човешкия фактор в кибер сигурността. Показателно е, че само 1 човек е посочил, че не е необходимо да се съсредоточи вниманието върху ролята на хората за предотвратяване на кибер инциденти, повишаване на общата осведоменост и адекватна реакция в случай на заплаха. Препоръки:

- Дългосрочна стратегия за осигуряване на необходимия човешки потенциал;
- Подбор, обучение, сертификация, ротация между публична администрация, индустрия, академичен сектор, НАТО и ЕС, проверка за лоялност;

- Важно е да се оценяват поведението, нагласите и настроенията на потребителите в кибер пространството с цел предвиждане на техните действия и очаквания;
- Технологиите за кибер сигурност са с много къс жизнен цикъл. Могат да се придобиват сравнително бързо и лесно. Трудното е да се изгради и развива човешкият потенциал. Трябва да се определят какви специалисти са ни нужни, за да се гарантира „здравословния излишък от специалисти във всяка една определена област на кибер сигурността“;
- Човешкият фактор е най-рисков; той е част от системата; основна уязвимост дори и при най-защитените системи;
- Като най-слабо звено във всяка организация изисква специално внимание най-вече по отношение на обучение с цел повишаване на компетенциите на служителите и спазване на добри практики в областта на киберсигурността.

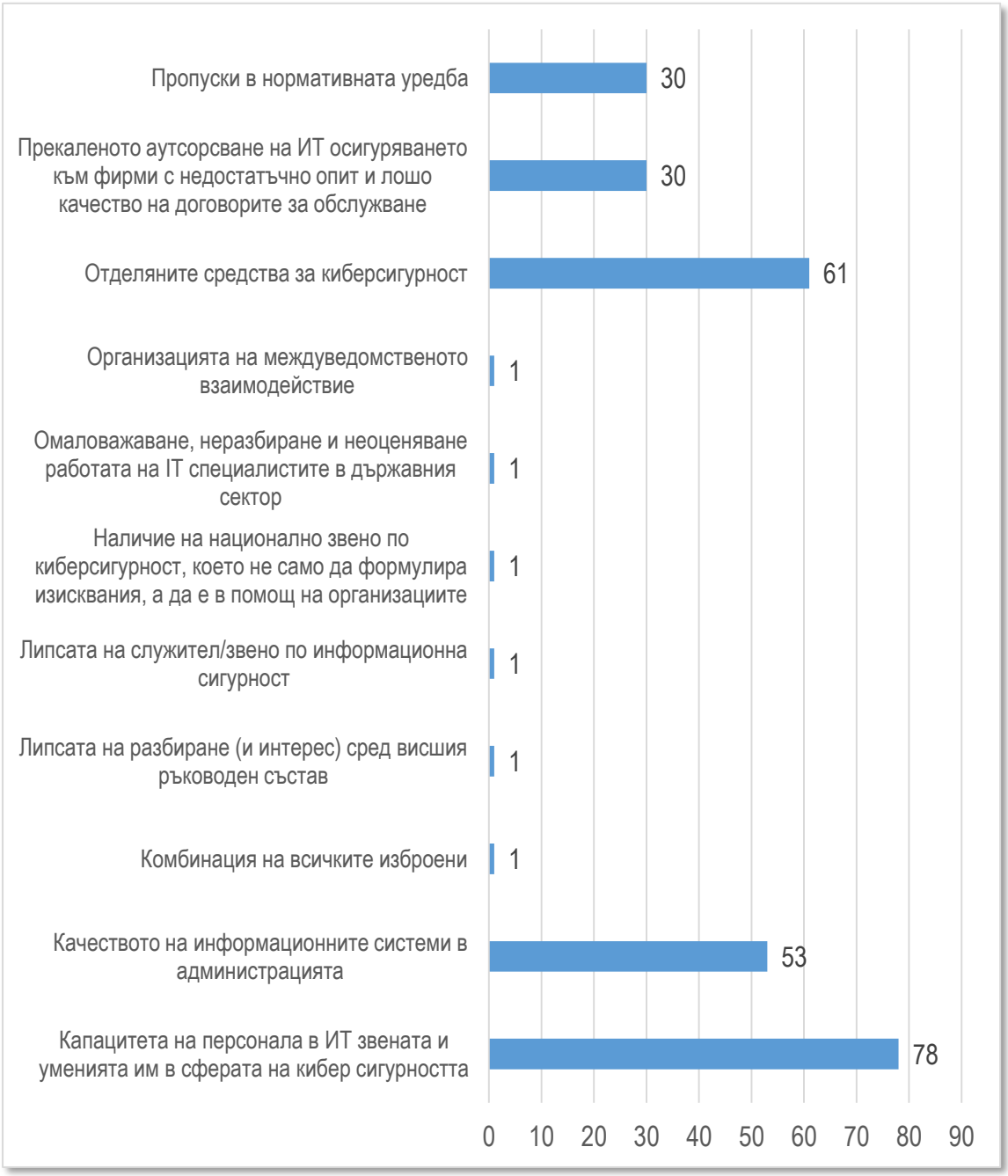
ГРУПА 2: Текущо състояние на оборудването и ресурсите

Кога за последно е проведено обучение по кибер сигурност във вашата организация?

Проучването показва, че в голяма част от случаите (55%) такива обучения не са правени. Под **Друг отговор** (14%) се включва:

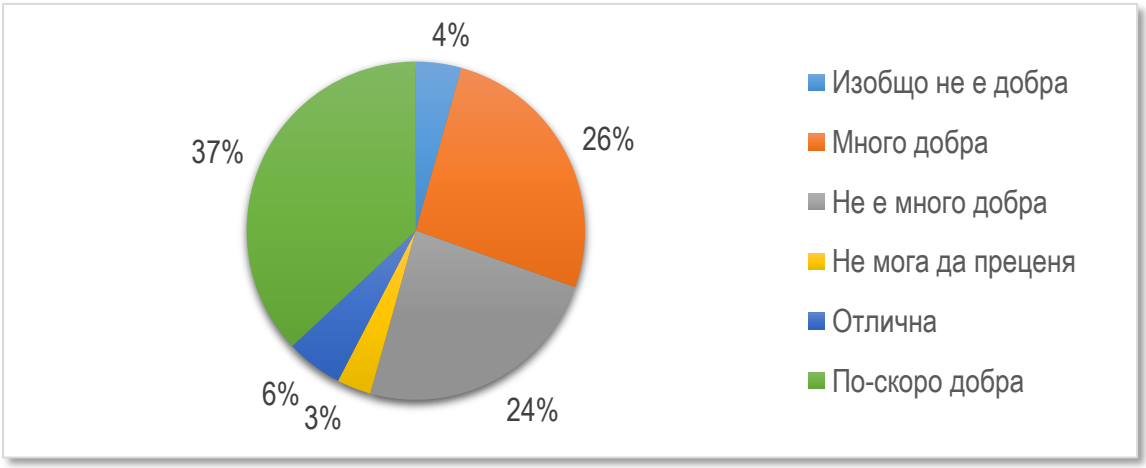
- ✓ Преди 3 години
- ✓ През последната година
- ✓ През последните 6 месеца
- ✓ Провежда се в момента.
- ✓ Такива обучения са провеждани само на администраторите на информационни системи.

Моля, посочете и обосновете трите най-важни проблема в момента в областта на кибер сигурността в България



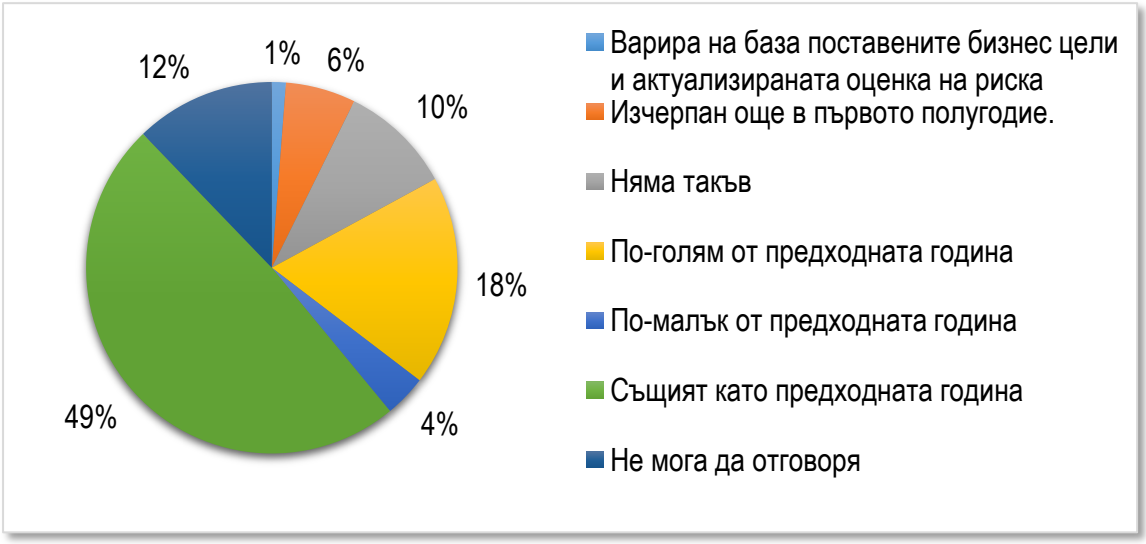
Респондентите са имали възможност да посочат всеки верен отговор и затова, те не се сумират до 100%. Като най-сериозни проблеми на кибер сигурността експертите определят недостатъчния капацитет (знания и умения) на ИТ персонала. На следващо място с почти еднакъв дял са посочени качеството на информационните системи в администрацията и недостатъчните средства, които се отделят за кибер сигурност. На трето място са посочени известни пропуски в нормативната база и практиката на прекалено аутсорсване на ИТ услуги, в някои случаи водещо до лошо качество. Единични експерти смятат, че липсва разбиране сред ръководния състав, че проблемът се омаловажава или, че се работи на парче.

Моля, посочете как оценявате защитата/сигурността на системите на Вашата организация



Данните показват твърде голямо разнообразие в отговорите. Повече от половината експерти дават оценки „“По-скоро добра“ – 37%, „Много добра“ – 26%. Около една четвърт смятат, че защитата/сигурността на системите на тяхната организация е „Не много добра“. Единични експерти дават оценки в като „Отлична“ и „Изобщо не е добра“.

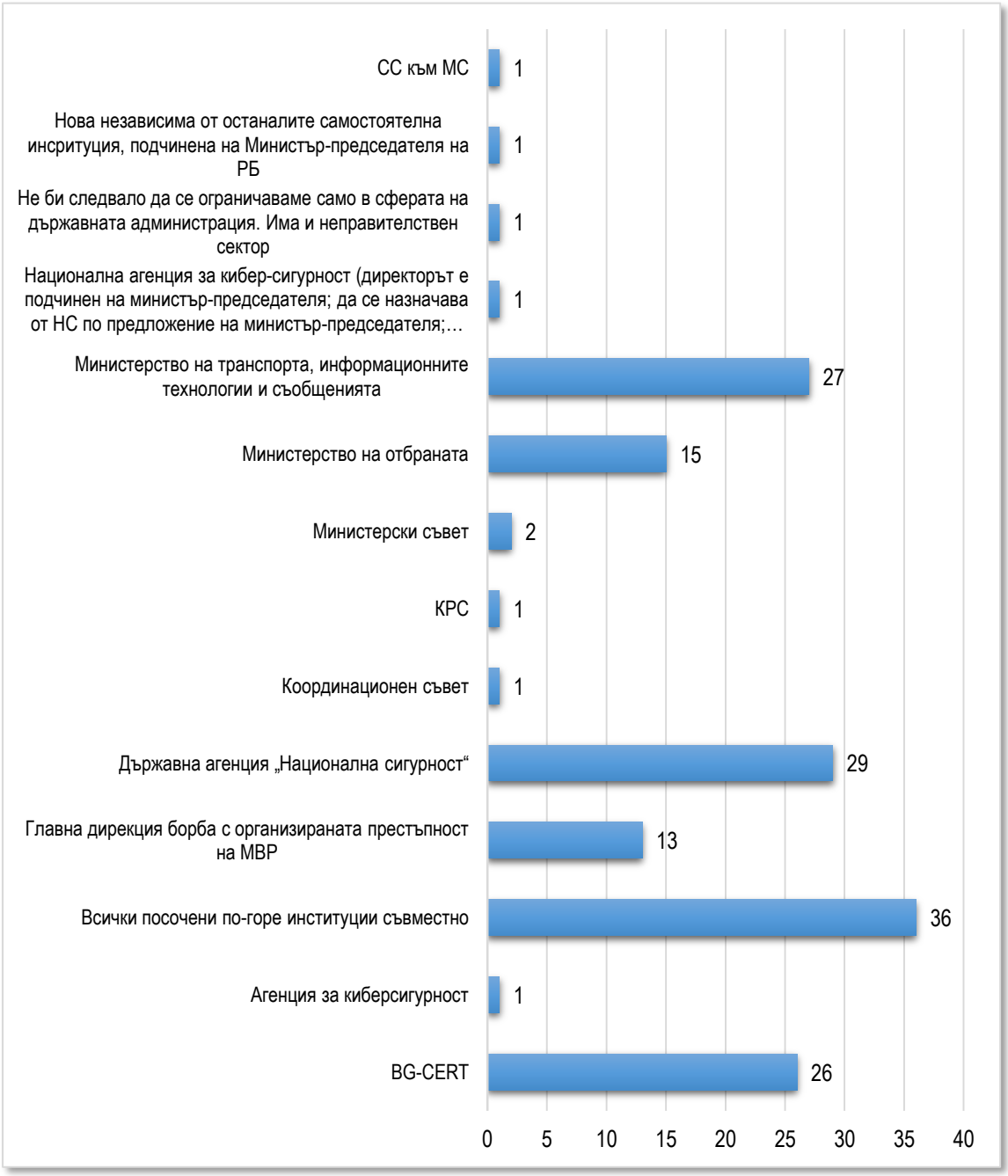
Годишният бюджет за 2018 г., предназначен за поддържане на сигурна и защитена информационна и комуникационна инфраструктура, е:



В 49% от случаите бюджетът за текущата година, предназначен за поддържане на сигурна и защитена информационна и комуникационна инфраструктура е същият като предходната година. В 10% от случаите такъв бюджет изобщо не се предвижда дори и за поддръжка на съществуващите системи.

ГРУПА 3: Управление и политики

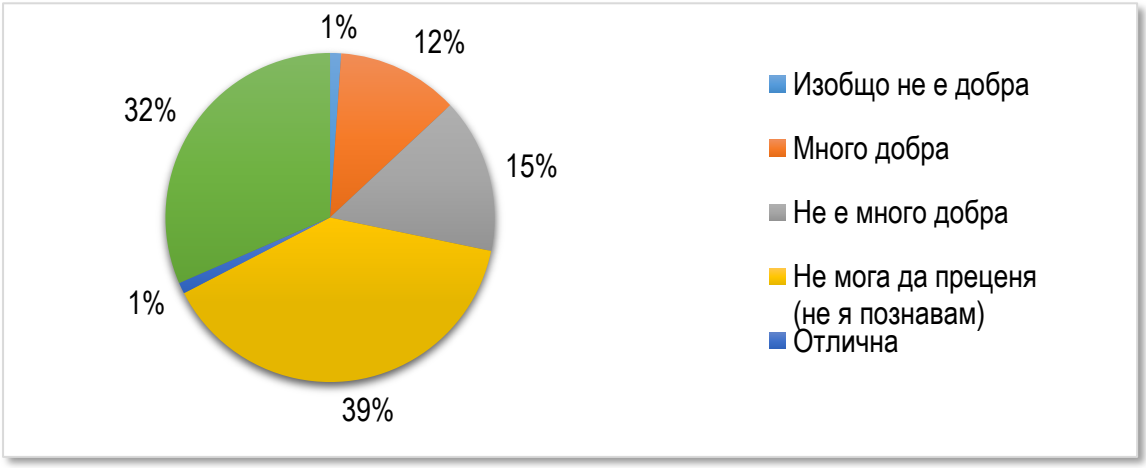
Коя институция/и в държавата следва да има водеща роля по въпросите на кибер сигурността според Вас?



Респондентите са имали възможност да посочат всеки верен отговор. Мнението им е категорично, че всички държавни институции следва да работят заедно и в синхрон, за да се гарантира кибер сигурността. Необходим е интегриран подход за работа, като се отчита ролята на индустрията, науката и управлението. На следващо място с почти еднакъв дял отговори са посочени BG-CERT, ДАНС и Министерство на транспорта, информационните технологии и съобщенията. Сравнително висок дял от експертите посочват и МО като институция, която трябва да има водеща роля в кибер отбраната.

Данните показват, че експертите не смятат за необходимо да се създават нови държавни структури, които да отговарят за кибер сигурността. Вместо това те препоръчат да се подобри взаимодействието и сътрудничеството между съществуващите.

Моля, посочете и обосновете Вашата оценка за действащата Стратегия за кибер сигурност „Кибер устойчива България 2020“



Данните, представени на тази графика будят тревога, защото твърде голям дял от участниците в изследването, които са експерти в киберсигурността (39%), посочват, че не познават Стратегията за кибер сигурност „Кибер устойчива България 2020“.

Под половината експерти дават оценки „По-скоро добра“ – 32%, „Много добра“ – 12%. Единични експерти дават оценки в като „Отлична“ и „Изобщо не е добра“. Заслужава внимание и фактът, че близо 15% оценяват Стратегията като „не много добра“. Очевидно са необходими действия за запознаване на експертната общност със Стратегията за кибер сигурност „Кибер устойчива България 2020“ и евентуална нейна актуализация.

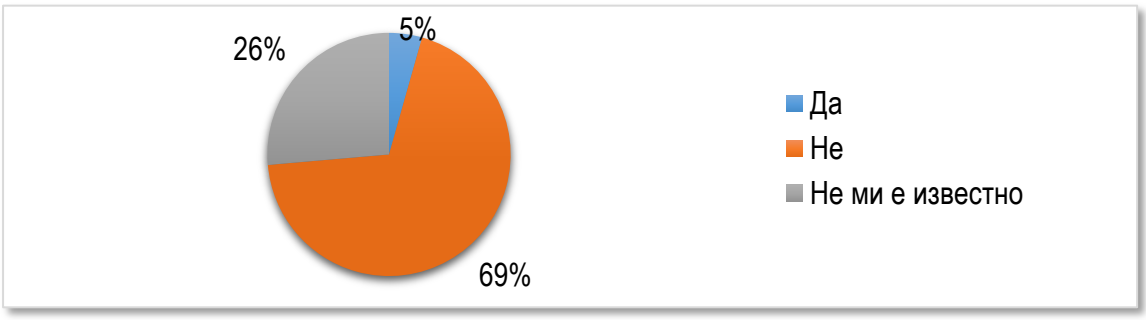
ГРУПА 4: Взаимодействие между трите основни сектора: държава, академия и индустрия.

Моля, посочете и обосновете кои са според Вас трите най-важни области, които изискват научни изследвания в областта на кибер сигурността

Респондентите са имали възможност да посочат всеки верен отговор. С най-голям дял отговори, като област, в която има потребност от допълнителни изследвания, е посочена ролята на човешкия фактор в кибер сигурността. Определено експертите смятат, че е необходим интегриран подход към кибер сигурността, който да включа човека в центъра на системата, новите технологии, софтуерни иновации, организационни и нормативни промени и др. Наред с това като важни изследователски области се определят защитата от вируси и зловреден софтуер, ефективното и ефикасно управление на информационните ресурси и изграждането на облачни инфраструктури. Третата група области, които се нуждаят от допълнителни научни изследвания, са изкуственият интелект, проектирането на системи и системите за персонална идентификация. Сравнително по-нисък е интересът към блокчейн технологиите, вероятно поради тяхната по-слаба популярност.

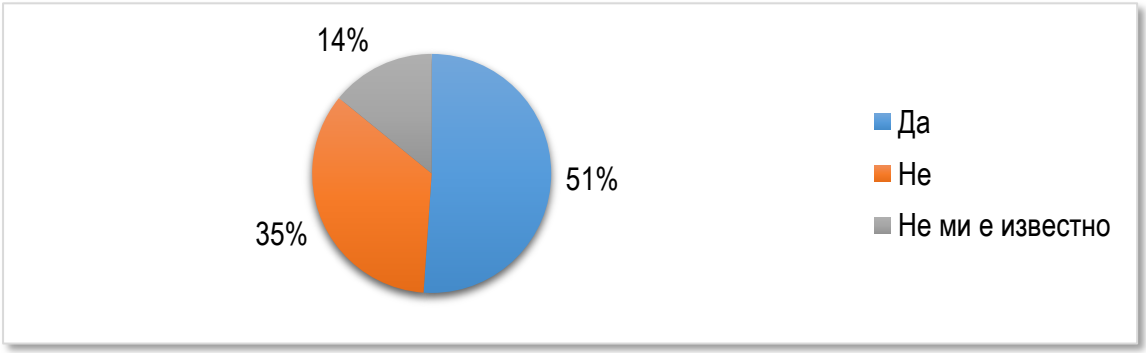
ГРУПА 5: Иновативни технологии

Използва ли се във Вашата организация (блокчейн) blockchains технологията?



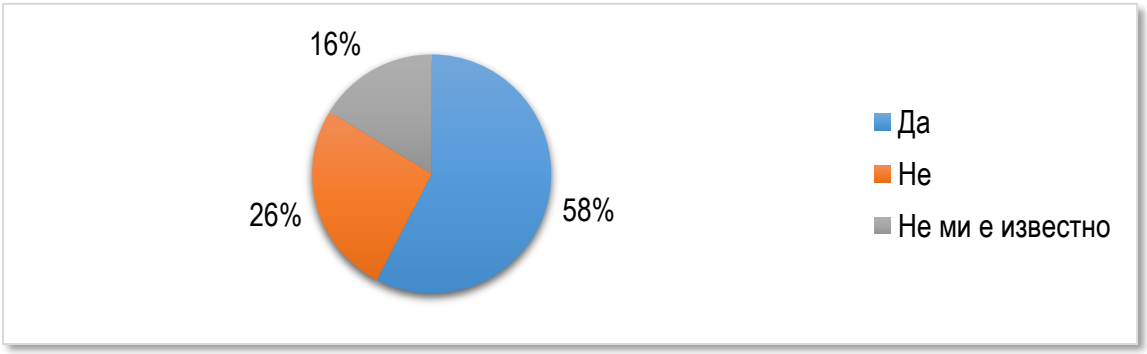
Само 5% от анкетираните заявяват, че използват блокчейн технология в тяхната организация. Останалата част или не използват или не знаят дали тя се използва.

Използвате ли във Вашата работа разпределени бази данни или разпределени места за съхранение и обработка на информация?



Разпределените бази данни или разпределени места за съхранение и обработка на информация се използват в повече от половината организации. В 35% от случаите не се налага използването на такъв тип бази данни.

Приложими ли са според Вас разпределени бази данни за Вашата организация?



Повече от половината анкетирани (58%) смятат, че в тяхната организация е приложимо използването на разпределени бази данни.

Пълният анализ на проучването, включващ всичките 50 въпроса, е представено в ПРИЛОЖЕНИЕ 3.

За **пряка обратна връзка** с представители на трите сектора бе организирана кръгла маса на тема: „*Кибер сигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България*“, състояща се 15 ноември 2018 г., гр. София. Кръглата маса бе организирана в две части.

В **първата част** бяха представени резултати от изследването по следните въпроси:

- **Анализ на държавната политика в областта на кибер сигурността**. Тук бе представен направения обзор и анализ на регулаторните инструменти, политики и стратегии на НАТО и ЕС, които влияят на кибер сигурността в България;
- **Общ преглед на блокчейн технология**. В тази част бе направено сравнение между публични и частни блокчейни, с техните особености, предимства и недостатъци. Също така бе представен анализ на същността и възможността за приложение на блокчейн технологиите в работата на държавната администрация и връзката им с кибер сигурността.
- **Анализ на възможностите за използване на изкуствен интелект и чатботове** при предоставяне на услуги и комуникация с потребителите, както и за поддържане на кибер сигурността.
- **Идентифициране на критични точки и перспективи.** Тук бяха представени резултатите от проведеното он-лайн изследване.

Във **втората част** беше дадена думата на участниците за мнения и препоръки по поставените в първата част въпроси и алтернативни модели за развитие на системата за кибер сигурност. В допълнение бяха представени шест базови алтернативни модели за организация на националната система за киберсигурност и критерии за тяхното оценяване. Предложените модели са съобразени с новоприетия закон за кибер сигурност. Присъстващите взеха активно участие в обсъждането на различните модели като общото мнение на участниците бе, че текущият модел за организация е най-неподходящ за постигане на система за кибер сигурност в България, чрез използване на иновативни технологии.

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО ПУБЛИЧНА
АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ

ГЛАВА ВТОРА

ПРИЛОЖЕНИЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ

ОБЩ ПРЕГЛЕД НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА. СРАВНЕНИЕ МЕЖДУ ПУБЛИЧНИ И ЧАСТНИ БЛОКЧЕЙНИ – ОСОБЕНОСТИ, ПРЕДИМСТВА И НЕДОСТАТЪЦИ. АНАЛИЗ НА СЪЩНОСТТА И ВЪЗМОЖНОСТИТЕ ЗА ПРИЛОЖЕНИЕ НА БЛОКЧЕЙН ТЕХНОЛОГИИТЕ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ВРЪЗКАТА ИМ С КИБЕР СИГУРНОСТТА

СЪЩНОСТ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА

ЗАБЕЛЕЖКА: Всички споменати в документа криптовалути и компании са представени единствено с илюстративна цел. Обсъждането на даден финансов инструмент в текущия документ не представлява препоръка за инвестиция или финансов съвет.

Блокчейн (в буквален превод „верига от блокове“) е публична база данни, в която транзакциите се групират в „блокове“, а между блоковете съществува криптографска връзка, която не позволява фалшифициране на съдържание в предходните блокове[104]. Впоследствие са създадени разновидности на технологията, които добавят други или премахват някои от тези свойства.

Първите сериозни стъпки в посока блокчейн са направени от Стюарт Хабер и У. Скот Сторнета, които предлагат архитектура на система за т.нар. “timestamping” на цифрови данни, т.е. верифицирано установяване на времето на публикуване на даден файл[105]. При тяхната архитектура съществува централизирана услуга, която предлага установяването на времето. Тази услуга издава (криптографски) сертификати, които съдържат времето, в което е подаден документа, хеш на съдържанието на документа, както и „указател“ към предишния издаден сертификат (формирайки „веригата“). По този начин системата осигурява ограничена защита дори и срещу злонамерена услуга, която е в съучастие с трета страна – при опит за по-късно фалшифициране на предишен сертификат, останалите добронамерени участници в системата биха могли да открият измамата, ако съхраняват своите сертификати и верифицират веригата. По-късна статия предлага оптимизация на схемата, при която вместо хеш-вериги се

[104] Narayanan A., J. Bonneau, E. Felten, A. Miller, S. Goldfeder: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016, ISBN: 978-0-691-17169-2, 336 p.

[105] Haber S., W.S. Stornetta: How to time-stamp a digital document. Journal of Cryptology, Vol. 3, 1991, pp.99-111.

използват хеш-дървета (по-известни като дървета на Merkle, на името на учения Ralph Merkle, който ги предлага)[106]. Това подобрение позволява по-ефективна проверка на криптографската валидност на издадените сертификати чрез намаляване на броя хешове, които е необходимо да бъдат проверени.

Следващият ключов компонент в блокчейн технологиите е свързан с борбата с непоискани електронни съобщения (т.нар. спам). През 1997, Адам Бек предлага схема с тази цел, която е базирана на т.нар. „Доказателство за работа“ (Proof-of-Work, PoW)[107]. При тази схема, изпращащият електронно съобщение следва да прикрепи към него специален низ, който съдържа метаданни за съобщението, както и произволна компонента, която изпращащият трябва да попълни по специален начин – хешът на целия низ (включително произволната компонента) следва да бъде по-малък (като число) от фиксирана константа. Тъй като не съществува ефективен алгоритъм, който да може да намери подобна компонента, изпращащият следва да изразходи известно (и предварително пресметнато) количество изчислителен ресурс, за да намери на случаен принцип подходяща стойност на тази компонента, което е същността на принципа „Доказателство за работа“. От своя страна, получателят може да провери дали низът е валиден чрез само едно пресмятане на криптографската хеш-функция. Съществуват и други съображения при имплементацията (например необходимост от база данни на вече използвани подобни низове). След известни успехи при внедряване на подхода в практиката, изникват сериозни проблеми, свързани с невъзможността за избор на подходящ праг на приемливи стойности на хеш-функцията, както и с различните изчислителни възможности на е-мейл сървърите, които изпращат съобщения[108].

Идеята за „остойностяване“ на изразходен изчислителен ресурс е представена от Уей Дай, който предлага „b-money”[109]. Първата „същинска“ имплементация на блокчейн технология е криптовалутата Биткойн. Автор на протокола на Биткойн, софтуерната му имплементация и статия, съдържаща математическо доказателство за смислеността на подхода, е Сатоши Накамото. Самият Накамото е изключително мистериозна личност до степен, в която до момента не е известно дали това е реално име или псевдоним и дори дали става въпрос за един човек, или за колектив[110].

[106] Bayer D., S. Haber, W.S. Stornetta: Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences II: Methods in Communication, Security and Computer Science, Springer-Verlag, 1993, pp. 329-334.

[107] Back A.: A partial hash collision based postage scheme. 1997, http://www.hashcash.org/papers/announce.txt

[108] Laurie B., R. Clayton: "Proof-of-Work" proves not to work. IN WEAS 04, 2004, pp. 1-11.

[109] Dai W. B-money. 1998. http://www.weidai.com/bmoney.txt

[110] S. L. "Who is Satoshi Nakamoto?". The Economist. 2015

Индивидът или групата Накамото притежават над 1 милион биткойна, придобити почти изцяло чрез т.нар. добив ("mining"), процес, при който участниците в мрежата биват възнаградени за вложения изчислителен ресурс. През 2010 г. контролът върху софтуерната имплементация на валутата е предаден на Гавин Андресен.

Следващата важна стъпка в развитието на блокчейн технологиите е платформата Етериум (също известна като Етереум, оригинално "Ethereum"). Етериум може да се използва и като криптовалута (наречена „етер"), но основната цел на платформата е да надгради Биткойн, като позволи изпълнение на т.нар. „интелигентни договори" („smart contracts"). По същество са самостоятелни единици в мрежата и могат да бъдат „извикани" с цел изпълнение на договора само ако заложените условия са изпълнени, което се верифицира с помощта на цялата мрежа[111]. Областта на приложение на „интелигентните договори" се счита за изключително перспективна, но също така и изключително трудна поради сериозността на последствията при уязвимости в договора.

Други платформи, които са важни стъпки в развитието на блокчейн технологиите, са:

- **Ripple:** екосистема, която е фокусирана повече върху функции като обмен на валути и система за сетълменти между участниците в нея, отколкото върху криптовалутата Ripple[112]. Сред потребителите на Ripple са международни банки, които използват платформата в капацитет на сетълмент система;
- **Dash:** криптовалута, чиято първа версия е публикувана януари 2014. Системата включва възможността за транзакции с таен получател, които се постигат чрез „размесване" на валутата, така че проследяването на крайния получател на сумата да бъде затруднено[113];
- **Monero:** друга криптовалута, фокусирана върху анонимност. Първата версия на софтуерната имплементация на валутата е публикувана през април 2014. За разлика от Dash, при Monero всички транзакции са анонимни – трети лица не могат да установят изпращащия, получателя или сумата;
- **Zcash:** още една криптовалута, която добавя тайни транзакции. При Zcash, валутата може да се намира в „прозрачен" или „непрозрачен"

[111] Buterin, V. White paper. Ethereum Wiki. https://github.com/ethereum/wiki/wiki/White-Paper
[112] Ripple Inc. Math Based Currency. 2015. https://ripple.com/
[113] Prusty, Narayan, Building Blockchain Projects, 2017

адрес. За гарантиране на невъзможността да се похарчи една и съща валута повече от веднъж се използват т.нар. “Zero-knowledge proofs”[114].

Освен криптовалутите и интелигентните договори, блокчейн намира приложения и в други области, като например управление на верига от доставчици (Supply Chain Management), гарантиране на интегритет на данни (например логове от информационни системи) и други.

Данните в блокчейн мрежата се записват за постоянно чрез файлове, наречени „**блокове**“. Данните, които се съхраняват в блока, са непроменливи. Блокът може да се представи като списък от транзакции, съхранен в публичен регистър на транзакциите (public ledger). Информацията в този регистър се обработва като записите от всяка транзакция се записва в блокове. Всеки блок е свързан със следващия блок чрез криптографски хеш (hash), т.е. когато един блок бъде завършен, той създава уникален код, който се свързва със следващия блок. Всеки блок започва с информация от предходния блок във веригата и завършва с информация, въвеждаща в следващия. По този начин се създава **верига от блокове** или **блокчейн (blockchain)**, където блоковете следват в хронологичен ред (Фигура 13).

Фигура 13. Блокчейн процес

[114] Ben-Sasson, Eli; Chiesa, Alessandro; Garman, Christina; Green, Matthew; Miers, Ian; Tromer, Eran; Virza, Madars, Zerocash: Decentralized Anonymous Payments from Bitcoin, IEEE Symposium on Security and Privacy, 2014, 459-474

Хешът в блокчейна се създава от данни, които се съдържат в предишния блок и може да се представи като пръстов отпечатък на тези данни. По този начин блокът се „заключва“ по ред и време. Въпреки, че блокчейнът е иновативна технология, хеширането не е. То се използва вече повече от 30 години и се характеризира с това, че създава еднопосочна функция.

Веригата от блокове (**блокчейн**) се съхранява в мрежата в разпределен вид, като минимум половината компютри в мрежата притежават копие от този публичен регистър и не съществува едно единствено „главно копие“. Това прави компрометирането на транзакциите практически невъзможно, тъй като участниците във веригата от блокове са равноправно участващи компютри в **децентрализирана мрежа** и няма как да се направят промени в регистъра (това, обаче, не означава, че не може да бъде променян статуса на транзакцията). След като един блок е валидиран и записан, той не може да бъде променян, без да бъдат променени всички следващи го блокове.

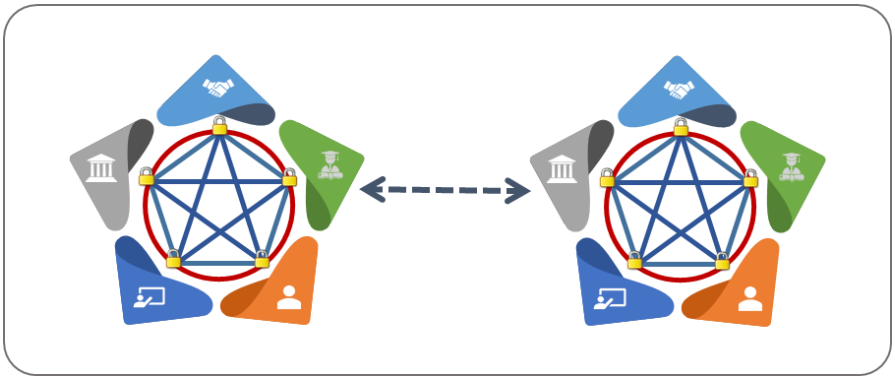
Видове блокчейн

Съществуват три основни вида блокчейн: публичен, частен и федериран (споделен)[115] (Фигура 14).

а) Публичен блокчейн

б) Частен блокчейн

[115] https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/ accessed on 15.11.2018



в) Федериран блокчейн

Фигура 14. Публичен, частен и федериран блокчейн

Публичният блокчейн представлява децентрализирана мрежа, в която всеки може да се присъедини, тъй като няма нужда от разрешение за присъединяване. Потребителите свързват техните компютри чрез P2P (Peer-to-Peer) като образуват т.нар. „мрежа от възли“. Всеки възел съдържа запис от блокчейна, който се съхранява на техния компютър. Така информацията на всеки публичен блокчейн се репликира върху хиляди възли в мрежата. На практика никой от възлите не се администрира централизирано, поради което не може да бъде унищожена мрежата като бъде изваден от строя един централен сървър.

При **частния блокчейн** членуването на отделните участниците в мрежата е строго контролируемо. Те също могат да бъдат както големи и разпределени системи, които използват собствен маркер (token). Тези типове блокчейни се предпочитат от консорциуми, които имат доверие в членовете и търгуват с поверителна информация.

Федериранят (споделеният) блокчейн функционира под управлението на определена група потребители. За разлика от публичният блокчейн групата не разрешава всеки потребител с достъп до Интернет да участва в процеса на верифициране на транзакциите. Федериранят блокчейн е по-бърз и позволява по-добра поверителност на транзакциите. Този тип блокчейни се използват предимно в банковия сектор. Правата за четене от системата могат да са както публични, така и ограничени до определен брой потребители.

Едно от най-известните и получили популярност приложение на блокчейн технологията е при криптовалутите. Някои от по-известните криптовалути са: Биткойн, Етериум, Dash/Monero/Zcash, които са описани в ПРИЛОЖЕНИЕ 4.

Основни елементи на блокчейн технологията

На практика почти всички криптовалути притежават няколко основни елемента: публични транзакции; сметки, адреси и портфейли; транзакции и блокове; консенсус в мрежата и Доказателство за работа; Начален блок, възнаграждение за „добив“ на блок и контролирано предлагане.

Публични транзакции

Тъй като основното определящо свойство на блокчейн технологиите е децентрализацията (или иначе казано липсата на централна власт), за да бъде гарантирана сигурността на транзакциите срещу (например) „двойно похарчване“ на валута, е нужно всички транзакции да бъдат публични[116].

Редно е да се спомене, че е възможно част от атрибутите на транзакциите да не бъдат публични (както е например при Dash, Monero и Zcash), а също е възможно транзакциите да не бъдат публикувани извън потребителите на въпросната блокчейн мрежа (както може да бъде при т.нар. „частни“ блокчейни).

Сметки, адреси и портфейли

В повечето блокчейн екосистеми за отваряне на „сметка“ не е необходима формална регистрация към външна организация – всеки потребител може да създаде множество свои „сметки“ като просто генерира криптографска двойка публичен/частен ключ. Разбира се, подобни „сметки“ започват празни.

Вместо банкови номера като IBAN или имена на собственика, криптовалутите използват като идентификатор на „сметките“ адреси. Въпросните адреси са криптографски обвързани с публичния ключ чрез хеш по начин, който е на практика 1-към-1[117].

Транзакции и блокове

Макар и „блокът“ да е основен градивен елемент на структурата от данни, която представлява блокчейнът, в повечето случаи най-малката градивна единица на тази структура е транзакцията, а един блок може да съдържа повече от една транзакция. Всеки нов блок във веригата съдържа в себе си набор от транзакции между адреси заедно с криптографска структура, гарантираща невъзможността да бъдат подменени данните в

[116] Dai W. B-money. 1998. http://www.weidai.com/bmoney.txt

[117] BlockGeeks, Inc., Blockchain Address 101: What Are Addresses on Blockchains?, https://blockgeeks.com/guides/blockchain-address-101/

транзакцията (вече споменатата структура хеш-дърво или дърво на Merkle). Освен това блокът съдържа хешът на предходния блок, както и текущото време. При криптовалути, използващи модел Доказателство за работа, в блока често се съдържа и текущата „трудност“ на задачата (еквивалентна на константата, която е граница за приемлива хеш-стойност в изчислителната задача; обсъдена по-надолу), както и един или повече произволни параметри. Тези параметри са единствените, върху който „добиващият“ има пълен контрол, но те участват по критичен начин в изчислителната задача, която е основа на Доказателството за работа.

Консенсус в мрежата и Доказателство за работа (Proof of Work, PoW)

Предвид разпределения характер на криптовалутите, изключително важен въпрос е как могат различните членове в мрежата да достигнат консенсус за това кои транзакции са изпълнени и по-конкретно кое е текущото състояние на блокчейна.

Макар и да не се използва от всички криптовалути, към момента стандартният модел за достигане на консенсус е чрез „Доказателство за работа“. При този модел за да бъде добавен към блокчейна, даден блок трябва да има хеш-стойност, по-малка от зададена константа. Това се постига чрез търсене с изчерпване на произволните параметри в блока (виж по-горе). Изрично изискване на хеш-алгоритмите, използвани в блокчейн технологиите е най-ефективният алгоритъм за намиране на такива стойности да бъде търсене с изчерпване, тъй като в това се състои същността на доказателството за работа – „добилият“ блока участник в мрежата доказва, че е инвестирал необходимите изчислителни ресурси, за да реши тази задача. Гореспоменатата константа се определя от параметъра „сложност“ на изчислителната задача и обикновено се обновява на даден брой „добити“ блокове. Целта на това обновление е да запази фиксирано средното време между „добиване“ на два блока, тъй като това е един от фундаменталните параметри на даден блокчейн и определя възможността за дадено приложение в практиката. Съществуват алтернативни модели за консенсус в мрежата, например набиращият популярност „Доказателство за залог“ (Proof of Stake, PoS), който е обсъден по-надолу.

Начален блок, възнаграждение за „добив“ на блок и контролирано предлагане

С цел да гарантира мотивацията на участниците при „добива“ на блокове (например за осигуряване на реалните разходи, които възникват при решаването на изчислителната задача в модела Доказателство за

работа), блокчейн системите предлагат възнаграждение за „добиване“ на блок. Традиционно по-голямата част от съответната криптовалута влиза в обращение по този начин, но е стандартно част от валутата да е раздадена още в първия блок. Този блок се нарича начален или „генезис“ блок (Genesis block) и е внедрен в софтуера за работа със съответната криптовалута, тъй като няма предшественик[118]. Друга стандартна практика е наградата за „добиване“ на блок да се намалява с фиксиран процент след определен брой добити блокове. Тези особености позволяват да бъде изчислена общата наличност в съответната криптовалута, свойство, наречено „контролирано предлагане“ (т.нар. “controlled supply”), тъй като предлагането на валутата е публично и предвидимо[119].

Основни характеристики на блокчейн технологията

Въпреки че първоначално е свързана с биткойн, блокчейн технологията може да бъде използвана самостоятелно в разнообразни приложения, в които се управляват активи и се извършват сделки. Тя може да осигури сигурна верига на попечителство както за цифрови, така и за физически активи чрез своите функционални възможности, които улесняват транзакциите чрез доверие, консенсус, сигурност и интелигентни договори. Като основни нейни характеристики може да посочим (Фигура 15):

- **надеждност и наличност**: доколкото множество участници споделят блокчейна, много по-малка е вероятността от унищожаване на данните и уязвимост от атаки;
- **непроменяемост**: почти невъзможно е да се направи промяна във веригата без да остане следа, което намалява възможностите за измами;
- **неотменимост**: има възможност записите да бъдат направени неотменими;
- отчитане в почти реално време;
- **намаляване на разходите** чрез премахване на зависимостта от посредници или трети страни (банки, правни институции, държавно управление);
- **прозрачност**: консенсусният механизъм осигурява възможност за получаване на консолидиран и свързан набор от данни с намалени грешки;
- **консолидиране на бази от данни**: подход при който няколко бази данни се обединяват с цел по-добро използване както на

[118] https://en.bitcoinwiki.org/wiki/Genesis_block
[119] https://en.bitcoin.it/wiki/Controlled_supply

изчислителни ресурси, така и на изискванията за сигурност и нормализация;

- **споделяне на данни между участниците**: основна характеристика на блокчейн технологията, която гарантира невъзможността за промяна на транзакциите;
- **адаптивни интелигентни договори** (customizable smart contracts);
- **сигурност и защита на данните**: характеристика имаща отношение към тайната, целостта, наличността и поверителност на данните и транзакциите.

Фигура 15. Характеристики на блокчейн технологията

НАПРАВЛЕНИЯ ЗА ПРИЛОЖЕНИЕ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

Блокчейн-базираните решения са подходящи за използване при случаи, в които много страни, които имат ниски нива на доверие, сключват сделки един с друг. Технологията е приложима в области, в които информацията за една и съща транзакция се съхранява в различни системи или бази данни. Конкретното решение зависи от чувствителността на данните по време, от разходите за съгласуване, от необходимостта от сигурност на данните и от изискването за удостоверяване. Ако обаче

съществува само една страна, блокчейн не осигурява допълнителни ползи спрямо традиционните приложения, използващи база от данни.

Основни направления за приложение на блокчейн технология са описани в ПРИЛОЖЕНИЕ 5, а тук са споменати някои от най-подходящите за приложение в държавната администрация (Фигура 16):

- персонална идентификация;
- системи за електронно гласуване;
- публични регистри и администриране на нотариални актове – кадастър, поземлен регистър, на превозните средства и др.;
- здравеопазване – електронни здравни досиета;
- образование – дипломи, сертификати и др.;
- съдебна и правна система;
- следене произхода и пътя на продукти (управление на доставки);
- МВР и гранична полиция – управление на бежанския поток, граничен контрол и др.;
- взаимодействие между различни администрации (цифровизация и ускоряване на административните процеси);
- система за управление на обществени поръчки.

Фигура 16. Приложение на блокчейн в държавната администрация

Сигурност

Сигурността на блокчейн технологиите безспорно е един от най-важните аспекти, които всички изследователи и разработчици трябва да имат предвид. Най-общо може да се дефинират в следните направления, в които трябва да се разглежда и оценява сигурността на блокчейн:

- **Сигурност на физическия слой на IT инфраструктурата**, който включва специфични регулации и имплементации като EAL5, мрежова инфраструктура и изисквания за изолация/разделяне. Средният слой на

блокчейн включва изисквания към криптографските модули, нива на криптиране, алгоритми за криптиране, начини за съхранение на данните, трансфер на данните и достъп до данните от различните типове потребители в мрежата.

❖ **Блокчейн консенсус (или т.нар. доверен слой на системата).** Този слой е централен за блокчейн архитектурата и трябва да осигури основните изисквания към съхранението на данни. Ако има повече потребители на мрежата, то е необходимо да се поставят изисквания към начина на съхранение на данните и техният обем. За постигане на тези изисквания и начина на разпределение на данните е необходимо постигането на т.нар. консенсус. По този начин се разделят системите, които са за използване на крипто-валута и такива, които използват блокчейн технологиите с друго предназначение.

От друга страна, когато се планира и изгражда решение на базата на блокчейн, е необходимо да се адресират и следните аспекти:

❖ **Поверителност.** Поверителността на транзакциите е една от основните характеристики на блокчейн технологията. Въпреки, че всички го смятат за нещо дадено и логично, особено в публичните блокчейн системи, т.е. всичко е прозрачно и видимо, тази характеристика има голямо влияние и значение за някои от сферите на приложение като финанси, здравеопазване и др. В някои от блокчейн имплементациите поверителността е едно от изискванията и, когато се проектира и изгражда такъв тип система, е необходимо да се отчита този аспект.

❖ **Неразличимост.** Това са криптографски техники, които могат да се използват като катализатор за всички въпроси/предизвикателства, свързани с поверителността и тайната на данните в блокчейн технологиите. За съжаление тези техники не са все още достатъчно добре изследвани, за да бъдат имплементирани в конкретни реализации. Тези техники са познати като „Indistinguishability obfuscation“. За първи път концепцията е предложена от Sahai и съавтори в доклад на тема „Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits“[120]

❖ **Хомоморфна криптография.** Този вид криптография позволява да бъдат извършвани различни операции върху криптирани данни. При условие, че технологията се имплементира в блокчейн системата, то това ще позволи обработка на криптирани данни чрез запазване на поверителността и тайната им. Тази концепция е тествана в проекта Enigma от MIT's Media Lab, което позволява множество потребители да извършват

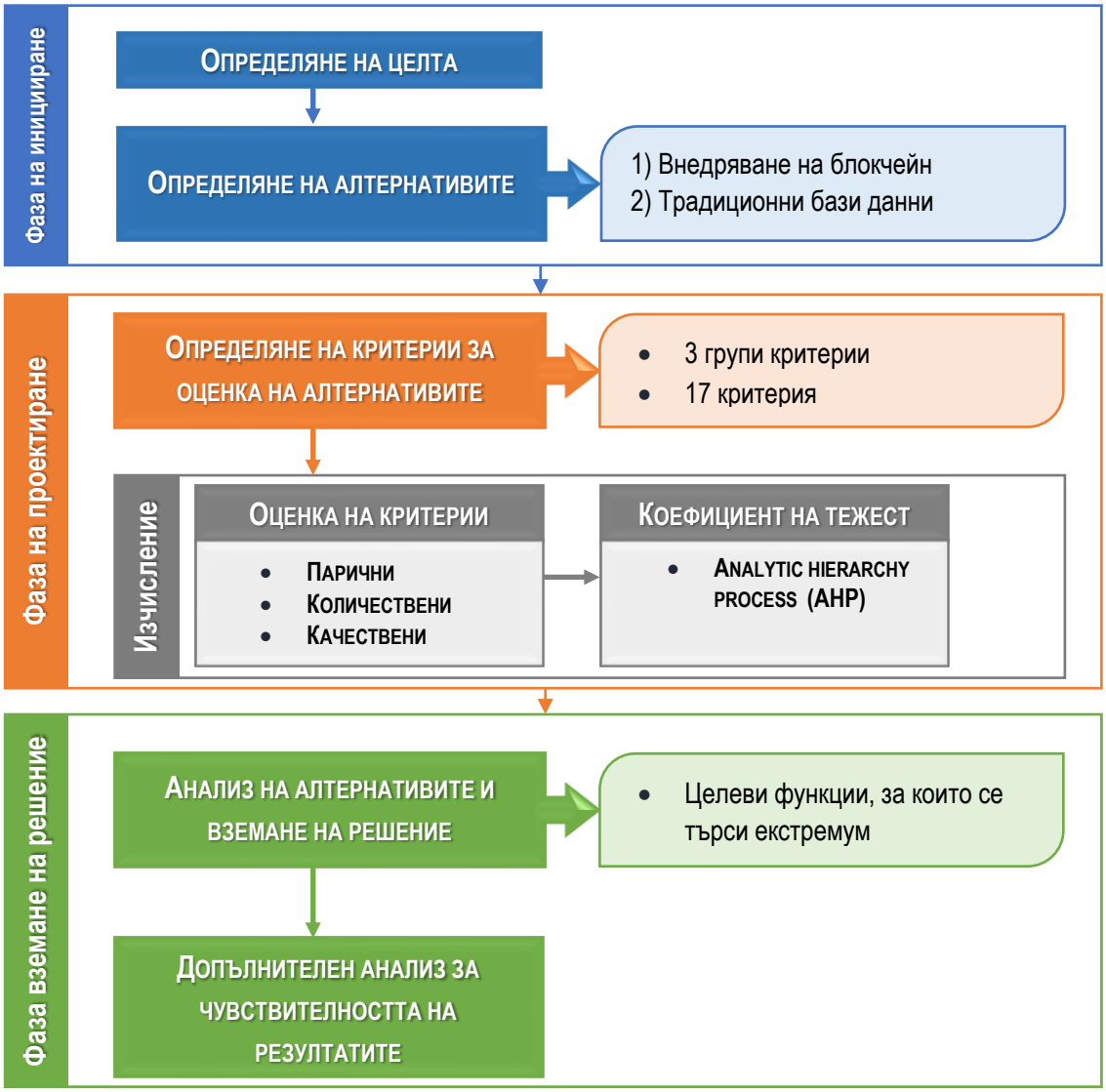
[120] https://eprint.iacr.org/2013/451.pdf

различни изчисления върху криптирани данни без да имат реалната информация за тяхното съдържание.

- **Доказателство за нулево познание (знание).** Този тип концепция е имплементирана в Zcash, като целта й е запазване на поверителността на транзакцията. Също така тя е приложима и за Ethereum.
- **Сигурни разпределени изчисления.** Идеята за разпределени изчисления не е нова и е базирана на концепцията, че данните се разпределят между множество потребители, чрез използване на единен механизъм за сигурно (тайно) споделяне. След това изчисленията се извършват на различните места и не е необходимо данните отново да се съберат на едно централно място, за да се получи крайният резултат. Резултатът, получен след изчисленията, също е разпределен между участниците.
- **Използване на хардуерни решения за гарантиране на тайната.** Защитените/сигурните изчислителни платформи (Trusted computing platforms) могат да се използват за създаване на механизъм, чрез който да се гарантира тайната на транзакцията, извършвана в блокчейн системата. Ако тази технология бъде имплементирана в интелигентните договори, то когато една страна изпълни интелигентният договор, тогава тя може да създаде елемент (изчислен от системата), който да служи като доказателство за коректно и успешно изпълнение. По този начин другите страни само трябва да го проверят.

ПОДХОД ЗА ИЗЧИСЛЯВАНЕ НА ПОЛЗИТЕ И РАЗХОДИТЕ ОТ ВНЕДРЯВАНЕ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

За изчисляване на ползите и разходите от внедряване на блокчейн технологията в държавната администрация е подходящо използването на многокритериалния анализ (Фигура 17).



Фигура 17. Многокритериален анализ

Предложеният подход се основава на идентифицирането на алтернативи за намиране на най-доброто решение, като се отчитат различни фактори и очакванията на лицата, вземащи решение.

Фазите, през които преминава процесът на многокритериалния анализ, са: фаза на иницииране, фаза на проектиране и фаза на взимане на решение. (Фигура 18).

Фигура 18. Фази на многокритериалния анализ

Фазата на иницииране:

- Определяне на целта;
- Определяне на алтернативите за постигане на целта;
- Определяне на критериите за оценка на отделните алтернативи;
- Оценяване на критериите;
- Поставяне на коефициент на тежест на критериите;
- Анализ на алтернативите и вземане на решение;
- Допълнителен анализ на чувствителността на резултатите.

Целта е подобряване на ефективността на работа на държавната администрация като се отчита възможността чрез приложение на блокчейн технологията да се повиши кибер сигурността, доверието и прозрачността в работата на държавната администрация.

При **определянето на алтернативите за постигане на целта** се разглеждат различни варианти за подобряване работата на държавната администрация, които включват, освен внедряване на блокчейн технология в системите на държавната администрация и стандартни алтернативи, задължителни при този тип анализ, а именно: нищо не се прави или се прави минималното ("business as usual" или "do-minimal").

Една от най-сложните задачи е да се **определят групи критерии и самите критерии**, по които ще се оценяват отделните алтернативи.

За конкретния анализ предлагаме **три основни групи критерии**: технически, функционални и правни, които обобщават аспектите за оценка на ползите от внедряването на блокчейн технологията в държавната администрация. Основните групи и съдържащите се в тях критерии, са представени в секция „Критерии за оценка на внедряването на блокчейн в държавната администрация“ от този раздел.

За да бъде направена оценка на критериите, се съставя матрица, в която:

- всеки ред описва отделната алтернатива;
- всяка колона отговаря на отделен критерий и съдържа неговото измерение на ползата, което носи за съответната алтернатива.

Съществуват три основни типа техники за измерване на различните критерии:

- **парични** – където могат да се извлекат парични стойности, например базирани на принципите на анализа разход-полза;
- **количествени** – където не могат да бъдат определени парични стойности, но има възможност влиянието на критерия да бъде измерено количествено в непарична единица;
- **качествени** – в тези случаи въздействието на критерия не може да бъде оценено количествено и тогава се прилага цифрова скала за експертна оценка (напр. от 0 до 6).

Поставяне на коефициент на тежест на критериите

Важен момент при този подход е **определянето на коефициент на тежест** на критерия при вземането на решение. Тегловият коефициент на отделния критерий показва степента, с която оценката на съответния критерий оказва влияние върху общата оценка на групата, към която той

принадлежи. Тегловият коефициент за отделния критерий може да се определи с помощта на метода AHP (Analytic Hierachy Process)[121].

С помощта на различни методи за вземане на решение се **анализират алтернативите** и се прави **избор** на една от тях, като се използват тегловите оценки и стойностите на всеки един критерий. Методите за анализ могат да бъдат представени като множество от целеви функции, за които се търси екстремум (максимум или минимум).

Когато се прави изследване в публичния сектор може да се получи различно „виждане“ за определянето на тежестите на съответните критерии за оценка на алтернативите. В тази връзка могат да бъдат консултирани различни групи от участници и да се **направят различни сценарии** на изследването.

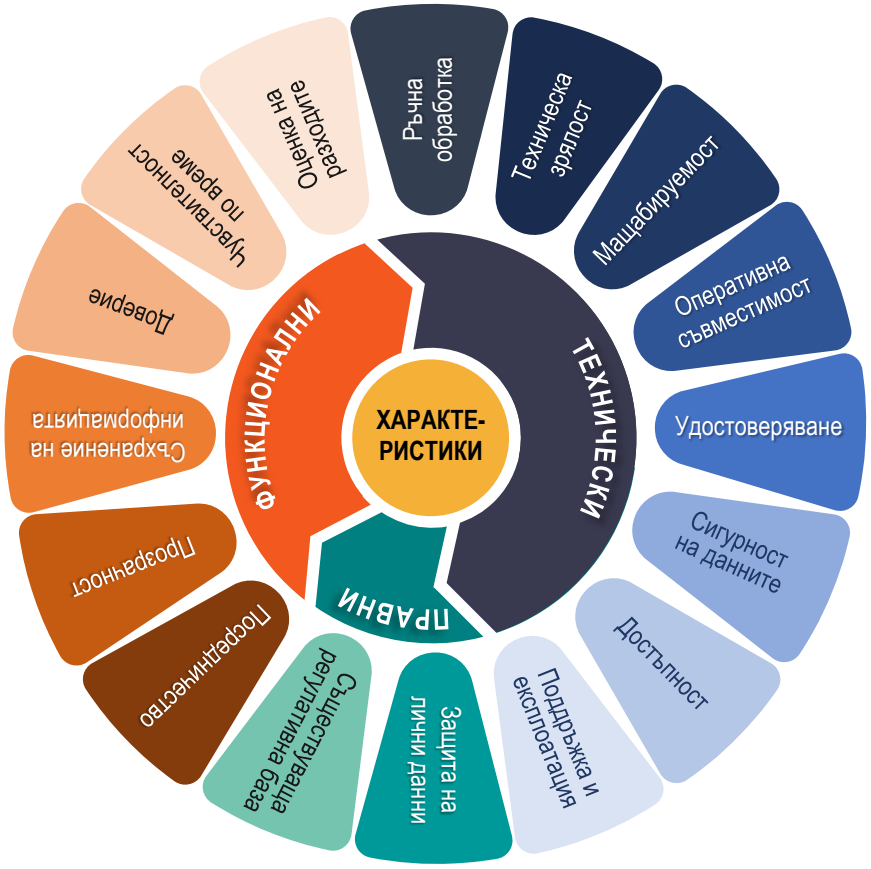
КРИТЕРИИ ЗА ОЦЕНКА НА ВНЕДРЯВАНЕТО НА БЛОКЧЕЙН В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

На Фигура 19 са представени критериите и съответните групи от критерии, които могат да бъдат използвани при прилагане на многокритериалния анализ.

Технически критерии:

- **ръчна обработка:** оценка на количеството документация и доклади, които се изготвят ръчно (водещо до увеличаване на възможността за грешки и разход на човекочасове);
- **техническа зрялост:** анализ на количеството последователни стъпки, през които минава процесът на предоставяне на услугата (управление на работния процес). Оценка на количеството документи, които се обработват и проверяват ръчно. Оценка кои от процесите могат да бъдат цифровизирани и съответно интегрирани в блокчейна.
- **мащабируемост:** блокчейн технологията има способността да обработва голям обем сделки или данни в относително кратък период от време. Когато, обаче, става дума за интегриране на много големи бази данни или обработка на изключително големи обеми данни едновременно, мащабируемостта е проблем. Колкото по-голям е блокът, толкова по-тромаво се обработват транзакциите. Затова трябва да се направи оценка на размера на услугата, за да се прецени дали решението да се приложи блокчейн технология е правилния избор;

[121] Thomas L. Saaty, Mathematical Principles of Decision Making: The Complete Theory of the Analytic Hierarchy Process (Pittsburg, PA: RWS Publications, 2010)



Фигура 19. Критерии за оценка на внедряване на блокчейн в ДА

❖ **оперативна съвместимост:** оценка на степента на интеграция с други блокчейн системи, предоставящи услуги, свързани с разглежданата услуга;

❖ **удостоверяване:** колко от отделните етапи от услугата са все още хартиено-зависими и по тази причина изискват ръчна проверка на истинността; оценка на количеството хартиени документи, които са необходими да бъдат валидирани през целия процес на предоставяне на услугата;

❖ **сигурност на данните:** данните трябва да бъдат защитени от евентуално фалшифициране и кражба, като едновременно с това се осигури контролирано споделяне между участниците (напр. осигуряване на възможност за прехвърляне на активи сред гражданите и бизнеса,

удостоверяване пред трети страни като работодатели, банки и др.); оценка на типа на данните, които трябва да бъдат споделени между участниците в процеса (граждани, бизнес организации, работодатели, банки, администрация и др.);

- **достъпност:** задължителен критерий при оценка на системата, предоставяща услугата, е дали може да гарантира достъп на хората с увреждания;
- **поддръжка и експлоатация:** оценка на ресурсите, необходими за поддръжка и експлоатация на системите (хардуер, софтуер, човешки ресурс).

Функционални критерии:

- **посредничество:** оценка на количеството посредници, от които зависи изпълнението на услугата (големият брой посредници води до повишаване на цената на услугата, увеличаване на времето за изпълнение, възможност за грешки и намаляване на доверието);
- **прозрачност:** ще подобри ли качеството на обслужване възможността за видимост на текущото състояние в реално време. Оценка на ползите от възможността за проверка на статуса по изпълнение на услугата от отделните участници;
- **съхраняване на информацията:** оценка на възможността от използване на централизирано/децентрализирано хранилище;
- **доверие:** оценка доколко предоставяната услуга предполага зависимости между участници с ниска степен на доверие един към друг (документи, които могат да бъдат фалшифицирани; документи, които може да съдържат грешки поради ръчната им обработка), което налага намесата на държавни органи в проверката и удостоверяването на документацията;
- **чувствителност по време:** оценка на ефекта от намаляване на времето за валидиране и проверка на всяко ниво, което ще се постигне от използването на блокчейн технологията;
- **оценка на разходите** за проучване и развитие, за внедряване, поддръжка и експлоатация;

Правни критерии:

- **защита на личните данни:** GDPR, закон за защита на личните данни, и др.
- **съществуваща регулативна база:** закон за електронен документ, закон за електронния подпис и др.

ПРИМЕРИ И ВИЗИЯ ЗА ПРИЛОЖЕНИЕ НА БЛОКЧЕЙН В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ, ВКЛЮЧИТЕЛНО ПРИ ИЗГРАЖДАНЕТО И ПОДДЪРЖАНЕТО НА ПУБЛИЧНИ РЕГИСТРИ И ОЧАКВАНИТЕ РЕЗУЛТАТИ ОТ ТОВА

ПРЕГЛЕД И АНАЛИЗ НА СВЕТОВНИТЕ ТЕНДЕНЦИИ И ДОБРИ ПРАКТИКИ ПРИ ВНЕДРЯВАНЕ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА

Анализ на блокчейн технологията имплементирана в Естония

Да си част от цифровото общество означава да си отговорен за начините на ползване на информацията, но също така и да приемеш, че ще бъдеш изложен на кибер заплахи. Със стабилни и последователни инвестиции в инфраструктурата за кибер сигурност, Естония разви широка експертиза в областта и се превърна в една от водещите държави.

На базата на опита на Естония след кибер атаките през 2007 г., в страната беше разработена скалируема блокчейн технология, която да осигури интегритет на съхраняваните данни в държавните/правителствените системи, а също така и да защити данните от вътрешни атаки.

Keyless Signature Infrastructure (KSI) Blockchain

KSI е блокчейн технология разработена в Естония и използвана в няколко международни организации. Целта на технологията е да „създаде“ сигурни мрежи, системи и данни, които не могат да бъдат компрометирани и в същото време да осигурява 100% неприкосновеност на личните данни.

Както вече беше споменато в предишната глава, блокчейн технологията се основава на създаването на разпределен публичен регистър – база данни с множество предварително дефинирани правила, за това как се добавя запис в регистъра (в базата данни). В основата на тези правила е изискването, за невъзможност за промяна на вече въведени и записани/проверени данни в регистъра/системата.

Чрез използване на KSI блокчейн в Естония се гарантира, че записаната информация в правителствените/държавните мрежи и системи не може да бъде променяна назад във времето от никой, а също така се гарантира, че автентичността на данните може да бъде математически проверена и доказана. Това означава, че никой – хакер, системен

администратор или правителството като цяло не може да манипулира данните без това да бъде установено.

Същност на Keyless Signature Infrastructure (KSI)

KSI е метод и широко (глобално) разпространена разпределена мрежова инфраструктура за издаване и проверка (верификация) на KSI електронни подписи. В сравнение с традиционните системи за създаване на електронни подписи, като инфраструктури с публичен ключ (Public Key Infrastructure – PKI), които се основават на т.нар. асиметрични криптографски алгоритми (или криптография с публични ключове), в KSI се използват само криптографски хеш функции. По този начин проверката се извършва и основава само на сигурността на хеш функциите и наличността на публичния регистър – известно като блокчейн.

KSI блокчейн технологията преодолява две основни слабости на традиционните блокчейн технологии, което от своя страна я прави удобна за използване в различни системи, изискващи скалируемост до големи мащаби, а именно:

- Скалируемост: Едно от основните изисквания към съвременните блокчейн технологии е скалируемостта – те скалират с комплексност $O_{(n)}$, т.е. те скалират линейно с броя на транзакциите. В сравнение KSI блокчейн скалира с $O_{(t)}$ комплексност, т.е. скалира линейно в съответствие с времето и независимо от броя на транзакциите.
- Време за съгласуване: За разлика от широко използвания подход при имплементиране на блокчейн технологията в системи за криптовалута, при KSI броят на участниците е ограничен. Чрез ограничаване броя на участниците е възможно да се постигне синхронно съгласуване между тях. По този начин се постига съгласуване в системата за една секунда.

Предимства на KSI

В тази част от доклада са посочени предимствата на KSI.

- **Скалируемост до големи мащаби**. KSI подписите могат да бъдат генерирани в мащаб на екзабайти. Независимо дали екзабайт данни се генерират всяка секунда, всеки запис може да бъде подписан с KSI минимални изисквания за изчислителна мощ, място за съхранение и допълнителен мрежови трафик.
- **Преносимост**. Свойствата на подписаните данни могат да бъдат проверени независимо, че са преместени/пренесени в друго географско местоположение, друга организация или друг доставчик на услуги.
- **Квантов имунитет (устойчивост на квантови атаки)**. Криптографските алгоритми използвани в KSI са с доказана устойчивост на

квантови атаки и гарантират, че системата ще може да се използва и да е сигурна дори и след изобретяване и пускане в употреба на т.нар. квантов компютър.

❖ **Независима проверка**. Характеристиките на подписаните данни могат да бъдат проверени без да е необходимо да има сигурен (доверен) доставчик.

❖ **Поверителност на данните**. KSI не записва (интегрира) никакви данни, касаещи потребителите. За тази цел системата използва еднопосочни криптографски хеш функции, които генерират уникални стойности и по този начин еднозначно представят данните. В същото време те са необратими, т.е. не може да се възстановят данните имайки резултантния хеш. По този начин поверителността на данните е гарантирана във всеки един момент.

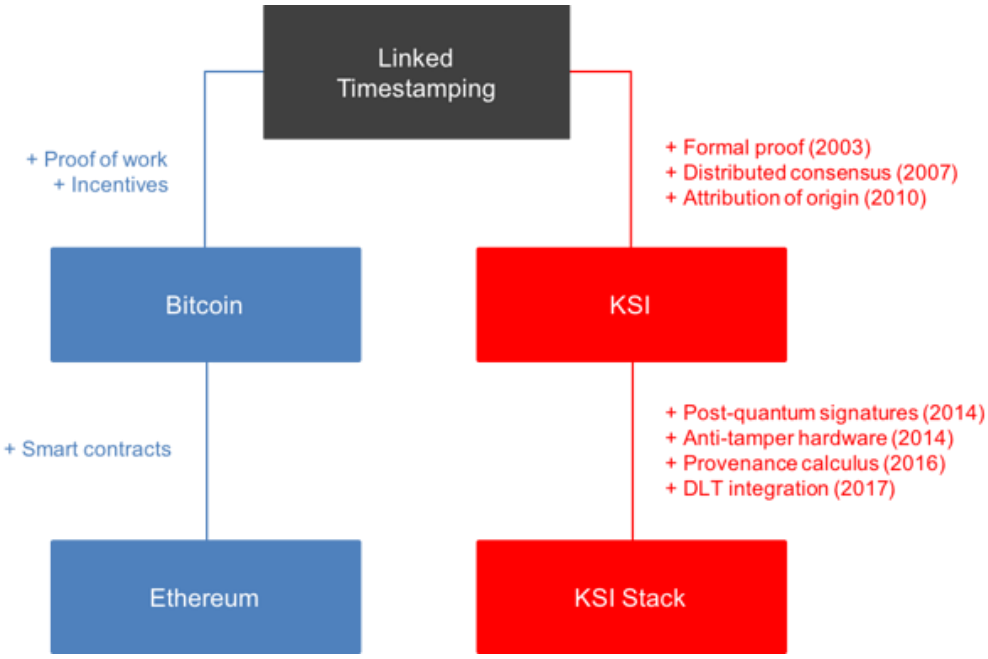
На Фигура 20 са дадени някой от основните характеристики на KSI.

Property	Keyless Signature Infrastructure (KSI) Blockchain
Intended use case:	Data Management and Digital Assets
Blockchain type:	Permissioned / Private
Platform hardening:	Anti-tamper hardened nodes
Blockchain scalability:	10^{12} registrations / second, globally
Blockchain settlement time:	1 second, globally
Blockchain size:	Blockchain growth deterministic and linear in time
Data privacy:	Information nor use patterns are never disclosed
Time:	No external timestamps necessary for a proof of time
Trust anchor:	Widely witnessed, electronic and physical media
Formal security proof:	Yes
Quantum threat:	Not vulnerable

Фигура 20. Характеристики на KSI блокчейн[122]

На Фигура 21 е представено различното развитие и реализация на класически блокчейн технологии и KSI

[122] Randy D Bishop, Introduction to Guardtime and KSI Blockchain, guardtime



Фигура 21. Развитие и реализация на класически блокчейн технологии и KSI[123]

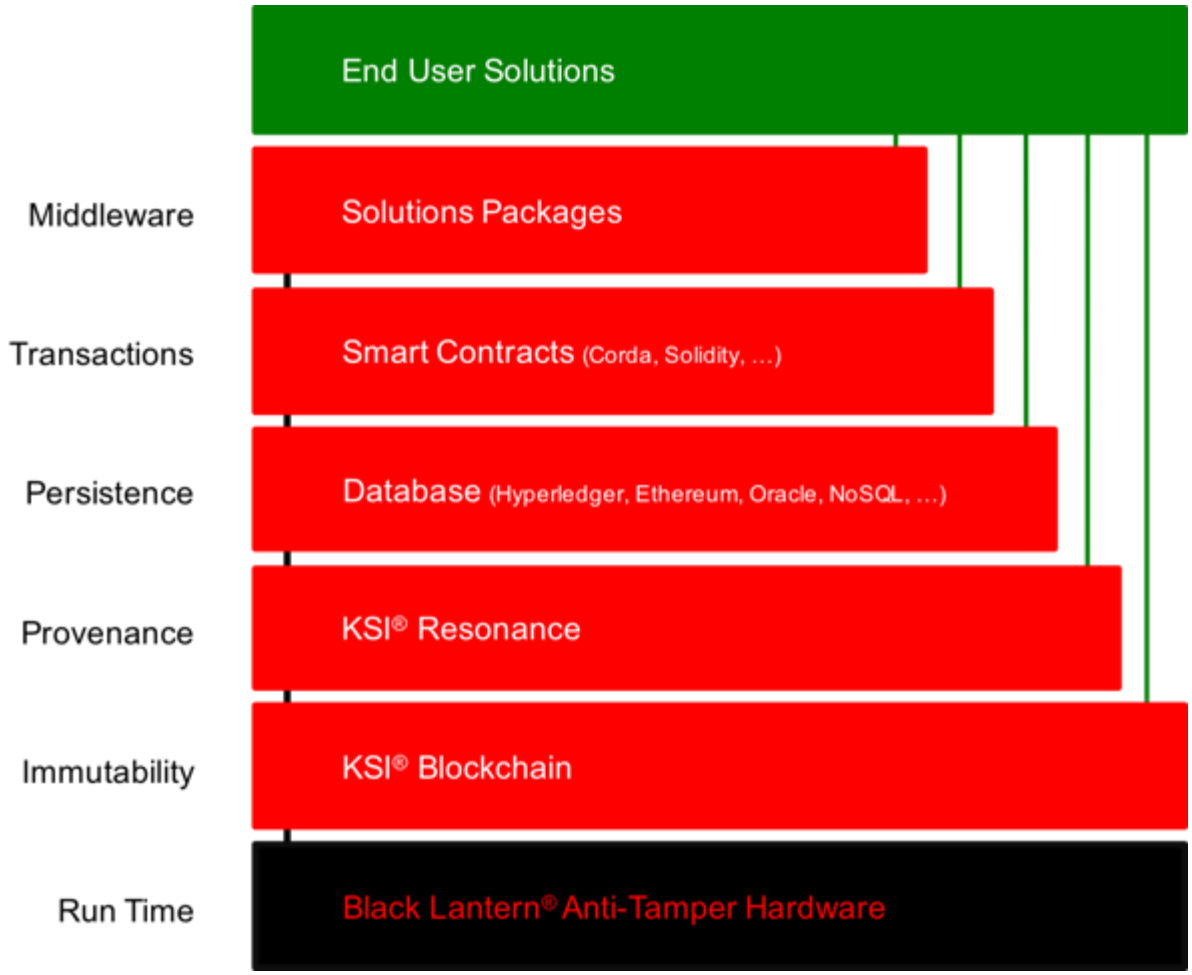
На Фигура 22 е показан технологичният стек на KSI, разработен на база на философията на Unix системите – енкапсулиране на функции в различни нива.

Проектът Verifiable Organizations Network (VON) на Канада

Проектът Verifiable Organizations Network (VON) е съвместно усилие за търсене, издаване и надеждно съхранение на данни за организациите – местни или световно представени. Правителството на Британска Колумбия, Канада използва VON, за да въведе цифровизацията при издаването на правителствени документи – регистрации, лицензи и разрешения. С помощта на съвременни решения, базирани на блокчейн технологиите, VON помага за:

- по-бързо и с по-малко грешки издаване на пълномощия;
- по-сигурно и по-опростено издаване и преиздаване на пълномощия;
- проверка на удостоверения във всяка точка на света.

[123] https://guardtime.com/technology



Фигура 22. KSI технологичен стек[124]

Проектът Verifiable Organizations Network (VON) на Канада

Проектът Verifiable Organizations Network (VON) е съвместно усилие за търсене, издаване и надеждно съхранение на данни за организациите – местни или световно представени. Правителството на Британска Колумбия, Канада използва VON, за да въведе цифровизацията при издаването на правителствени документи – регистрации, лицензи и разрешения. С помощта на съвременни решения, базирани на блокчейн технологиите, VON помага за:

- по-бързо и с по-малко грешки издаване на пълномощия;

[124] https://guardtime.com/technology

- по-сигурно и по-опростено издаване и преиздаване на пълномощия;
- проверка на удостоверения във всяка точка на света.

Целта на проекта VON е да се даде възможност на гражданите и организациите да извършват онлайн бизнес по сигурен начин. Основното предизвикателство е, че в интернет е трудно да се определи самоличността на отсрещната страна. Всяка страна се нуждае от надежден начин да потвърди своята самоличност, по подходящ начин да се потвърди вида на транзакцията, но също така и по начин, чрез който се запазва неприкосновеността на личните данни. Проблемът с "натрапването" се увеличава от нарастването на боря на хакерите, които излагат личните данни на потребителите, като в същото време тези данни биха били полезни при процеса на доказване на самоличността на даден гражданин. Затова е необходим нов подход, който да дава възможност за проверка, че изискуемата транзакция може да бъде извършена от даденият потребител.

Проектът VON се основава на използването на концепцията за Self-Sovereign Identity (SSI). Целта му е да се създаде надеждна цифрова мрежа от проверени данни за организации, като тези данни са свързани, оперативно съвместими, сигурни и лесни за проверка. Това е постигнато чрез блокчейн технологията на основата на Self-Sovereign Identity.

Предизвикателствата при създаване на проекта VON и присъединяване на организации към него са:

- **Доставка:** Съществуващите към момента на стартиране на проекта организации не поддържат „проверими" данни на основата на блокчейн, поради факта, че до този момент те нямат собствен SSI.
- **Търсене:** Организациите нямат нужда от собствени SSI, поради факта, че няма услуги, които да изискват използването му.

Първата имплементация на VON е в т.нар. система TheOrgBook в Британска Колумбия, Канада.

TheOrgBook е цифрова услуга, която предоставя достъп до записи за организации, които са съхранени и проверени. TheOrgBook е създадена като проект с отворен код.

Основните модули са:

- **'TheOrgBook" – BC Businesses:** хранилище от данни за юридически лица, регистрирани и проверими в системата и в Британска Колумбия;
- **"TheOrgBook" – Procurement:** хранилище на данни, съхраняващо проверима информация за обществени поръчки и всички, свързани с това дейности;

- **Supplier Registration:** система за регистриране на доставчици на услугата;
- **BC Registries:** регистър на услугите предоставяни от правителството на Британска Колумбия (в системата).

Двете **основи характеристики** на TheOrgBook са:

- системата съдържа проверени и проверими данни за организациите и юридическите лица;
- правителствени (вкл. и неправителствени) организации които трябва да събират и обработват информация за различни компании с цел извършване на проверки и бизнес с тях, могат да използват TheOrgBook, за да получат тези данни, които са проверени и сигурно съхранявани.

В ПРИЛОЖЕНИЕ 6 са дадени примери за това как изглежда и какво съдържа TheOrgBook.

АНАЛИЗ НА ПРИМЕРИ ЗА ВНЕДРЯВАНЕ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА – ПРЕДИМСТВА, НЕДОСТАТЪЦИ И РИСКОВЕ

Моделът на е-Управление

Съвременните системи за е-Управление, които съществуват в редица страни, са предимно услуги и инструменти за гражданите, достъпни през уеб портал. За да се въведе единна цифрова екосистема е необходимо да има регистър на услугите, регистър на гражданите, механизъм за идентификация на гражданите и система за заплащане на услугите.

Съществуващите системи за е-Управление са огромни по мащаби от гледна точка на изискванията за сигурност, но в същото време са тривиални от архитектурна гледна точка, т.е. централизирано управлявана база данни и набор от приложения, които я свързват с уеб интерфейси. По този начин, въпреки модернизацията на услугите, фрагментацията на държавната машина, големият брой посредници, бюрокрацията и липсата на прозрачност остават.

Блокчейн базиран модел

Технологичната парадигма на блокчейн включва публично и сигурно съхранение и предаване на данни. Данните могат да се предават без необходимостта от централен орган и посредници, но в същото време с гаранция, че участващите страни ще изпълняват задълженията си. Също така данните могат да имат и прогнозна стойност. Това е възможно чрез

използване на блокчейн технологията и интелигентния договор. Потокът от държавни документи, регистрацията на компании, електронно гласуване, обществените поръчки и търгове са някои от областите, нуждаещи се от намаляване на разходите, свързани с обмена на данни и обединяването им в обща система за съхранение.

ПРИМЕРИ ЗА ВНЕДРЯВАНЕ НА БЛОКЧЕЙН

Електронно гласуване: Системата за електронно гласуване може да бъде интегрирана в системата на блокчейн чрез използване на криптография, базирана на елиптични криви. По този начин ще се гарантира точност и надеждност[125].

Администрация на граждани: На основата на интелигентните договори е възможно да се разработи платформа, която да осигури правни и икономически услуги на гражданите.[126]

Обществени поръчки и търгове: Някои от наличните услуги за регистрация и участие в обществени поръчки и търгове могат да бъдат заменени с такива, базирани на блокчейн технологиите. По този начин ще се намали необходимостта от издаване на едни и същи документи за участие в повечето поръчки или търгове. Също така ще има прозрачност и проследимост на процеса на подготовка, участие и изпълнение.

Е-закон: На основата на блокчейн технологията е целесъобразно да се създаде/подобри системата за онлайн публикуване на всички проектозакони, предназначени за обществено обсъждане. По този начин ще се подобри координацията и прозрачността. Потребителите на системата ще имат възможност да виждат кой е предложил законопроекта, неговият текущ статус, предложените промени. Подобна система може да се изгради и за областните и общинските решения за по-големите общини (София, Пловдив, Варна и др.).

Е-правосъдие: Съвременният живот е доста забързан и в отговор на това съдебните процедури трябва да могат да следват това темпо. Това може да стане чрез имплементиране на напълно автоматизирани съдебни процеси и инструменти за електронна комуникация. Това ще доведе до повишаване на ефективността и доверието в съдебната система. На основата на блокчейн технологиите може да се изгради система, която позволява да се проследи едно дело във всеки от неговите етапи. Да се видят съдебните решения и процесуалните действия. Интегрираната

[125] https://followmyvote.com/

[126] http://www.borderless.tech/

система трябва да дава възможност за обмен на информация между всички заинтересовани страни като: полиция, прокурори, затвори, съдия-изпълнители, данъци и такси, граждани и др.

Е-полиция: Идеята за системата е, че осигуряването на възможно най-добра комуникация и координация ще доведе до най-ефективни полицейски услуги. На практика това означава комуникация и координация между всички полицейски управления, патрули и полицаи на улицата. Системата трябва да предоставя на потребителите лесен и опростен достъп до необходимата справочна информация. Също така потребителите трябва да са сигурни, че информацията е навременна, непроменена и актуална. За осигуряване на това „доверие“ е целесъобразно да се използва блокчейн технологията.

Предимства на блокчейн технологията за е-Управлението

Технологията на блокчейн използва неизменим модел за съхранение на данни, което е едно от важните предимства в сравнение с със стандартните бази данни – този подход защитава данните от възможни измамни манипулации. Това означава, че записаните данни за гражданите, компаниите, правата на собственост и т.н., в държавните блокчейн базирани регистри е невъзможно да бъдат променени. По тази причина ще е възможно да се използва информация от тези регистри като стандартни правни документи, доколкото записът в регистъра е с висока степен на надеждност и обществено достъпен.

Основното предимство на блокчейн технологията за е-Управлението е използването на интелигентни договори. Тъй като разпределеният блокчейн регистър съдържа законно валидна информация, много механизми и процедури за взаимодействие между гражданите и държавата могат да бъдат осъществени чрез интелигентен договор. Изходният код елиминира риска от неоторизирани промени и осигурява уникалността на изпълнението на договорния алгоритъм по всяко време и във всяка точка на мрежата.

Една от важните функции на държавата е да съхранява точни данни за гражданите, организациите, активите и дейностите. Блокчейн технологията, основаваща се на принципа на верига от блокове, свързани посредством хеша на предишния блок, прави разпределеният регистър една от най-подходящите среди за съхранение и обмен на данни. Така както крипто валутата и интелигентните договори могат да намалят корупцията и броя на посредниците, така и блокчейн технологията прави всяка транзакция прозрачна и достъпна за преглед от всеки.

ВЪЗМОЖНОСТИ ЗА ВНЕДРЯВАНЕ И ПОДДЪРЖАНЕ НА ПУБЛИЧНИ РЕГИСТРИ НА ОСНОВАТА НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА

Блокчейн технологията по своята същност е технология която гарантира доверие (сигурност в съхранените данни) и прозрачност на транзакциите.

Публичните регистри са един от основните елементи на е-Управлението като те спомагат за интегриране на различи системи и потребители.

За внедряване на блокчейн технологията е необходимо да се отговори на следните въпроси:

- Кои са публичните регистри които подлежат на автоматизация от гледна точка на блокчейн технологията?
- Кои са потребителите на тези регистри и до колко те са е-ориентирани и обвързани?
- Съгласни ли са потребителите на тези регистри да използват блокчейн технологията?
- Как да се регистрират потребителите на регистрите?
- Как по сигурен начин да се достави информацията от регистрите до техните ползватели?

Давайки отговор на тези въпроси и отчитайки спецификата на блокчейн технологията е целесъобразно да се определи множество от регистри, които са най-често използвани, и за тях важат следните изисквания: да бъдат проследими назад във времето и информацията от регистрите да се изисква от множество институции и организации.

В контекста на казаното до тук следва да се отбележи, че към момента не съществува в държавната администрация система, базирана на блокчейн технологии и създаването на такъв тип система ще изисква както финансови, така и организационни ресурси. В същото време това ще доведе до нова философия на работа в държавната администрация и ползвателите на е-услуги, което от своя страна ще изисква усилия за обучение и разяснения.

Използването на сленият подход за идентифициране на публични регистри, при които е възможно да се имплементира блокчейн технологията, ще даде отговор на въпроса кои регистри подлежат на автоматизация чрез тази технология Фигура 23:

- регистърът се поддържа от едно или от множество ведомства;
- регистърът се съхранява централно или разпределено;
- регистърът е необходимо да поддържа данни и назад във времето;

- регистърът не трябва да променя своите данни назад във времето;
- регистърът (справки от него) се ползва от много различни организации;
- данните от регистъра могат да имат и юридическа стойност;
- потребителите на регистъра са юридически и физически лица;
- достъпът до регистъра трябва да е проследим.

Фигура 23. Подход за идентифициране на публични регистри

На базата на така дефинираните изисквания се идентифицира публичният регистър, за който може да се използва блокчейн технология с цел създаване на проследимост, сигурност на данните и прозрачност.

Обобщение

Като обобщение може да се каже, че очевидният ефект от имплементирането на блокчейн технологията и интегрирането ѝ в системата за електронно управление ще повиши ефективността на правителството и управлението, ще намали цената на транзакциите, ще ги направи по-опростени, по-бързи и по-ефективни и следователно по-удобни за взаимодействие между държавата и гражданите. На практика извършването на всяка административна процедура води до записване на определени данни в даден регистър (публичен или не). В резултат на това блокчейн технологията може да се разглежда като уникална и универсална технология, която помага да се рационализират и автоматизират почти всички административни процедури, като същевременно се увеличи прозрачността и ефективността на електронното правителство и електронното управление.

АНАЛИЗ НА ВЪЗМОЖНОСТИТЕ ЗА ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ И ЧАТБОТОВЕ ПРИ ПРЕДОСТАВЯНЕ НА УСЛУГИ И КОМУНИКАЦИЯ С ПОТРЕБИТЕЛИТЕ, КАКТО И ЗА ПОДДЪРЖАНЕ НА КИБЕР СИГУРНОСТТА

ИЗКУСТВЕН ИНТЕЛЕКТ (ИИ) – ИСТОРИЯ, ПОСТИЖЕНИЯ, НАПРАВЛЕНИЯ

Интересът на човек към мислещи машини, както и към формално структуриране и моделиране на знанията ни за света и развитие на формализирани (логически) разсъждения, датира от дълбока древност. Различни представи и истории за мислещи същества, животни и машини, както и свързани с това социални и етични аспекти достигат до нас от древните общества (Египет, Персия, Древна Гърция – например механичният помощник на ковача Хефест). В по-ново време (XVII-XIX век) те преминават през механистичната теория на Рене Декарт, машините на Блез Паскал и Лайбниц (който създава и двоичната система за изчисления), програмируемата изчислителна машина на Чарлз Бабидж и Ада Лъвлейс и приноса на редица философи, математици, инженери и изследователи в областта на неврологията, психологията и теория на информацията и познанието. Не може да не спомена името на създателят на Булевата алгебра – Джордж Бул, който в труда си „Изследване на законите на мисленето, върху които се основават математическите теории на логиката и вероятностите“ (1854 г.) изследва законите и операциите на разсъжденията, които определят човешкия разум и възможността да бъде създаден съответен математически модел[127].

През 1931 г. австрийският математик Курт Гьодел формулира и доказва две важни твърдения – теоремата за непълнота (доказва математически невъзможността за изразяване на цялата истина за дадена предметна област с формални средства) и свързаната с нея Теорема за непротиворечивостта. С тези две теореми той дава „отрицателен“ отговор на поставения от Хилберт „проблем за разрешимостта” с три аспекта – *„Математиката пълна система ли е? Тя хомогенна ли е, т.е. вътрешно непротиворечива ли е? Математиката решима ли е?“* На последният въпрос, макар и частичен отговор, е даден в теориите на Тюринг. През 1936 г. Алън Тюринг опростява определението на понятието формален

[127] https://en.wikipedia.org/wiki/George_Boole

метод, свеждайки го до „Машина на Тюринг“, като формулира и първите алгоритмично нерешими задачи и връзката им с теоремата на Гьодел.

Тюринг се смята за баща на ***съвременната теоретична информатика и теорията на Изкуствения интелект***, като описва и концепцията за „мислеща машина“ (thinking machine)[128], преди още да има компютри в съвременния им смисъл. Той дефинира и класическият „Тест на Тюринг“, който цели да провери дали компютърът проявява „разум“ в човешкия смисъл на думата.

За начална дата на съвременната представа за ***термина „изкуствен интелект“ (ИИ)*** можем да считаме 1956 г., от конференция на група световни учени в Колежа „Дартмут“ (Dartmouth College), посветена на „симулиране на интелект“ (или интелигентност). Формално за „баща“ на термина изкуствен интелект се приема Джон Маккарти[129], автор и на един от основните езици за програмиране на ИИ – LISP, който формулира и дългосрочната цел, и основните методи на ИИ.

Дългосрочната цел на ИИ е ИИ на висотата на човешко ниво. Мисля, че най-добрата надежда за ИИ е логически ИИ, базиран на формализирането на общото познание и разсъждения на базата на математическа логика.

John McCarthy, Stanford University

Father of LISP language, Introduced the term artificial intelligence in August 1955: „The long-term goal of AI is human-level AI.

I think the best hope for human-level AI is logical AI, based on the formalizing of commonsense knowledge and reasoning in mathematical logic.“

Малко преди това писателят-фантаст и философ Айзък Азимов дефинира[130] трите принципа на роботиката, известни като „закони на роботиката“.

Основни школи и първи успехи

Участниците в „Дартмутската“ конференция през 1956 г. са и основателите на основните направления на изследвания в ИИ и ръководят

[128] https://bg.wikipedia.org/wiki/Алън_Тюринг

[129] Нишева М., Д. Шишков. Изкуствен интелект, Добрич, „Интеграл“ 1995, http://megimg.info/mg/modules/booklists/knigi/Comp/Programirane/izkustven%20int.pdf

[130] https://bg.wikipedia.org/wiki/Айзък_Азимов

и развиват главните школи и изследователски центрове за следващите няколко десетилетия – Джон Маккарти (Stanford), Марвин Мински (MIT), Алън Нюел и Хърбърт Саймън (Carnegie Mellon), Артър Самюел (IBM). Всички те са били оптимисти за бъдещето на новосъздадената научна област. Саймън предсказва, че „до двадесет години машините ще бъдат способни да извършват същите действия, които и човек може“, а Марвин Мински е уверен, че само „в рамките на едно поколение проблемът със създаването на изкуствен интелект ще бъде разрешен в значителна степен“.

За да си обясним „бума“ на интереса и инвестициите (а и на редица реални и успешно приложими „интелигентни“ системи) е полезно да се върнем към първите впечатляващи практически успехи и демонстрации на ИИ реализации, които очертават и основните направления (а и школи, световните центрове) за развитие и до днес:

❖ **Логика и доказателство на теореми:** на Дартмутската среща Нюъл, Саймън и Шоу (RAND Corporation) на практика демонстрират *първата програма с ИИ* – „Логик-Теоретик“ (*Logic Theorist*)[131], която е предназначена да доказва теореми в математическата логика. Тази програма доказва 38 от 52-те теореми включени в книгата на Уайтхед и Ръсел „Principia Mathematica“. За първи път се използва „евристичен подход“ (а не по метода на пълното изчерпване) и математическите доказателства се правят на основата на формулиране на догадка за характера на решението и след това се проверява дали догадката е правилна. Друга система, разработена от екипа на Саймън и Нюъл през 1959 г., е „Универсален решавач на задачи“ GPS (*General Problem Solver*)[132], създаден в новооснованата Лаборатория за ИИ в Университета „Карнеги Мелън“, който акцентира върху логическата част и формални разсъждения. През 70-те групата предлага обща методика за създаване на програми, които моделират човешките разсъждения, а през 90-те – обща теория на познанието и когнитивна архитектура (Soar[133]).

❖ **Обработка на естествен език, машинен превод:** практическата цел на това направление е да се постигне по-добро общуване човек-машина. Първите програми, които преобразуват естественоезикови текстове във вътрешномашинна форма и обратно са направени през 1959 г. (Маккарти, MIT). Паралелно се развиват и идеите да се осъществи превод от един естествен език на друг. През 1966 г. Джоузеф Вайценбаум създава програма, която дори изглежда способна да мине през теста на Тюринг.

[131] https://en.wikipedia.org/wiki/Logic_Theorist

[132] https://en.wikipedia.org/wiki/General_Problem_Solver

[133] https://en.wikipedia.org/wiki/Soar_(cognitive_architecture)

Програмата ELIZA работи чрез идентифициране на ключови думи в коментарите на потребителя и прилагане на съответни правила за конструиране на отговор. Ако не бъде намерена ключова дума, ELIZA използва генерични универсални коментари или повтаря модифициран предишен коментар. ELIZA е развита и в посока да симулира поведението на психотерапевт, който не „знае“ нищо за реалния свят. Програмата успява да заблуди доста хора, че те говорят с истински човек, и макар и оспорвано, се приема за първата програма, която би могла да мине теста на Тюринг. Създадената от Колби през 1972 г. програма PARRY се описва като "ELIZA с манталитет" и имитира поведението на параноиден шизофреник. PARRY е тествана със завиден успех в началото на 70-те години с вариация на теста на Тюринг и две групи психиатри. През 1972 г. PARRY „се среща“ с вариант на ELIZA (“Doctor”) и двете програми „разговарят“ чрез прототипа на съвременния интернет (ARPANET). Постигнатите твърде скромни резултати обаче водят до известно замразяване на инвестициите през 70-те години. До края на 80-те години повечето системи за обработка на естествен език се базират на сложни и въведени експлицитно от хора системи от правила, но благодарение на развитието на техниките за машинно самообучение, както и на използването на „концептуалните онтологии“ и съвременни методи, настъпва истинска революция в общуването на естествен език.

❖ **Машинно самообучение:** Терминът Machine Learning (буквално „машинно учене“, но по смисъл е „самообучение“) е въведено през 1959 г. от Артър Самюел134. Алгоритмите за машинно самообучение изграждат математически модел по примерни данни, наречени „обучаващи данни“, за да прогнозират или да вземат решения, без да са експлицитно програмирани за това.

❖ **Възприятие (perception) и компютърно зрение:** През 1969 г. в Станфордския изследователски институт (SIR) е разработен роботът SHAKEY[135] – малък компютър, поставен на комплект от колела и инсталирана камера. Камерата е в състояние да прави оглед на стаята, а компютърът анализира и идентифицира предметите за да се придвижва около тях, с което започват истинските проблеми. Анализът и преобразуването на пикселите от камерата в геометрични форми изисква часове за най-прости линейни модели на стаи (прави линии, квадрати, триъгълници), а повечето тела в реална среда са съвсем неправилни, и триизмерни. Камерите подават двумерна и динамична информация за тези релефи, а програмата разпознава лицата, ръбовете и върховете, заедно със сенките, които трябва да водят към третото измерение. Ограничението

[134] https://bg.wikipedia.org/wiki/Машинно_самообучение
[135] https://en.wikipedia.org/wiki/Shakey_the_robot

е, че програмите, обработващи данните от камерата, фактически обработват поредици от пиксели, които определят като прави линии, триъгълници и други правилни фигури.

Една от основните школи в областта е основана от Марвин Мински и Сеймор Пепърт[136], които поставят основите ѝ в книгата си "Perceptron" (1969 г). През 80-те Мински развива модели на възприятието и разсъжденията в „Общество на разума"[137].

❖ **Роботика и изкуствен интелект:** благодарение на ИИ роботиката претърпява силно развитие. След двата периода на „ИИ зима" (и разочарование от липсата на практически резултати) през 70-те и после в края на 80-те години на XX век, през 1993 г. именно проектът за хуманоиден робот **Cog project** на Масачузетския технологичен институт, който е базиран на Dynamic Analysis and Replanning Tool (DART) се „отплаща" за всички инвестиции в областта от 1950 г. През 1997 г. DeepBlue детронира Каспаров от шах-сцената. Системи, базирани на ИИ, композират различните елементи на интелигентния робот – от сетивата и зрението до сложни решения и планиране на действията, реакция при ситуации, комуникация.

❖ **Експертни системи:** през 80-те години на XX век се развива силно друг клон на ИИ – „експертни системи" – компютърни системи, които наподобяват способността за вземане на решения от човек, експерт в дадена област. Разсъжденията и изводите в тези системи са въз основа на формално описани знания за предметната област („база знания"), а не са процедури и алгоритми, написани от програмист (конвенционалните програми). Експертните системи са сред първите наистина успешни форми на софтуер, разработен на базата на изкуствения интелект. Първите експертни системи са резултат от работата на изследователи от Станфордския евристичен проект (1965 г.), като сред тях са Брус Бюкенън и Рандал Дейвис (създали системите Dendral – за идентифициране на неизвестни органични молекули и Mycin – за диагностика на инфекциозни заболявания)[138]. Те са базирани на правила (представящи експертните знания) и механизми за интерпретацията им (в права или обратна посока – т.е. от данните към заключенията или от целта към данните). Във Франция е разработен и специален език за формално описание на разсъждения с правила или „логическо програмиране" – Prolog[139], който и до днес се използва в много системи за логически извод. Приложни експертни системи в различни направления се развиват в САЩ, Франция, Великобритания,

[136] https://en.wikipedia.org/wiki/Perceptrons_(book)
[137] https://en.wikipedia.org/wiki/Society_of_Mind
[138] https://en.wikipedia.org/wiki/Expert_system
[139] https://en.wikipedia.org/wiki/Prolog

Япония и до днес се смятат за едно от най-успешните направления (макар и терминът „експертни системи“ да е заменен с по-модерни).

Тези направления са условни, тъй като в реалните системи и приложения се използват смесени техники и модели, които стават все по-сложни и разнообразни, в зависимост от знанията за предметната област и видовете задачи, които трябва да се решават. Интерфейсни модули за комуникация на естествен език (реч, ръкопис и текст) се предлагат за всички основни езици. Разпознаването на изображения и обекти, машинното зрение (и „възприятие“), при това в реално време, също вече са стандарт и се предлага в различни варианти – от навигация за домашен робот до сложни медицински манипулации, автономни транспортни средства (които от използване на мисии на Марс и други планети вече „слязоха“ на земята в автомобилите, и под земята в метрото и мините). Машинното самообучение (или още повече – „дълбокото самообучение“) се предлага вече като „услуга под наем“, тъй като изисква огромни изчислителни ресурси и обеми памет.

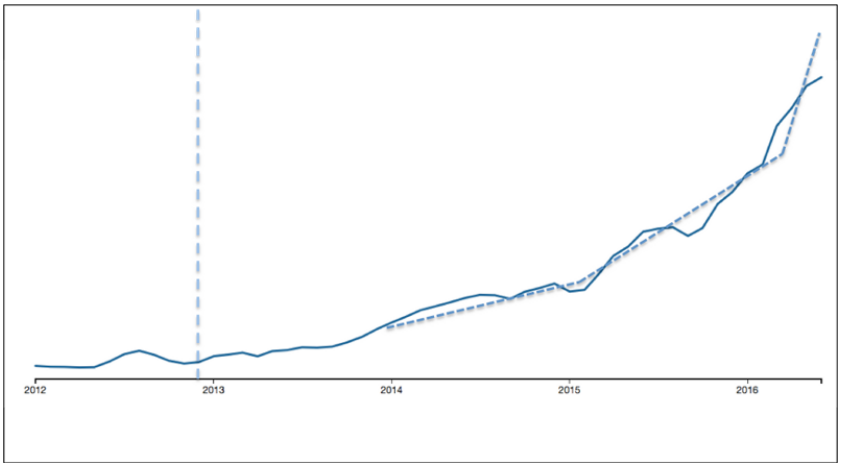
СЪВРЕМЕННИТЕ ТЕНДЕНЦИИ И ТЕХНОЛОГИЧНИ РЕШЕНИЯ ЗА ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ ПРИ ПРЕДОСТАВЯНЕ НА УСЛУГИ

От зората на системните изследвания през 60-те години на XX век, работата и инвестициите в ИИ се движи с приливи и отливи и две характерни „ИИ зими“ през 70-те години и началото на 90-те години. Във всички основни направления са постигнати значителни резултати, като напоследък се заговори за концептуална промяна на парадигмата и дори вече за „зависимостта“ на обществото от цифровите интелигентни системи.

Фактори за навлизане на ИИ от изследванията в реалния живот

Бурното развитие на ИИ се дължи на много причини, но, според експертите, едно конкретно събитие „отключва“ бума през последните 5 години[140] (което има пряка връзка с предмета на настоящото изследване).

[140] https://www.kdnuggets.com/2017/04/brief-history-artificial-intelligence.html



Фигура 24. „Популярност“ на ИИ за периода 2012-2016 г. (CBInsights Trends)

На Фигура 24, се забелязва, че, независимо от всички постижения, до края на 2012 г. интересът към ИИ расте плавно (проучването е направено чрез CBInsights Trends, която от своя страна използва техники за машинно обучение за глобален анализ на популярни думи и теми, както в изследователското, така и в бизнес и публичните новини пространство) – в този случай, анализът е приложен за Artificial intelligence (AI) и Machine Learning. Датата и събитието е свързано с доклад на 4 декември 2012 г. от група изследователи, представен на конференцията Neural Information Processing Systems (NIPS) за използването на конволюционни невронни мрежи, което им е донесло първото място в конкурса за класификация на ImageNet малко преди това[141]. Работата им подобри алгоритъма за класификация от 72% на 85% и сигнализира използването на невронни мрежи за фундаментално за развитието на системите с изкуствен интелект. За по-малко от две години напредъкът в областта донесе класификация в конкурса ImageNet с точност от 96%, малко по-висока от тази на човека (около 95%).

От графиката се забелязват също и три основни тенденции на растеж в развитието на ИИ (прекъсната пунктирана линия), също свързани с три ключови събития:

1) Придобиването от Google през януари 2014 г. на стартиралата три години преди това фирма DeepMind за приложен ИИ на база самообучение;

[141] Krizhevsky, A., Sutskever, I., Hinton, G.E. (2012). “Imagenet classification with deep convolutional neural networks”. Advances in neural information processing systems: 1097–1105.

2) Откритото писмо на „Институт за бъдещето на живота“ (Future of Life Institute), подписано от над 8 000 специалисти с проучването за значението на „дълбоко самообучение с утвърждение“ (deep reinforcement learning), публикувано от DeepMind през февруари 2015 г.[142];
3) Статия в „Nature“ от януари 2016 г.[143] на учени от DeepMind за самообучаващи се невронни мрежи и два месеца по-късно – впечатляващата победа на AlphaGo над Лий Седол, втори в световната ранг листа за играта ГО (GO), както и много други удивителни постижения, обобщени в блога за технологични постижения на Ед Нютон-Рекс[144].

Връзката на този повишен интерес, както и трите идентифицирани знакови събития, с бурното развитие на методите и средствата на ИИ за самообучение не е случайна. В контекста на многократно увеличената изчислителна мощност на компютрите (според интерпретация на Законите на Мур **изчислителната мощност на микропроцесорите се удвоява** на всеки 18-24 месеца[145]), на новите механизми и платформи за **високопроизводителни изчисления** (High Performance Computing), както и на **глобализацията и достъпността на данните** („отворени данни“) и споделяне **структурирани „знания“ в интернет**, те позволяват вече постоянно самообучение и развитие чрез извличане на правила и динамични модели за поведение и решения. Често те са определяни и като „емпирични знания“, базирани или извлечени от анализ на големи масиви от данни (“big data”), цифровизирани сигнали (например от индустриални процеси), „откриване“ на зависимости, разпознаване и класифициране (клъстеризиране) на обекти и информация, както и възможности за непрекъснато усъвършенстване и развитие. Това самообучение и развитие вече е възможно и без наблюдение и реакция на човек-ментор, или поне има смесен характер (като дори успешно се демонстрира обучение на програми от други програми – например генератори на събития или сценарии), а областите на практическо приложение са вече много – от персонален асистент и чатботове, до наблюдение и управление на сложни системи (включително и системи от областта на сигурност и отбрана).

[142] Mnih, V., et al. (2015). “Human-level control through deep reinforcement learning”. Nature, 518: 529–533.

[143] Silver, D., et al. (2016). “Mastering the game of Go with deep neural networks and tree search”. Nature, 529: 484–489.

[144] https://medium.com/on-coding/the-state-of-ai-9aae385c2038

[145] https://bg.wikipedia.org/wiki/Закон_на_Мур

Съвременни методи и техники

Съвременните изследвания в областта на ИИ се разделят в три направления[146]:

1) Информационното направление се основава на методите за създаване на компютърни програми (системи), които автоматизират човешки дейности, смятани за интелектуални. До голяма степен това съответства на представата на Маккарти и колеги от Дартмутската конференция през 1956 г. Тези методи нямат връзка с изучаването на процесите в нервната система на човека при решаването на определени задачи, затова и често водят до „механистично“ копиране на поведението, но без да се постигне някакво „разбиране“.
2) Биофизическото направление се фокусира именно на тези процеси с цел създаване на компютърни модели и съответни програми.
3) Еволюционното направление обединява информационното и биофизическото направление и отчита двата вида „архитектури“ (често силно различни и противоречиви) – на компютърните системи и на човешката нервна система.

На базата на признака дали системите с ИИ имат механизъм за „разсъждение“, който използва формализирана база знания (във формат и съдържание четими, разбираеми и валидирани от хора-експерти) и също така логика или механизъм на разсъжденията, която може да бъде проследена (т.е. имаме отговор на двата принципа – **прозрачност и проследяемост**), можем условно да разделим съвременните системи с претенции за ИИ на два вида:

❖ **Изчислителен изкуствен интелект** (или **„реактивни системи“,** без „разбиране“ по същество и без прозрачен механизъм за логически извод и заключение/действие), които имитират и дори постигат резултати и поведение, сравнимо с поведението, реакциите или заключенията на човек, но най-общо неспособни да отговорят по разбирам за човек начин на въпроса „Защо?“. Тук спадат интерактивни системи с обучение и самообучение (основано на емпирически данни и асоциирани с тях „гъвкави“, но не и „символни“ изчисления) Основни методи са:

- Невронни мрежи – обучавани обикновено с тестови примери и заключения, но имат много разновидности с най-голямо практическо приложение;

[146] Нишева М., Д. Шишков. Изкуствен интелект, Добрич, „Интеграл“ 1995

- Размити системи – методи за разсъждение и извод в условия на неопределеност (използват се „размити“ – fuzzy логики);
- Еволюционни и Генетични алгоритми – използват се механизми и понятия, аналогични на биологията, като популация, мутация и естествен отбор за усъвършенстване на решенията в задачите. Тези изчисления се делят на еволюционни алгоритми, генетически алгоритми и методи на „композитен“ интелект (подобни на сборния „интелект на мравуняка“);
- Обучение с утвърждение – методи за автоматично обучение, отличаващи се със способността си да функционират без необходимост от примерни решения на поставения проблем.

❖ **Конвенционален изкуствен интелект – „интелигентни“ („умни“) системи**, които притежават и двете посочени свойства в различна степен. Най-общо, при тях имаме **представяне на знанията от дадена предметна област** (формализирано, на базата на семантични, когнитивни модели) и **интерпретиране на знанията** (с логически, евристични, асоциативни и други механизми, включително статистически базирани), т.е. те разсъждават „рационално“, а не имитират поведение. Тук попадат методите:

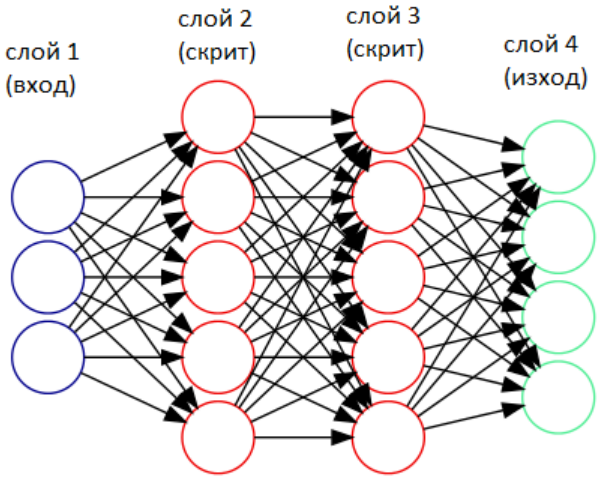
- Експертни системи – програми, които работят по определени правила, отделени в база знания – общи и специфични за предметната област, и използват механизми за обработване на голямо количество информация и правят изводи, заключения, препоръки (могат дори да „вземат решения“);
- Разсъждения по аналогия (Case-based reasoning);
- Мрежи на Бейс – вероятностен графов модел, който представя множество от случайни величини и техните условни зависимости (ориентиран граф без цикли). Например така могат да се представят вероятностните връзки между болести и симптоми, като по дадени симптоми мрежата може да се използва, за да се изчислят вероятностите за наличието на различни болести (подобно на експертната система MYCIN, описана по-горе);
- Дърво на решенията – използването на логически графи за връзки/асоциации и различни методи за търсене в тях (на решение);
- Поведенчески подход – системите се разделят на сравнително автономни модули, които си взаимодействат в зависимост от средата.

Очевидно втората група е по-близо до общата концепция за ИИ, но за съжаление тя е все още далече от задоволително пълна и практически

полезна реализация, макар да има значителни успехи в различни направления. Повечето от споменатите успехи в последното десетилетие попадат условно в първата категория, което изобщо не принизява или омаловажава тяхната полезност и приложимост, а е съществена крачка от научно-изследователските прототипи към хилядите системи, които вече ни помагат.

Ето някои от основните техники, които променят вече живота, услугите и бизнеса:

❖ **Невронни мрежи (изкуствени невронни мрежи) машинно самообучение** – получили името си от аналогията или асоциацията с механизма на разпространение на сигналите (нервните импулси) в мозъка на човек, но това е математически модел, който не моделира тези биофизични процеси. Най-обща представа за механизма на действие на невронните мрежи е показана на Фигура 25. В мрежата условно има входен слой (от неврони), няколко междинни (скрити), и изходен слой. Всеки неврон приема "сигнали" от предхождащите го в мрежата (числа), „сумира ги“ и извършва аритметични действия, в съответствие с функцията си на активация и изпраща сигнали към следващия слой. Всяка връзка има тегло, което, умножавайки се със сигнала, определя неговата значимост (сила). Теглата могат да усилват или потискат сигнала. Чрез промяна на теглата се извършва „обучение“ или „самообучение“ на мрежата. Има десетки разновидности на мрежите.



Фигура 25. Общ изглед на опростена невронна мрежа.

❖ **Машинно самообучение**[147] (Machine Learning) – използва различни техники и теоретични модели за развитие на „изчислителния тип ИИ“ към този на „правдоподобните разсъждения“. Както отбелязахме, именно тяхното развитие през първото десетилетие на този век води и до големия „бум“ на инвестициите и възобновения интерес към ИИ. Използват се два основни подхода за самообучение, както и смесени модели от двата типа:

- *самообучение с учител* (Supervised Learning) на базата на обучаващи данни и „тренировка“ от обучаващ;
- *самообучение без учител* (Unsupervised Learning) – алгоритъмът построява математически модел на съвкупност от входящи данни, които не съдържат указания за желаните резултати. Използва се за откриване на структура в данните, например групиране или клъстерен анализ. Самообучението без учител може да открива закономерности в данните и да групира входовете в категории, например при извеждане на признаци.

❖ **Дълбоко обучение/самообучение** (Deep Learning) **–** ново развитие на самообучението (на база невронни мрежи), известна още като дълбоко структурирано обучение, „дълбоки“ невронни мрежи или йерархично обучение. То също е базирано предимно на данни за учене, вместо алгоритми, специфични за задачите. Дълбоките невронни мрежи имат много повече слоеве, позволявайки на системата да работи с много по-големи и по-сложни масиви от данни, като изображения, видео, текст и аудио, за да се идентифицират по-фини модели, за които се изисква и голям изчислителен ресурс за да се интегрира специфична информация за проблема. Въпреки слабата (или недостатъчно изучена) теоретична база, практическите резултати и постижения са впечатляващи, използвани в следните области (в които се смята, че точно дълбокото самообучение е доминиращо за 2018 г.)[148]:

- Автономни автомобили (self-driving cars);
- Здравеопазване;
- Гласова комуникация, търсене и гласови команди;
- Автоматично „озвучаване“ на неми филми;
- Автоматично генериране на текст (включително и ръкописен);
- Разпознаване на изображения;
- Автоматично „описание“ на изображенията (с разпознаване);

[147] https://bg.wikipedia.org/wiki/Машинно_самообучение

[148] https://medium.com/@vratulmittal/top-15-deep-learning-applications-that-will-rule-the-world-in-2018-and-beyond-7c6130c43b01

- Оцветяване на фотографии/филми;
- Реклами (персонализирани, фокусирани);
- Предсказване на земетресения;
- Ранна диагностика на мозъчни тумори;
- Финанси и финансови услуги;
- Предсказване на цените на пазарите на енергия.

❖ **Обучение с утвърждение**[149] (Reinforcement Learning) – един от най-популярните и перспективни за момента методи, който не изисква обучение с примери и ментор, а „извлича“ правила и знания за правилните или по-точно „добри“ решения на базата на принципа „награда“, като постоянно се усъвършенства. Именно на негова база DeepMind създават AlphaGo и AlphaZero, предизвикали успешно световните шампиони на играта Го и шах. В основата си тези методи се базират на известните вериги на Марков и процеса на Марков (използвани за вземане на решение въз основа на вероятностен модел). Популярната илюстрация на тези методи е аналогията с дресировка на куче. С всяка следваща стъпка системата се самоусъвършенства на базата на удовлетвореността (не непременно от ментора) на предната стъпка/решение. А по-модерната илюстрация е със самообучението на „интелигентна прахосмукачка“ (един от най-успешните брандове Roomba е на фирма с даденото от Айзък Азимов име „I, robot”). Базовите модели на така наречените „vacuums” използват простите и много продължителни методи на самообучение по метода „проби и грешки“, но по-развитите разпознават сцените и предметите, изготвят сами карта на помещенията и „решават“ кои зони да почистват, кога да спрат почистването, и нещо много важно – как да избягват менящите се динамично зони, където са домашните любимци (за робота често равносилни на „самоубийство“).

❖ **Комуникация на естествен език, автоматичен превод –** В продължение на изследванията от миналия век, в края на 90-те години се създава програмата за гласово разпознаване ViaVoice. В една от последните си версии може да трансферира текста в текстообработваща програма. Понастоящем, като отделна много широка област се развива „компютърната лингвистика“ и комуникацията на човек с компютърни системи на естествен (или ограничен естествен) език, развиват се модели и методи за обработка на естествен език (NLP – Natural Language Processing), които интерпретират семантиката на езика и позволяват неговото „разбиране“ на базата на концептуални онтологии. Практически всички системи вече разполагат със стандартни интерфейси и модули за преобразуване на реч към текст и обратно на основните естествени

[149] https://bg.wikipedia.org/wiki/Обучение_с_утвърждение

говорими езици, което позволява машинен превод в реално време. Възможни са различни варианти: човек-машина, човек-машина-човек на различни езици, при това писмено и говоримо, т.е. пълната схема става:

Реч(език1)<>Текст(машина:език1)<>Текст(машина:език2)<>Реч(език 2)

Тези услуги се предлагат и в „облачна среда“ и единственото, което ви е необходимо за да ги използвате, е бърза връзка с интернет. Измежду лидерите в услугите и приложенията за автоматичен превод са: Google Translate – със 103 езика (52 оф-лайн), Microsoft Translator, Baidu и много други (вкл. и специализирани за мобилни платформи). Все по-голяма част предлагат и гласова комуникация (но с различно ниво на достоверност). Важно е да отбележим и всички проблеми с конфиденциалността – доколкото повечето платформи са „облачни“ и използват тази сила за самообучение, то и цялата информация и разговори са евентуално уязвими за изтичане, манипулация, злоупотреби. Това се отнася и за „интелигентните“ асистенти на умните мобилни платформи – Siri, Cortana, Google Assistant, Alexa и над 30 приложения за Android, голяма част рекламирани като „изкуствен интелект“.

Чатбот или „интелигентен виртуален асистент“? Тест на Тюринг

Тестът на Тюринг, формулиран през 1950 г., в различни варианти стана изключително популярен и актуален напоследък във връзка с развитието на „чатботовете“ (известни също като smartbots, talkbot, chatterbot, интерактивен агент, разговорен асистент, събеседник, разговорен интерфейс и др.). Това са „компютърни програми или системи с изкуствен интелект, които могат да провеждат диалог/събеседване с човек чрез текстови или гласови съобщения на естествен език“[150].

Оригиналният „тест на Тюринг“ цели проверка дали компютърът проявява „разум“ в човешкия смисъл на думата. Тюринг предлага този тест, който да замени безсмисления според него въпрос „Може ли машината да мисли?“ с по-формален тест, който най-общо се състои в следното: ***Човек (жури) взаимодейства дистанционно с двама събеседници – компютър и човек, като само въз основа на отговорите на своите въпроси трябва да определи с кого разговаря – с машина (изкуствен интелект/компютърна програма) или с жив човек.***

[150] https://en.wikipedia.org/wiki/Chatbot

Следователно, задачата на компютърната програма (т.е. на нейните създатели) за да премине **теста на Тюринг**, е да заблуди човека-жури, имитирайки естествен диалог и поведение. Този тест по същество е разновидност на „играта на имитация“ (Imitation game)[151] и на практика проверява способността да се имитира човешко поведение и реакции, а не извършване на интелигентна дейност. Или за да мине теста, машината би следвало да може да имитира и **„неинтелигентно“ човешко поведение** (т.е. да прави типични човешки грешки, включително и правописни, дори да „лъже“, да е „глупава“ или „наивна“), да реагира отрицателно на обиди, както и **да не проявява свръх-интелигентност** или **супер-информираност** (например да решава сложни задачи, да прави сложни и прецизни изчисления, да демонстрира енциклопедични познания и т.н.).

Тези особености дават основание да се замислим за използването на термина „чатбот“ за описване на услуги, които държавата и бизнеса би искал да предостави на своите потребители и клиенти. Очевидно не става дума за **„имитация“ на разговор** (с човек), а за „разбиране“ и рационално („разумно“) предоставяне на информация, отговор, насоки и препоръки. Гражданите не очакват от подобна услуга да бъдат „заблуждавани“ или да получават понякога „глупави“ отговори (което би се случило, ако наистина целим машината да мине теста на Тюринг). В повечето случаи се използват по-коректните термини – ***„виртуален асистент (с ИИ)“***, или ***„интелигентен (виртуален) асистент“***. Поради придобилият гражданственост термин (което се подсилва и от имената на самите технически платформи и средства – рекламирани точно като „умни“ чатботове), ще продължим да го използваме, но препоръката е винаги да подчертаваме смисъла на ***„интелигентен асистент“***, а не на имитатор-събеседник.

Известните приложения могат най-общо да бъдат характеризирани като:

- **Интелигентен Help**, както и справочник за съдържание, често задавани въпроси/отговори (включително и чрез гласова комуникация);
- **Асистент/навигатор** за услуги – за фиксирани сценарии или списъци от услуги, техника на „водене по менюто“;
- **Комплексни „динамични“ услуги** – на базата на интерактивен диалог, уточняване на отделните компоненти, динамично „сглобяване“ на услугата и съответните документи, инструкции и процес на изпълнение. Изисква силно формализиран механизъм и развита „семантика“ на описание на услугите, както и наличието на такива „комплексни услуги“ (по смисъла на нормативната уредба на „Електронното управление“);

151 https://en.wikipedia.org/wiki/Turing_test

❖ **Профилирани/персонализирани услуги** – идентифициране на тип клиент (гражданин/организация) и тип дейност, „водене“ на диалог на базата на персонален (или избор от типизиран) профил.

Могат да бъдат отбелязани редица **предимства на „чатбота“** – в сравнение с обслужването от човек, чатботът е:

- Винаги търпелив, внимателен, любезен;
- Не се „обижда“, няма главоболие;
- Кооперативен, ненатрапчив, следващ еднотипен фиксиран разговор „по рецепта/меню“;
- Обучаем (както от ментор, така и от клиентите – тук следва да сме много внимателни поради възможни манипулации и атаки, както са посочените в следващата част примери със самообучаващите се ботове на Майкрософт и Фейсбук);
- Напълно проследим и „отговорен“ за стъпките на диалога и отговорите;
- Може да е сравнително успешен „психолог“ (дори с чувство за хумор, забавен);
- Многофункционален („поливалентен“) – има достъп до различни „бази знания“ и информация, енциклопедичните познания на целия интернет (но трябва да се има предвид това „предупреждение“ от теста на Тюринг – за опасност от смазваща свръх-информираност);
- Лесно се „клонира“ / мултиплицира (база знания) и адаптира (към нови области/услуги), „преквалифицира“;
- Адаптивен – може да адаптира диалога към идентифициран тип потребител (попадащ в идентифицирани категории с помощта на самообучение, или при зададени критерии) – така ще води разговора в полезна за потребителя посока, и ще дава „отговори с предсказване“;
- Може да помогне съществено за подобряване на качеството на самите услуги – да помага (събира системно информация) за:
  - Идентифициране на липсващи услуги или информация – при експеримент с онлайн услуги в Берлин, чатботът идентифицира и изготвя системна справка за потърсена и липсваща информация или вид услуга, докато операторите-хора не са отбелязали нищо за такива заявки;
  - Оптимизация на услуги (включително събиране/използване на Big Data);
  - Профилиране на клиентите (поведение, интереси) – запазване на анонимност.

Примери за използване на интелигентен асистент или чатбот в е-услуги

Световните примери за използване на чатботове (използваме този разговорен термин, макар и вложеният в него смисъл да е **„интелигентен виртуален асистент“)** показват ясно ползите, но и идентифицират част от практическите проблеми (не само от морално-етично естество).

Ето някои успешни и поучителни истории на държавни агенции, пионери в прилагането на ИИ и чатботове за услуги[152]:

❖ Имиграционните служби на щата Масачузетс (Department of Homeland Security) използва чатботът **EMMA** – виртуален асистент помагащ на хората за искания, свързани с имиграционни услуги, зелена карта, паспорти и всяка услуга, предлагана от този отдел. EMMA използва испански или английски език, като на английски комуникира и гласово. Дава пълна информация за отдела и услугите и асистира навигацията в уеб сайта с услуги. Обработва месечно над 1 милион заявки.

❖ Чатботът **MISSI** (щата Мисисипи, САЩ) помага на жителите и посетителите да се запознаят с всяка информация относно щата, както и да споделят мнения, използват се чат съобщения или гласова комуникация през асистента на Amazon – Alexa (приложението "Ask Mississippi"). Помага на граждани и бизнес по въпросите на данъчното облагане, здравни услуги, обществен транспорт, семейни услуги, възможности за работа и други, както и с места за посещение и актуални събития.

❖ Администрацията на Сан Франциско използва асистент **PAIGE** (Procurement Answers and Information Guided Experience). PAIGE помага на служителите в правителствените агенции за цифровизирания процес на възлагане на обществени поръчки. Използва услугата за обработка на естествен език (NLP) на Facebook (wit.ai).

❖ Правителството на Канзас Сити предлага услугите на чатбота **OpenDataKC** за да ориентира потребителите в отворения портал за данни, който се е разширил толкова много, че практически е станал неизползваем за хора и бизнес. Използва се приложението на Facebook (messenger chatbot).

❖ Администрацията в Лос Анджелис използва **CHIP** (City Hall Internet Personality), който съветва за възможностите за бизнес в областта. Базиран е на облачната платформа на Майкрософт – Azure Bot. Друг чатбот – L.A. Alexa отговаря на всякакви въпроси за събития и новини в града (използва платформата Amazon Alexa).

[152] https://blog.vsoftconsulting.com/blog/15-governments-agencies-that-use-chatbots

❖ Държавната администрация на САЩ използва кооперативния бот **Mrs. Landingham** – една от иновативните инициативи от програмата за цифровата трансформация на правителството/администрацията на САЩ. Подпомага всички назначени (и нови) служители за ориентиране във вътрешно административните процеси (формуляри, услуги, срещи, и др.), услугите между различни агенции и администрации.

❖ Националната служба за електричество и вода в Дубай използва асистент **RAMMAS** върху Google AI Platform за поддържане на 24/7 услуги (консултации, изискване и плащане на сметки), достъпен по различни канали – през сайта на службата, приложения на IOS, Android, Amazon Alexa, Facebook, дори като физически робот-асистент. От старта си през 2017 г. е обработил близо 1 милион заявки по различни канали.

❖ **Gov.sg** е чатбот на Министерството на комуникациите и информацията (MCI) на Сингапур, който помага на граждани и посетители да намерят лесно информация за правителствените агенции, новини, прессъобщения, възможности за работа и политики. В платформата могат да се подават и проследяват оплаквания във връзка с пропуски в някоя от обществените услуги. Чатботът сам извлича и използва информацията от портала за публични услуги на правителството.

Машинен превод и публичната администрация

Специално внимание заслужава примерът с Европейската комисия (ЕК). Още в периода от 1970 до 1994 се работи по финансиран от ЕК проект Eurotra за превод между езиците на Европейския съюз (ЕС). Проектът тогава не успява да достигне до практически използваем продукт, но работата по него повлиява положително на изследванията и разработките в областта на „машинния превод“ в отделните страни-участнички.

От 2017 г. през портала на ЕК Connecting Europe Facility (CEF) работи с голям успех ***eTranslation***[153] услуга (машинен онлайн превод) на документи на 24-те официални езика на ЕС. Освен автоматичен превод на официалните документи на ЕС, тази услуга може да се използва за:

- Еднократни свободни преводи на текстове (интерфейс човек-машина);
- Услуга, достъпна за различни цифрови услуги през специален интерфейс API (Application Programming Interface).

[153] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Machine+Translation

Опитът на е-гражданин на е-Естония

Показателен е и успехът на асистентът на Естонският правителствен „стартъп“ – **e-Residency**[154]. Тази малка организация управлява пилотната програма за е-гражданство на е-Естония (виртуални граждани на виртуална-реална държава), която от старта през декември 2014 г. има близо 40 хиляди е-граждани, регистрирали над 3500 фирми, но само за 2018 г. се очаква близо 100% увеличение на заявките. За да се справи с драматичното увеличаване на интереса и свързаното с това обслужване на заявки от цял свят за е-гражданство, отговори на въпроси и справки, както и за условия за бизнес, организацията внедрява виртуален асистент, използващ ИИ. Въпреки очакването за успешно обработване на 10-20% от въпросите, само за няколко месеца асистентът постига близо 50% успеваемост с методите на „самообучение“. Създателите подчертават следните предимства:

- При добра реализация нивото на обслужване (и успеваемост) постоянно се подобрява (на моменти над 60%);
- Сложните случаи се идентифицират и предават на човек автоматично;
- ИИ става все „по-умен“, и работи 24/7, не се разболява и не ползва отпуск;
- Спестява над 50% от средствата за обслужване – създателите са разработили дори програма, която показва спестяванията от ползването на чатбота – https://chatcreate.com/.

Чатботът е по-добър от уеб-сайт

Проведено изследване с административните услуги в Милано[155] показва, че чатботът **далеч превъзхожда уеб-базирана консултация по показателите прозрачност и ефективност**. Ако питаме чатботът по правилен начин, пълен отговор се получава за много кратък срок, докато за намиране на отговор в традиционния уебсайт се изискват повече усилия. В уебсайтовете потребителите се нуждаят от време, за да се ориентират, чатботът използва стандартен интерфейс за online messaging, познат за повечето хора. Взаимодействието с чатбот е средно до 3 минути по-бързо от това с уебсайтовете. И не на последно място – близо 50% от тестваните потребители не са успели да намерят информацията или завършат сесията през стандартния уебсайт, докато с чатбот **успеваемостта е 100%**. Все пак,

154 https://medium.com/e-residency-blog/how-we-use-ai-to-help-users-get-answers-instantly-and-increase-customer-satisfaction-95d1a06caad

155 Valtolina, S., Barricelli, B.R., Gaetano, S.D., & Diliberto, P. (2018). Chatbots and Conversational Interfaces: Three Domains of Use. CoPDA@AVI. – достъпна на: http://ceur-ws.org/Vol-2101/paper8.pdf

известно предимство има показателят „доверие“ към лично намерена информация през уебсайта, като се отчита и психологическата бариера с новата форма на консултация с „машина“.

е-Правителство и изкуствен интелект – нива на зрялост

Логично, а и видимо от анализираните примери, съществено условие за успешното развитие и прилагане на ИИ в сферата на услугите (публични и бизнес) е услугите да са „цифровизирани“, т.е. да е извършена цифровата трансформация в съответните организации, сектори и екосистеми. В сферата на публичните услуги това означава да е изграден поне фундаментът на общото електронно управление (е-управление) и основните услуги за администрация-граждани, администрация-бизнес и администрация-администрация (известни като G2C, G2B и G2G, съответно и застъпени в „Стратегия за развитие на електронното управление в Република България 2020“[156] и съответните нормативни актове за изпълнението ѝ). Наличието и актуалното поддържане на единни регистри с информация за субекти, данни и електронни услуги, оперативна съвместимост на системите, стандартизирани протоколи за данни и услуги, както и не на последно място – тяхната защита и кибер сигурност и устойчивост, е необходимото условие за изработване на формализирано описание на „знанията“, методи и правила за тяхната интерпретация, които са базата на методите и средствата на ИИ.

В „Талинската декларация“[157] на министрите на е-управлението от октомври 2017 г. се призовава за изучаване на добрите практики и прилагане на стандарти за прилагане на трите бързо развиващи се направления на ИКТ – анализ на данни, **изкуствен интелект** и блокчейн.

Нива на зрялост на е-услугите – от автоматизация към „интелектуализация“

На 19 юли 2018 г. ООН представи своето ново изследване на електронното управление на страните членки на ООН[158]. Изследването представя индекс за държавите членки, който измерва степента на употреба и ползваемост на информационни и комуникационни технологии (ИКТ) за предоставяне на публични услуги на гражданите. В сравнение с 2016 г., България се е изкачила в класацията с 5 места – от 52-ро място през 2016 г. до 47-мо място. Във връзка с индекса на ООН, както и на

[156] https://www.e-gov.bg/bg/41

[157] https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration

[158] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018

национални стратегии и стандарти, има над 20 модела за „нива на зрялост“ на електронно управление/правителства (от 3 до 6 нива). **Моделът за „класация“ на ООН** има 4 нива:

Първият етап е услугата **„нововъзникваща информация“**: на този етап уеб сайтовете за електронно правителство предоставят статична информация.

Вторият етап е **„подобрени информационни услуги“**: на този етап присъствието се подобрява с еднопосочна или проста двупосочна комуникация.

Третият етап е **„транзакционни услуги“**: в този етап е възможно двустранно взаимодействие с гражданите.

Четвъртият етап е **„свързани услуги"**: на този етап уеб сайтовете проявяват активна роля при искането на обратна връзка от страна на гражданите чрез средствата на Web 2.0. Държавните агенции са ориентирани към гражданите и услугите са ориентирани към клиентите.

По-показателни са нивата и моделите на „зрялост“, базирани на нивата, използвани от ИТ и цифровата индустрия (и приложими и на ниво държава и услуги), например **нивата на зрялост, предложени от Gartner**[159] (много близки до нивата на зрялост от модела CMMI на Карнеги Мелън) с цел да ги свържем с тяхната интелектуализация (и прилагане на ИИ):

Ниво 1 – **Първоначално** („информационно“ електронно правителство) – фокусът е върху преместването информация и услуги онлайн за удобство на потребителите и спестяване на разходи, но информацията и базови (справочни) услуги са на „силози“ и ограничени. Други модели го определят като „каталог“, налична и достъпна информация за услуги (естествено, изисква и работещи услуги).

Ниво 2 – **Развитие** (отворено е-правителство) – програми, насочени към обществото, към насърчаване на прозрачността, ангажираността на гражданите и цифровата икономика (data economy), често в контекста на програми за интелигентни градове, например.

Обемът и потокът от данни в публичните административни услуги се увеличава и непрекъснато обогатява, във връзка с въвеждане на нови услуги и комбинирането на основни услуги в комплексни, но все пак стандартизирани услуги. Нарастващият обем и интензитет в контекста на обичайните финансови ограничения правят автоматизирането на тези услуги едно от първите приоритетни полета за ИИ. Така ИИ е не само пожелание, а се превръща в необходимост. Водещите държави в областта

[159] https://www.gartner.com/smarterwithgartner/5-levels-of-digital-government-maturity/

на е-управлението вече са реализирали пилотни, а някъде внедрили като стандартни услуги, базирани на ИИ технологии. Повечето приложения варират от автоматизирането на отнемащи време административни задачи (например, въвеждане и обработка на различни и обемни данни) до способността да се отговори на заявките за потребители в реално време (например, различни видове чатботове). Така основните изтъквани предимства са ограничени до стремежа за оперативна ефективност, като:

- Намаляване на публичните разходи;
- Повишаване производителността и бързината за изпълнение на задачите;
- Освобождаване на квалифициран човешки ресурс за решаване на по-сложни задачи и предоставяне на директни услуги.

Ниво 3 – **Дефинирано** (Data-Centric) – фокусът се премества от „изслушване“ на нуждите на гражданите или потребителите към проактивни услуги, идентифициране и развитие на нови възможности, например свързани със стратегическото събиране и използване на данни. От първостепенно значение е фокусът към разработването и прилагането на стратегии и процеси, базирани на данни.

Ниво 4 – **Управлявано** (напълно цифрово, можем да го определим като **„интелектуализирано“**) – организацията, агенцията или отделът се ангажира изцяло с подход, основан на данните, за подобряване на управлението, а предпочитаният подход към иновациите се основава на принципите на отворените данни. На този етап са възможни затруднения, свързани с *неприкосновеността на личния живот, събирането и използване на данни.* Важно да се гарантира, че данните се използват в рамките на съществуващите норми и разпоредби. Въвеждат се услуги с добавена стойност, които не се предоставят на базата на човешките знания и възможности (на базата на big data, data analytics, адаптивни сценарии и др.) – типичната сфера на ИИ.

Ниво 5 – Оптимизиране („интелигентно“ е-правителство) – иновациите, използвайки отворени данни и цифрови методи и средства, са вградени в основата на държавното управление, с лидерство от най-високо политическо равнище. Процесът на иновации е предвидим и повторяем, дори и в случай на извънредни събития и ситуации.

В модела за електронно управление в България се споменават термини от категорията на ИИ (напр. „семантична“ съвместимост на системите), но не са посочени ясно нивата на амбиция и предлаганите

услугите (целевите нива на зрялост, което е основна задача на пътната карта)[160].

ПРАВНИ, ЕТИЧНИ И СОЦИАЛНИ ПРЕДИЗВИКАТЕЛСТВА ПРИ ИЗПОЛЗВАНЕТО НА ИИ И ЧАТБОТОВЕ

От фантастика към реалност – закони на роботиката

Писателят-фантаст, философ и визионер Айзък Азимов за пръв път систематизира принципите на съжителство на човек с интелигентни машини (през 1941 г. и публикувани отново в сборника „Аз, Роботът“ през 1950 г.), известни като „закони на роботиката“:

1. Роботът не може да причини или с бездействието си да допусне да бъде причинена вреда на човека.

2. Роботът трябва да се подчинява на командите, които му дава човекът, освен в случаите, когато тези команди противоречат на Първия закон.

3. Роботът трябва да се грижи за своята безопасност, ако това не противоречи на Първия и Втория закон.

По-късно Азимов добавя и **„нулев закон“** – Роботът не може да причини вреда на човечеството или с бездействието си да позволи на човечеството да му бъде причинена вреда.

В развитието им има и български принос – Любен Дилов (баща) добавя и **четвърти закон** – *Роботът трябва винаги да се представя като такъв.*

Както и **пети закон** (от Никола Кесаровски) – *Роботът трябва да знае, че е робот.*

Макар и предмет на научната фантастика, тези шест закона очертават и основните морални, етични, социални и правни предизвикателства пред съвременното общество. Те са напълно приложими (разбира се с уточнения) в реалния живот днес. На практика различни форми на интелигентни машини, програми, устройства вече заемат немалка част от бита, ежедневието, здравето, бизнеса, сигурността и държавното управление, цялото общество. Говорим не само за „цифрова зависимост“ (т.е. цифровият бизнес и софтуерът „изяжда“ света, както се изрази един от пионерите на съвременното общество – Марк Андресен), но и вече до

[160] Христов, Х. (19 02 2015 г.). Електронно управление в Р България. София, България.

известна степен го „управлява“, именно чрез използването на методи и средства на ИИ (пак той)[161].

Основни аспекти на дискусиите (и необходими действия, макар и леко закъснели), които се провеждат, включително и в Европейската стратегия за ИИ, и създадената през юни 2018 г. от ЕК специална Група на експерти от високо ниво, за разработване на план за развитие на ЕС в областта на ИИ, са:

- Принципи, норми:
  - Прозрачност;
  - Проследимост на действията и решенията (и на данните);
  - „Обяснимост“ на решения (логически стъпки – тук силна критика търпят обаче най-популярните засега техники на „невронните мрежи“, които са своеобразни „черни кутии“ по отношение на заключенията си);
  - Изясняване на отговорността за действия/решения;
  - Правоприлагане и „наказание“ за грешки (което силно се различава от въпроса за грешки/дефекти в софтуерни и ИТ продукти) – например при грешна диагноза, грешка на автономни автомобили, дронове и др. с фатални последствия за човек (с цялата сложност на материята).
- По отношение на хората, работа, заетост и професии:
  - Замества, не „измества“ човек;
  - Разширява, не ограничава дейностите и възможностите на човек.
- Обществото поставя ясни граници, които не могат да се преминават – „Red lines“.
- Наличието на „паник бутон“ – възможност за аварийно изключване. Специалистите алармират, че не всички процеси се „изключват“ безопасно, например при производство, дронове и автомобили, медицински грижи. Грижа за осигуряване на безопасността, минимални функции, както и „кой“ има право да го натисне. В някои сфери само машини биха могли да обхванат и следят сложната дейност на други машини (с ИИ).
- И по-общо – гарантирана възможност за контрол от човек. Напоследък защитниците на тезата за „пълен контрол над роботите“ дават за пример нашумелия през юни 2017 г. случай с чатбота на Facebook (FAIR – Facebook AI Research). Това по същество е научно изследване за развитието и самоусъвършенстването на два екземпляра на чатбот програмата (Алис и Боб, наречени неслучайно с популярните за

[161] https://a16z.com/2016/08/20/why-software-is-eating-the-world/

криптографите имена на комуникиращи си с шифър агенти). Самият чатбот се създава за целите на подобряване на чат-платформата на социалната мрежа – Facebook messenger. Медиите тиражираха „новината“ за аварийно спирането на ботовете поради отклоняване на комуникацията от първоначалните области („обучени“ чрез много примери на човешки комуникации в месинджъра) и най-вече заради „изобретяването“ от ботовете на нов език за комуникация между тях, неразбираем за инженерите. Истината е малко по-различна – наистина в някои моменти комуникацията се е отклонявала от стандартния английски език, но това не е нов, неразбираем език. Същината на изследването е да се накарат агентите да преговарят по-ефективно. Изследователите отбелязват, че агентите наистина са „измислили“ как да симулират интерес към неща, които на практика не ги „интересуват“, заради разговора. Подчертава се, че това е само експеримент по отношение на алгоритмите за самообучение и няма за цел практическо приложение и „заблуда“ на потребителите с ботове[162].

❖ Отговорност на „учителите“ (или обучаващите алгоритми, хората): Друг случай поставя много по-сериозен проблем – за качеството и „морала“ на данните и средата за обучение на чатботовете, както и отговорността на обучителите и менторите. Това е ботът “TAY” (Thinking About You) на Майкрософт, който при първото си активиране в мрежата на Tweeter, и самообучаващ се при комуникацията с хора, само в рамките на 16 часа през март 2016 г. става „анти-семит“ и започва да използва обидна фразеология (сексуално-ориентиран или със садо-мазохистичен жаргон), като генерира над 96 000 съобщения. Това принуждава създателите му да го изключат и да се постараят да изтрият съобщенията. Разследвана е също така организирана атака, която използва слабости в механизма за самообучение (базиран в основата си на функцията „повтаряй след мен“). След няколко дни и корекции в контролния механизъм е активирано в мрежата второ „издание“ на TAY, което пък залита в посока дрога и сленг, и скоро „зацикля“, повтаряйки безсмислен пост няколко пъти в секунда, Важно е да отбележим, че следваща версия “Zo” е доста по-успешна и се ползва и до днес във Facebook messenger. Zo дори проявява чувство за хумор, например при отговори на въпрос дали версия 10 на Windows е добра.

❖ Нови видове рискове и възможности за застраховане – напълно нова област, без натрупана статистика, принципи, правна регулация.

❖ Машините не бива да се използват за „оценка“ на хора и бизнес или вземане на решения за тях – например оценка на кредитен рейтинг,

[162] Deal or No Deal? End-to-End Learning for Negotiation Dialogues, https://arxiv.org/pdf/1706.05125.pdf

рискове (за застраховки), назначаване на работа, още по-малко за рискове във връзка с криминално и престъпно поведение, деяние.

ВЪЗМОЖНОСТИ ЗА ИЗПОЛЗВАНЕ НА ИИ ЗА КИБЕР СИГУРНОСТ И ОТБРАНА

Специфична област, която от зората на ИИ е представлявала особен интерес, е използването на „интелигентни машини“, „агенти“ в областта на сигурността, защита на обществото/човека и отбраната. Макар и позицията на хуманното общество да е ясна – неизползване на ИИ за разработване на автономни оръжия – то в съвременното общество, именно поради цифровата и ИТ зависимост, все повече се налага необходимостта от използване именно на високо-производителни и интелигентни системи за защита и следене на функционирането на комуникационните и информационни системи, системите за управление на индустрията, бизнеса и държавата. Това не само възобнови интереса към използване на методите и средствата на ИИ, но и доведе до нови, революционни технологични решения, приложими както в обществения живот и бита, така и в сферата на сигурността и отбраната, в частност за постигане на кибер сигурност и устойчивост (resilience).

Ето някои от тях (без да претендираме за изчерпателност):

- Следене за прилагане/спазване на „кибер хигиена“ или превантивните мерки за кибер сигурност – автоматични нива на „сигнализиране“ за отклонение от дейности, нарушение на норми/правила (както специфични, така и стандартни, общи).
- Интелигентни асистенти на професионално ниво (ИТ специалисти, специалисти по сигурността).
- Интелигентни помощници на ИТ мениджъри и ръководители на организации при оценка на ситуацията и вземане на решение (прилагане на мерки, реакция при инциденти, или по-стратегически решения за инвестиции в сигурността).
- Следене за експлоатацията и функционирането на системи, мрежи, комуникации:
  - отклонения от поведение / трафик / профил на дейности/потребители;
  - праг на сигнали – инциденти, ескалация (вземане на решения), SOP.
- Специализирани – „Интелигентни“ SIEM (Security Incidents and Event Management) и SOC (Security Operations Centers).

- Развитие на модели и методики за обучения – модели, симулации, установки (Cyber Ranges).
- Нови средства за защита – например базираните на ИИ „биометрични“ методи от нов тип – като „когнитивна автентикация“.
- Отбрана – национална/колективна сигурност:
  - Кибер операции по „защита“ на мрежи и системи (с национално значение, сигурност и отбрана);
  - Интелигентни/автономни системи за защита (кибер-оръжия) – за специфични области, сложни системи;
  - Идентифициране на летящи обекти.
- Хибридни въздействия – върху обществото, манипулации на мнението, избори и настройка на обществото (примерът с Cambridge Analitica и изборите в САЩ, вота Brexit и др. е достатъчно показателен), медии и дезинформация, фалшиви новини.
- Нова област – анализ на големи данни с цел ранно предсказване/предупреждение за престъпления.
- В сферата на защита от системите от ботове – използването на метода на „обратен тест на Тюринг“ (популярните методи и средства на CAPTCHA).
- Приложение на експертните системи е автоматизираното генериране на компютърни програми. Вече е официално представена на пазара спонсорираната от фонда на военновъздушните сили на САЩ експертна система (hprcARCHITECT), която генерира компютърни програми за системи, базирани на различни процесорни технологии (FPGA/GPU/Multicore) без нуждата от обучен персонал.

Използване на ИИ за „съществени“ услуги

Съгласно Закона за киберсигурност, който транспонира и Европейската директива за мрежова и информационна сигурност[163], като „**съществени услуги**“, са идентифицирани следните дейности:

а) секторите: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода, цифрова инфраструктура, или

[163] *Закон за киберсигурност, 31 октомври 2018 г.*, и Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза

б) цифровите услуги: онлайн място за търговия, онлайн търсачка и компютърни услуги в облак.

Този избор на секторите (с техните подсектори и свързани дейности) не е случаен – в условията на модерното общество и икономика те стават все повече цифрово зависими и тяхното нарушаване и прекъсване може да има сериозни последици за обществото. За целите на следенето на тяхното нормално функциониране, ранно забелязване на отклонения и заплахи и въздействия от различно естество (включително и „дълго спящи“ потенциални кибер въздействия), както и продължаване на работата им (service continuity) под зловредни въздействия все повече навлизат системи, използващи методи и техники на ИИ. Това се дължи от една страна на непрекъснато нарастващата сложност и свързаност на мрежите и системите, а от друга страна на невъзможността да се изследват, опишат и съответно тестват техните възможни състояния, както и неимоверното количество данни за следене на тяхната работа, което стандартните изчислителни методи и средства не могат да обхванат или обработят в реално време.

Измежду най-известните (и доказано успешни) области можем да посочим:

- Управление на „умни градове“, инфраструктура.
- Здравно обслужване, телемедицина – сектор, в който ИИ може драматично да промени и подобри предоставянето на услуги. Комбинацията от застаряване на населението, усложняването на здравните потребности, нарастващите изисквания на пациентите и финансовите аспекти са само част от обществения натиск. ИИ демонстрира вече потенциал да подобри целия цикъл на услуги, например:
  - Роботизирана хирургия – над 45 робота Da Vinci позволяват на хирурзите в британските болници (Англия и Уелс) да работят дистанционно с помощта на много малки и точни инструменти, прикрепени към роботизирани манипулатори;
  - Виртуални медицински помощници – например с помощта на умни „носими устройства“ (wearable) показатели за състоянието могат да се наблюдават от лекари (или дори от умни диагностични програми) и да дават по-добри решения или предупреждават за проблем;
  - Терапия, дозировка на лекарства – за персонализирана преценка и следене;
  - Управление на свързани с поддържане на здравето и обслужването устройства;

- Модерна диагностика – специализирани методи и системи за обработка на изображения, предварителна диагностика, например за подобряване на преценките на рентгенолозите рентгенови лъчи и други сканирания, както и за намаляване на човешките грешки (на базата на техниката „дълбоко самообучение“).

- Образование (управление, организация, съдържание).
- Финансови услуги (банки) и застрахователи.
- Работа с клиенти – помощ, чат, услуги.
- Оценка на риска (кредити, застраховки).
- Контрол и управление на сложни „Системи от системи“.
- Електроснабдяване – Smart Power Grid.
- Сателити и комуникации.
- Транспорт.
- Спекулации и манипулации на финансови/стокови пазари);
- Автономни (безпилотни) коли и устройства.

ПЕРСПЕКТИВИ И ПРЕПОРЪКИ

Макар да имат вече широка популярност, интелигентните асистенти или чатботове далеч не са основната сила на ИИ. Те са най-забележими, защото са най-близо до потребителите и веднага се отчитат много от изтъкнатите предимства. Освен ефективността и прозрачността на консултацията с чатбот, особено ценна е възможността той да докладва за липсваща информация или услуги, както и да допринася за оптимизиране на услугите, дори и динамичното конструиране на комплексни услуги (характерни за по-високото ниво на зрялост на е-услугите).

В допълнение, използваните други методи на ИИ, особено обработка на big data или намирането на зависимости чрез самообучение (или дълбоко самообучение) вече се използват ефективно за анализ, оптимизация и управление на редица съществени услуги за граждани и бизнес – оптимизация на транспорта, консумацията на енергия, финансови услуги и други.

Тестват се платформи като „ИИ под наем“ или „ИИ като услуга“ (тип „облачна“) – динамично мобилизиране на ресурси и памет (включително данни и знания) в зависимост от нуждите за конкретни системи и задачи. Това е една от разглежданите възможности за подпомагане на малкия и среден бизнес, както и на стартъпите, за преодоляване на „входната бариера“ за наблюдаваното „интелектуализиране“ на цифровия пазар и общество.

За целите на стимулиране на изследванията и практическото прилагане на методи и техники на ИИ, както в сферата на бизнеса, така и в публичния сектор, през април 2018 г. Франция обяви, че предвижда публично финансиране на ИИ от над 1.5 млрд евро до 2022 г., като привлича партньори като IBM, Samsung и др., със стремеж да се изправи срещу доминацията на Google и Facebook. Германското правителство е отделило около 3 млрд. евро до 2025 г. за проучвания и развитие на „изкуствен интелект, създаден в Германия“, опитвайки се да свие пропастта в софтуерните иновации между Германия, САЩ и Азия. Същевременно документът засяга и „социалната политика и работната сила“ като аспекти на ИИ, което отразява притесненията на Германия за опазването на личните данни и начина, по който подобна технологична промяна може да трансформира сегашните социални модели.

В изпълнение на декларацията за сътрудничество[164], подписана от 24 държави членки и Норвегия на 10 април 2018 г., ЕК организира изготвянето на координиран план за развитие на ИИ, с основна цел постигане на увеличаване на инвестициите на равнище ЕС и на национално равнище, насърчаване на сътрудничеството в ЕС, обмен на добри практики и определяне на начините за гарантиране на глобалната конкурентоспособност на ЕС в тази област. Комисията ще продължи да инвестира в ключови инициативи в областта на ИИ, включително в разработването на по-ефективни електронни компоненти и системи (специално разработени за операции на ИИ), компютри на световно равнище, както и водещи проекти в областта на квантовите технологии и „карта“ на човешкия мозък.

Създаването на подходящите условия за развитие на цифровите мрежи и услуги е един от трите стълба на стратегията за цифров единен пазар (DSM – Digital Single Market) на ЕС. В предложения Регламент на ЕС през септември 2017 г. се предвижда през 2019 г. развитието на DSM да бъде подкрепено чрез стандартизацията, като освен другите нови технологични области, като интернет на нещата, големите информационни масиви, блокчейн, бъде обърнато особено внимание на приложни ИИ системи – съвместните **интелигентни транспортни системи** и автономния превоз, електронното здравеопазване, интелигентните градове, електронното управление и изкуствения интелект.

ЕК очертава европейски подход за стимулиране на инвестициите и задава насоки в областта на етиката, както и мерки за поставянето на ИИ в услуга на европейските граждани и за засилването на

[164] Европейска комисия: Декларация за сътрудничество https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

конкурентоспособността на Европа в тази област (юни 2018 г.) и сформира специална група експерти на високо ниво, която да развие и предложи план за развитие на ИИ изследванията и прилагането в индустрия, държавно управление и общество, както и конкретни мерки за инвестиции и развитие. Сформирана е и ИИ алианс (платформа за широко обсъждане).

ГЛАВА ТРЕТА

ВИЗИЯ ЗА БЪДЕЩЕТО В СФЕРАТА НА КИБЕР УСТОЙЧИВОСТТА

ОЧАКВАНИ РЕЗУЛТАТИ НА ВСИЧКИ НИВА ОТ ВНЕДРЯВАНЕТО НА ИНОВАТИВНИ РЕШЕНИЯ В ДЕЙНОСТТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ПУБЛИЧНИЯ СЕКТОР

СРЕДА ЗА КИБЕР СИГУРНОСТ В БЪЛГАРИЯ

Основни рискове и заплахи за кибер сигурността в НАТО и ЕС със специфични измерения за България

Според представеното на Световния икономически форум (WEF) в Давос през януари 2018г. изследване Global Risks Perception Survey (WEF-GRPS)[165], кибер заплахите растат видимо, като **мащабните кибератаки сега са на трето място по отношение на вероятността (след промените в климата и природните бедствия)**, следвани от кражба или измами с данни (както е представено на **Фигура 1**). **Кибер-зависимостта се класира като вторият най-значим** двигател, оформящ глобалната картина на рисковете за следващите 10 години.

Отчита се разширяване на обхвата и разрушителния ефект на кибер атаките, като тук ще спомена няколко от неблагоприятни тенденции, с възможно пряко или косвено отношение към средата в България, като се цитират различни проучвания и източници:

- Кибер-пробивите са се удвоили за последните 5 години – от 68 на фирма/организация през 2012 г. до 130 през 2017 г.[166] (като се отбелязва и годишно увеличение от 27.4% на оценка на щетите за организация).
- Изтичането на данни вече се измерва с десетки милиони (докато преди 5 години десетки хиляди се разглеждаше като „голяма кибер атака“) – само 2016 г. са докладвани над 4 млрд. случая (колкото сумарно за предходните години)[167] .
- Атаките тип “разпределен отказ на услуги“ (Distributed Denial of Service, DDoS) от висок интензитет (100 Gbps) са нараснали с над 140% само през 2016 г., като е увеличена тяхната „упоритост“ и интензитета (над 32 „серии“ атаки в рамките на 3 месеца за всяка една цел)[168] .
- Атаките и кампаниите от тип „откуп“ (ransomware) са засегнали два пъти повече организации в сравнение с 2016 г., като свързаните с тях емейли със зловредно съдържание са над 64 % от идентифицираните като

[165] http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/?doing_wp_cron=1544373533.2535779476165771484375#view/fn-36

[166] Цитира се проучване на Accenture 2017 (Cost of Cyber Crime Study): https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[167] IBM. 2017. IBM X-Force Threat Intelligence Index 2017. White Paper. https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/

[168] Akamai. 2017. Q2 2017 State of the Internet / Security Report. https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

"phishing" само за периода юли-септември 2017 г., като се отбелязват и следните „знакови" атаки с особености в сценариите, технологиите и пораженията (ефекта): Атаката WannaCry, Petya/NotPetya.

❖ Кибер престъпниците увеличават значително („експоненциално" като бройка) целите си, благодарение на навлизането на облачните технологии и платформи (за услуги), както и масовото навлизане в живота и бизнеса на умни устройства, „интернет на нещата" (IoT, Internet of Things) – като броят глобално им от 8.4 млрд за 2017 г. се очаква да нарастне до над 20.4 милиарда през 2020 г.

❖ Финансовите загуби от атаките нарастват средно с 27% годишно.

❖ Атакувани са ресурси и системи, инфраструктури от критично значение за икономиката и обществото – енергийната система в Украйна (неколкократно блокирана от известна APT група), в атаката срещу мрежата за съобщения на SWIFT предизвика над 81 млн USD загуби (Централна банка на Бангладеш), транспортни системи и пристанища, над 1000 атаки/месечно срещу авиационните системи отчита Европейската агенция за сигурност на авиацията (EASA), и др.

Независимо, че „публичният сектор" като финансови загуби е посочен като 50% спрямо най-атакувания сектор – „финансови услуги" (и на 8-мо място по показател „средна годишна загуба по сектори"), за общата оценка следва да се отчете и доминирането на другите свързани с публичните услуги и ангажименти на държавата сектори – това са комунални услуги, енергетика, отбрана, здравеопазване и практически формират „топ 5" на най-атакуваните сфери със значителни поражения. За втора поредна година форумът поставя акцент върху „Кибер устойчивостта" (Cyber Resilience) на критичните инфраструктури от жизнено значение за обществото, именно отчитайки нарастващата комплексност на заплахите, и необходимостта да се подготвим за нови, неизвестни досега заплахи[169].

Общата картина и прегледа на нарастване на заплахите и атаките в ЕС е подобна (част от основните световни инциденти и пробиви за 2017 г. са именно свързани с Европа – икономически, но и политически и социално – напр. с кампаниите около провежданите избори, Brexit, интензивни и мащабни DDoS – отказ на услуги атаки, и др.). Според годишния доклад "ENISA Threat Landscape Report 2017"[170] на Европейската агенция за мрежова и информационна сигурност (ENISA) ENISA предупреждава за две растящи опасности: правителствено-спонсорирани актьори са един от най-доминиращи злонамерени агенти в киберпространството и са растяща реална заплаха и проблем както за бизнеса, така и за правителства и

[169] http://www.ipex.eu/IPEXL-WEB/dossier/files/download/082dbcc554078eae01540b0b076200c3.do

[170] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

обществото. „Кибер войната“ настъпва динамично в киберпространството, което създава нарастваща загриженост за операторите на критична инфраструктура, особено в области, които вече са пострадали от кибер-криза. Тук открито се разглежда „активната защита“ като метод за кибер отбрана, включително и установяване на баланс (и политически и обществен контрол) върху „нападателните“ способности (offensive), които се налагат като необходимост за постигане на ефективна защита, и до голяма степен съответстват на подчертаната асиметричност на кибер атаките, както и невъзможността за защита с познатите до момента технологии и методи. В доклада се посочва нарастване на атаки тип DDoS (отказ на услуги, предимно уеб) – 33 % от организациите са били подложени на DDoS, срещу 17 % за 2016 г. Тенденцията е към „пулсиращи атаки“ (краткосрочни, но много интензивни атаки срещу много цели едновременно), като в най-интензивния случай атаката е достигнала 350 Gbps. Над 74% от DDoS атаките са мулти-векторни (т.е. използват се едновременно различни техники и подходи към една цел – например кампанията Mirai използва два протокола за комуникация за атака, като е изключително агресивна в индустриални системи и мрежи от „умни устройства“ (IoT). DDoS атака като „услуга“ („под-наем“) расте, и доведе до известния „Krebs доклад“ от януари 2017 г.[171] Като основна заплаха към бизнеса са посочени „Упоритите“ DOS атаки (Advanced Persistent DOS), често базирани на IoT ботнет мрежи (или мрежи от „зомбирани“ умни устройства, по-надолу сме представили примери на такива).

Според разпространения от ENISA годишен доклад за Великобритания[172] над 43 % от организациите (бизнес, неправителствени) са пострадали от пробиви в сигурността за последните 12 месеца. Основен фокус остават хората и човешките грешки – около 75 % са пострадали от зловредни емейли, като 28% - от други „персонално насочени“ атаки. Около 60-70 % считат, че екипите по киберсигурност са компетентни, но от друга страна едва 20% провеждат системни обучения, като само 25 % имат установени политики за киберсигурност. Голяма част (90 %) разчитат на технологиите за защита, firewalls, архивиране на информацията което доказано без прилагане на съответни политики, организация и обучение на хората е неефективно. Отбелязан е за втора поредна година „бум“ на атаките и фокуса върху малкия и среден бизнес (МСП), в диапазона от финансови и бизнес измами (фалшиви контрагенти, фактури) до кражба на информация, изнудване, блокиране на дейността (известните ransomware/cryptolocker, включително и споменатите особени NotPety, WonnaCry с различни модификации), други насочени атаки.

[171] https://krebsonsecurity.com/category/ddos-for-hire/

[172] https://www.enisa.europa.eu/news/member-states/cyber-security-breaches-survey-2018

По информация от Националния CERT в България, тенденцията е подобна, като се отчита все пак факта, че статистиката се изготвя на базата на докладвани случаи, което вероятно се разминава (като бройки, предполагаемо не и като профил) с действителната картина. Немалка част от инцидентите не се докладват, макар за тях информация да изтича в публичното пространство (или се получава от източници в чужбина, като част от по-комплексни атаки). Очаква се мерките, свързани с прилагането на Директивата МИС на ЕС и в изпълнение на Закона за киберсигурността (октомври 2018 г.), както и изготвяните съответни наредби и правилници под ръководството на ДАЕУ, да подпомогнат не само изготвянето на по-пълна картина, но и прилагането на ефективни превантивни мерки и ефективна помощ за засегнатите организации.

Сложен и многослоен кибер-терен

За да се изучат слабостите и заплахите, и свързаните с това възможности за реакция и отговор, е важно да разгледаме в цялостност и дълбочина „цифровата екосистема“. За целта напоследък все повече се използва понятието „кибер терен“ (Cyber Terrain)[173]. То е продължение на класическите многослойни модели (defence in depth multi-layered models), популярни за целите на обмен на данни в различни формати и протоколи, известни като OSI[174]. Кибер теренът (а и киберпространството) в неговата цялост надгражда тези нива с програми и системи, обработващи данни и информация, с последващи действия от кибер и физически системи, хора, организации, т.е. с интерпретацията и използването на данните (информацията). Защитата в дълбочина не е ефективна ако покрива само мрежовите нива на взаимодействие, следва да бъдат разгледани и покрити всички слоеве от по-високо ниво[175]. Цялостната визия за екосистема в дълбочина въвежда и нов поглед на кибер-терена чрез представяне на триъгълника на устойчивост, или трите стълба на кибер сигурността: ***Хора - Организации (с процеси) – Технологии.***

Сложни, съвременни и продължителни атаки с хибриден ефект

На базата на анализ на средства, източници и цели, както и подход, понякога и технически следи (но със съответната доза съмнение за тяхната

[173] Концепция, разработена за целите на отбраната на САЩ (U.S. Department of Defense) като осъвременен модел за „защита в дълбочина“ , https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

[174] https://bg.wikipedia.org/wiki/OSI_модел

[175] Raymond, D., Conti, G., Cross, T., and M. Nowatkowski. “Key Terrain in Cyberspace: Seeking the High Ground.” 6th International Conference on Cyber Conflict, ed P. Brangetto, M. Maybaum, J. Stinissen, 2014, 287-300.

достоверност), са идентифицирани различни хакерски групи („школи“ или „актьори“), някои с по няколко имена – общо известни под термина “съвременни упорити заплахи“ – **APT (Advanced Persistent Threats)[176].** Повечето от тях се определят като „кибер шпионаж“ (може би това са първоначалните им цели и задачи), но на базата на мощни и агресивни средства за атака, хибридни подходи и използвани разнообразни технологични, социални и други методи (включително и изкуствен интелект, високопроизводителни изчисления) вече могат да постигнат много по-сложни сценарии, и в редица случаи доказано да въздействат върху редица критични за обществото ресурси, системи и услуги (критична инфраструктура). Те са посочени и в доклада на ENISA за 2017 г. като едни от най-сериозните и мащабни механизми за атаки, въздействие и предизвикване на кризи.

Според Европейска стратегия за кибер сигурност в енергийния сектор[177], APT са разгледани като една от основните заплахи и фактор за дестабилизация и сериозни въздействия с каскаден и хибриден ефект.

Тези заплахи са особено критични при системите за (цифрово) управление (в по-ранните години наричани „за автоматизация“) на индустрия, производство, услуги и бизнес, известни като и бизнес и индустриални процеси, бизнес – известни най-вече като **ICS/SCADA** (Industrial Control Systems, Supervisory Control and Data Acquisition)

В модела за зрялост, разработен от Европейската агенция за мрежова и информационна сигурност ENISA - „Анализ на нивата на зрялост за киберсигурността на ICS/SCADA системите в критичните сектори“ [178], над 55% от атаките и заплахите за тези системи са именно от типа APT (при изследване от 2015 г.). Проблемите, произтичащи от тяхната комуникационна, мрежова и информационна свързаност са предмет на следващ доклад – „Communication network dependencies for ICS/SCADA Systems“[179] (2017 г.).

В рамките на настоящото изследване, не бяха открити в публични източници доклади и проучвания в България за наблюдавани и отчетени APT (от „класическите“ известни, или друг тип) кореспондира и с липсата на специални и периодични проучвания за навлизането на съвременни технологии (напр. IoT, изкуствен интелект, блокчейн), както в бизнеса, така и в публичния сектор, образованието. Информацията за „регистрирани“ активности (или сигнали за такива) на различни APT върху обекти или

[176] https://en.wikipedia.org/wiki/Advanced_persistent_threat

[177] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

[178] https://www.enisa.europa.eu/publications/maturity-levels

[179] https://www.enisa.europa.eu/publications/ics-scada-dependencies

системи в България се получава индиректно по наблюдения „отвън“, и само не са достатъчни за да бъдат анализирани, както и възможните свързани с това насочени атаки или поредици от инциденти с голяма мащаб. Доколкото тези заплахи са насочени към правителствени организации и критични ресурси и инфраструктури) – то е от критична необходимост внедряването на средства за мониторинг и анализ с цел разкриване и сигнализиране на такива кампании, както и осигуряване на „терена“ за получаване на специализирана помощ (включително и от съюзници и партньори от ЕС и НАТО). Това е от съществено значение и за защитата на споделените ресурси и споделеното интернет пространство, доколкото атаките към общността се насочват към по-слабо защитените и уязвими звена от веригата.

Цифровизацията – предимство и заплаха

Цифровизацията (или „дигитализацията“) на икономиката и държавното управление е основната характеристика на съвременното общество и приета за движещ фактор на ново общество - общество на знанията, с икономика на знанията. Един от показателите за развитие на е-управлението, и също така индикатор за прехода от началната стъпка на „електронно правителство“ към „електронно управление“ (залегнал в стратегията на ЕС, както и в националната стратегия и законодателна база) – е **необратимостта на електронните услуги**. Това е и един от показателите в представения от ООН доклад „E-Government Survey 2018” и съответен индекс за развитие и „етапи на зрялост“ [180].

След дългогодишни отлагания на срокове, през 2017-2018 г. в България с ускорени темпове се внедряват планираните електронни услуги от всички държавни ведомства, стимулирани от решения на правителството и създаването на нова Държавна агенция „Електронно управление“ (ДАЕУ). Отчетен е определен успех в необратимостта на този процес в България, с поставени ясни крайни срокове за преминаване изцяло на електронен документооборот между ведомствата (ноември 2018 г.), както и редица ключови и масови услуги за граждани (например – е-Връчване).[181]

Същевременно, тази необратимост поражда обосновани страхове (които са реални рискове) от надеждността, сигурността и устойчивостта на съответните системи. При това с отчитане на тяхната взаимосвързаност и зависимост, т.е. с отчитане на опасностите и последствията с „каскаден ефект“. „Предупреждението“, получено с прекъсването на услугите на Търговския регистър в продължение на 18 дни през август 2018 г. е ясен

[180] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018

[181] https://e-gov.bg/bg/news/110

знак за възможните каскадни ефекти, както и за ключовата важност за предприемане на мерки както по отношение на базовата „кибер хигиена“, така и за осигуряване на „кибер устойчивост“ (resilience) на системите и услугите с особена значимост (които до голяма степен се покриват и със „съществените услуги“, по смисъла на Европейската „Директива за МИС“, и Закона за киберсигурност, Октомври 2018 г.).

Заплахите и отговорностите, свързани с тази необратимост, са застъпени в Национална стратегия за киберсигурност (2016 г.), както за сектора на публични (електронни) услуги, така и за цифрово-зависимите бизнес и индустриални сфери. Очаква се те също да бъдат включени в разширения обхвата на Национална система за киберсигурност, чрез развитие на „Националната координационно-организационна мрежа за кибер сигурност (НКОМКС)“, регламентирана за реализация и в Закона за КС.

Мерките за постигане на мрежова и информационна сигурност, визирани (но все още нерегламентирани или изпълнени) в Закона за киберсигурност, във връзка с очакваната към него Наредба (и свързани с транспониране на „Директивата за МИС“) са само минималната база. Следва да се отчете, че повечето от тези системи попадат в категорията „критични инфраструктури“ и към тях по силата на „Закона за КС“ Държавната агенция за национална сигурност (ДАНС) би следвало да предяви допълнителни изисквания за осигуряване на непрекъсваемост, защита и надеждност на работата. Още по-високи изисквания за устойчивост към системите, свързани с националната сигурност и управление и функциониране на държавата в извънредни ситуации следва да бъдат дефинирани и реализирани под ръководството на Министъра на отбраната (МО).

Фалшиви новини, кибер-пропаганда, дезинформация и манипулация

Използването на нови технологии (предимно методи и средства на ИИ) дава възможност за все по-убедително и „достоверно“ съобщаване на дезинформация (или известна като misinformation), както и дори за незабележима, подсъзнателно манипулация. Естествено поле за използване на тези методи са изборите и политически интереси и манипулации, включително и кампании от хибриден характер за дестабилизиране на демократичните общества. Тук вече „класически“ е примерът с Cambridge Analytica[182], която формално се рекламира като „ние използваме данни за промяна на поведението (на групата, обществото)“. Използването на средствата и методите за т.нар. „персонално

[182] https://en.wikipedia.org/wiki/Cambridge_Analytica

профилиране“ на гражданите (директно на база на техни интереси, в случая в социалните мрежи, Facebook, но и индиректно за техните близки приятели) при референдумът за Брекзит във Великобритания и президентските избори в САЩ през 2016, както и другите изборни кампании в ЕС след това показаха, че постиженията в областта на ИИ и новите високо-производителни технологии предоставят нова серия от мощни механизми („оръжия“) за кибер-пропаганда. Нещо повече - манипулацията на съзнанието и чувствата на гражданите се използват освен за публично забележимата част (избори, политическа сцена), така и за икономически и други интереси.

Друга сфера от постижения за прилагане на ИИ се оказа също мощно „оръжие“ за различни измами и манипулации – възможността за незабележимо с технически средства модифициране и трансформиране на елементи от снимки и видео - с особено голям интерес към модифициране на лица, жестове, говор и получаване на напълно реалистичен, и доста убедителен материал. Използва се вече за шаржове на политици и известни личности, но освен забавната страна има много силен потенциален разрушителен ефект, както и мощно оръжие в хибридна война[183].

Нови технологии – нови предизвикателства за киберсигурността

В доклад на Европейската агенция ENISA от януари 2018 г. – *„ Looking into the crystal ball - A report on emerging technologies and security challenges“*[184], следните нови или бързо развиващи се технологични области отправят нови предизвикателства пред киберсигурността:

- IoT - Интернет на нещата (Internet of Things);
- Взаимодействието между навлизането на технологиите и социалните предизвикателства;
- ИТ инфраструктура от ново поколение;
- Виртуална реалност (VR) и добавена реалност (AR);
- Автономни системи (превозни средства, автомобили);
- Интернет на био-нано-нещата (IoBNT);
- Изкуствен интелект (ИИ) и роботи.

Рисковете в киберпространството – готовност за „неизвестното“

По отношение на оценката и подготовката за посрещане на рисковете в киберпространството, на базата на представените по-горе съвременни заплахи и тенденции, ще се ограничим да потвърдим приложимостта на

[183] https://singularityhub.com/2018/09/03/the-new-ai-tech-turning-heads-in-video-manipulation-2/
[184] https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

дефинирания в Националната стратегия за киберсигурност (2016 г.), който описва не само нивото и вида на заплахи, но и обосновава стратегиите за подготовка и етапите („нивата на зрялост“) за достигане на състояние на „кибер устойчивост“ (cyber resilience).

Разглеждаме **два аспекта**:

✓ общоприетата „триада“ от областта на информационната сигурност;

✓ **Конфиденциалност–Интегритет–Наличност (КИН)** [185];

✓ нивото на познаване на заплахите и съответните рискове – класификацията за **„известните неизвестни“**, използвана също и в областта на националната сигурност[186].

Тези два аспекта позволяват ясно структуриране на целите и областите на действия, както и три нива на зрялост на организации, държава и общество - **информационна сигурност, кибер сигурност и кибер устойчивост**[187].

- **„известни известни“** – защита и предпазване на информационните активи и комуникационна инфраструктура от известни слабости, заплахи и пробиви, свързани с основната „триада“ на информационната сигурност (КИН);
- **„известни неизвестни“ (не-КИН)** - комплексни и комбинирани заплахи, свързани с информационната сигурност, ИКТ, мрежите и системите, разнообразието от **съвременни упорити заплахи** (APT[188]), атаки срещу репутацията на организации и личности, кампании за дезинформация, и други непредсказуеми последствия от масовото пренасяне на дейностите ни в кибер пространството, пробиви в КИН в особено големи мащаби (национални, регионални и световни), изискващи разширено и системно прилагане на КИН за всички активи в дигиталната екосистема - информация, технологии, хора и съоръжения, за постигане на **кибер сигурност**;
- **„неизвестни неизвестни“** или подготовка за неизвестното - неочаквани заплахи в киберпространството, динамично променящи се рискове и комплексни въздействия с непредсказуеми последствия, които изискват гъвкавост и устойчивост на системите, организацията и процесите, и

[185] Confidentiality, Integrity, Availability (CIA)

[186] Насим Талеб, Черният лебед - https://en.wikipedia.org/wiki/Black_swan_theory;

[187] Eurocontrol: Manual for National ATM Security Oversight (2012)

[188] Advanced persistent threats (APT)

съответни стандарти при разработването и внедряването им, състоянието на **кибер устойчивост**.

Стандарти за оперативната съвместимост и кибер сигурност / устойчивост в България и НАТО/ЕС

Цифрова Европа = технологии + киберсигурност

Определените в предложението за Регламент на Европейския парламент и на Съвета за програма **„Цифрова Европа“ 2021-2027г.**[189], от юни 2018 г. приоритетни области за развитие и инвестиции са:

- високопроизводителните изчислителни технологии;
- изкуствения интелект;
- киберсигурността;
- задълбочените цифрови умения.

Подчертава се, че *„пренебрегването или отслабването на един от тези стълбове ще подкопае цялостната конструкция, тъй като те са тясно свързани помежду си и взаимно зависими: например, изкуственият интелект се нуждае от надеждна киберсигурност, киберсигурността се нуждае от високопроизводителни изчислителни технологии за обработка на огромното количество данни, които трябва да бъдат защитени, цифровите услуги се нуждаят и от трите, за да покрият бъдещите стандарти; и накрая, всички по-горе се нуждаят от подходящите задълбочени умения.“*

Следователно важно е също така и на национално ниво да се направи баланс и адекватно приоритизиране. Политиката на ЕС в това отношение е да бъде поставен акцент върху областите, в които публичните разходи **оказват най-силно въздействие, най-вече върху подобряването на ефективността и качеството на услугите в области от обществен интерес** като здравеопазването, правосъдието, защитата на потребителите и публичните администрации, както и върху подпомагането на малките и средните предприятия (МСП) да се адаптират към промените в цифровите технологии.

Инвестициите в рамки, стандарти, оперативно съвместими решения и пилотни трансгранични услуги чрез „Механизма за свързване на Европа“ (МСЕ)[190] и програмата за решения за оперативна съвместимост и общи рамки за европейските публични администрации, предприятията и гражданите вече дават първите резултати – голяма част от публичните

[189] http://ec.europa.eu/transparency/regdoc/rep/1/2018/BG/COM-2018-434-F1-BG-MAIN-PART-1.PDF
[190] https://www.mtitc.government.bg/bg/category/233/mehanizum-za-svurzvane-na-evropa

администрации на държавите-членки извършват цифрова трансформация и преход от **електронно правителство (т.е. услуги) към зряло, интегрирано, цифрово управление**.

Политики на ЕС в областта на стандартите и киберсигурността

Създаването на подходящите условия за развитие на цифровите мрежи и услуги е един от трите стълба на стратегията за цифров единен пазар. През 2019 г. се очаква значителен прогрес в областта на стандартизацията, като бъде обърнато особено внимание на интернет на нещата, големите информационни масиви, блокчейн, взаимодействащи се интелигентни транспортни системи (и автономното шофиране), електронното здравеопазване, интелигентните градове, достъпността, електронното управление и изкуствения интелект.

Основата на подновения ангажимент на ЕС за справяне с кибер заплахите е изготвен от Европейската комисия пакет с реформи в областта на киберсигурността, представен през септември 2017 г. Целта на реформите е да се доразвият мерките, въведени със стратегията за киберсигурността и нейния основен стълб – директивата за мрежовата и информационната сигурност (Директивата за МИС), като новите инициативи са основно:

- изграждане на по-солидна агенция на ЕС за киберсигурността (известна още като ENISA 2.0);
- въвеждане на обща схема за сертифициране на киберсигурността на равнище ЕС;
- бързо прилагане на Директивата за МИС.

Изискванията за киберсигурност следва да предлагат едновременна защита от кибер атаки срещу процесите, системите и оборудването за управление на софтуера и хардуера. В пакета за реформа се предлага въвеждането на **схеми за сертифициране на ИКТ продукти, услуги и процеси на равнище ЕС**[191]. Целта на тази инициатива е да се даде възможност за растеж на пазара на ЕС в областта на киберсигурността. Схемите за сертифициране ще бъдат под формата на правила, технически изисквания и процедури. Чрез тях ще се намали фрагментираността на пазара и ще се премахнат регулаторните пречки, като същевременно се изгражда доверие. Те ще бъдат признати във всички държави членки, което ще улесни трансграничната търговия за предприятията.

[191] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

Модели и стандарти, сертификация

Нуждите от стандартизация в подкрепа на политиките на ЕС са очертани в ежегодно актуализирания текущ план за стандартизация в областта на ИКТ, публикуван от Комисията. Във варианта на текущо актуализирания План за стандартизация в областта на ИКТ от 2018 г. ("Rolling Plan for ICT standardisation")[192] се определят 170 действия, организирани около четири тематични области: ключови фактори, социални предизвикателства, иновации за единния пазар и устойчив растеж.

Във връзка с една от най-бързо развиващите и масови области - „интернет на нещата" (IoT), и посочените по-горе рискове, произтичащи от масовото, до голяма степен безконтролно, навлизане във всички сфери - бита, управлението на бизнес, ресурси и държава, на ниво ЕС е отчетена липсата (или изостаналостта, неприложимостта) на стандарти за различните категории. Това е валидно както за оперативната им съвместимост с други устройства и системи и за надеждното им функциониране, така и за тяхната защита, кибер сигурност и устойчивост. Отчитайки тази важност, двете стандартизиращи организации в ЕС – CEN/CENELEC[193] и ETSI[194], във взаимодействие със световните организации (ISO, IEEE), разработват редица технически и организационни стандарти и спецификации, включително и по отношение на сигурността и надеждността на „индустриалните" IoT – „IIoT", протоколи за криптирана/защитена информация. В текущия План на ЕС за стандартизация в областта на ИКТ[195] е обърнато специално внимание на киберсигурността и на IoT[196].

Към момента на изследването, в Европа има установени или са в процес на разработка все още малък брой стандарти в областта на ИКТ, IoT, киберсигурността и свързани с тях (технически спецификации – Technical Specifications/TS по терминология на ETSI[197], или CEN Workshop Agreements/CWA по терминологията на CEN[198]), в сравнение с амбицията на EU Rolling Plan (2018, и новият за 2019г). Основните групи са (неизчерпателен списък, за подробности – в сайтовете на стандартизиращите организации):

[192] https://ec.europa.eu/growth/content/2018-rolling-plan-ict-standardisation-released_en
[193] https://www.cen.eu/News/Workshops/Pages/WS-2018-04.aspx
[194] https://www.etsi.org/technologies-clusters/technologies/internet-of-things
[195] https://ec.europa.eu/growth/content/2018-rolling-plan-ict-standardisation-released_en
[196] https://ec.europa.eu/transparency/regdoc/rep/1/2018/BG/COM-2018-686-F1-BG-MAIN-PART-1.PDF
[197] https://www.etsi.org/technologies-clusters/technologies/cyber-security
[198] https://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

- Комуникация между устройства и сигурност, IoT – M2M, One M2M, Light-weight cryptography;
- Персонални данни и защита (във връзка с GDPR) – Privacy by design:PII (Personally Identifiable Information);
- Защита на информацията/данните – ABE (Attribute Based Encryption), Attribute Based Access Control;
- Защита на информация при Quantum Computing – QSC (Quantum Safe Cryptography), (ETSI TC CYBER).

Стандартизиран обмен на информация – TVRA (Threat, Vulnerability and Risk Analysis), включително и методи и протоколи за структурирани данни, контрамерки (ETSI TC CYBER):

- Сигурност на комуникациите.
- Роботи и ИИ (в начална фаза).
- Стандарти (таксономии, рамки) за ИКТ компетентности – European e-CF (e-Competence Framework, CEN TC 428).
- Свързани с реализирането на eIDAS – Регламент на ЕС (ETSI)[199].

Въпросът за стандартизация на дейностите в областта на ИКТ, киберсигурност, кибер отбрана и устойчивост е в основата на създадената през 2016 г. мега-организация в Европа – голямо Публично-Частно-Партньорство (contractual Public-Private-Partnership, cPPP) за Кибер Сигурност – ECSO (“Contractual PPP” European Cyber Security Organization)[200]. Работна група 1 (WG1) е ангажирана с развитие на базата от стандарти в областта, в тясно взаимодействие с ENISA, ЕК и проекти за тяхното популяризиране, внедряване, обучение и развитие на капцитет.

В България тези стандарти се адаптират (или признават) с изграден механизъм към „Българския институт за стандартизация“ (БИС)[201] – Технически комитет 47 (ТК 47). Голяма част от стандартите в областта се развиват (и също адаптират/приемат от БИС) от световните организации – ISO (например „класическият“ пакет стандарти за информационна сигурност, известни като „ISO 27k[202]), ITU (по-скоро насоки, guidelines, както и Global Cybersecurity Index[203]).

Други модели/изисквания/препоръки не са формално приети като стандарти от стандартизиращи организации, но са де-факто стандарти (приети от индустрия, правителствени и публични организации). Такива са

[199] https://www.etsi.org/news-events/news/1111-2016-07-etsi-publishes-european-standards-to-support-eidas-regulation

[200] https://ecs-org.eu/

[201] http://www.bds-bg.org/

[202] https://www.iso.org/standard/73906.html

[203] https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

стандартите от групата на „модели на зрялост“ (оригинално от Института по Софтуерно Инженерство, на Университета Карнеги Мелън)[204], известни като CMMI (Capability Maturity Model Integraiton). Понастоящем тези стандарти се поддържат от специална организация – CMMI Institute[205]. В областта на „кибер устойчивостта“ (cyber resilience) – там е разработен и специален модел, обобщаващ над 20 съществуващи модели и стандарти: SEI-CERT RMM (CERT Resilience Management Model)[206].

Това се отнася и за „стандартизирани“ протоколи за обмен на информация, световно приети между организации на оперативно ниво. Такава е групата STIX, TAXII, CyBox[207], за обмен на структурирана информация за заплахи, инциденти, наблюдения/доказателства и друга техническа и оперативна информация. Изработен и поддържан към комитет на OASIS, в момента е в процес на развитие (нова версия TAXII 2.0), като е разпознат от ETSI TC CYBER, и също като един от протоколите за обмен на техническа информация в ЕС (в мрежата на центровете CERT/CSIRT). Друг подобен стандартизиран протокол за споделяне на информация е въведен от MISP (Malware Information Sharing Platform)[208].

Системи за споделяне на информация и съвместна бърза реакция в България и в рамките на НАТО и ЕС – провеждане на учения по кибер устойчивост

Към настоящия момент в Европа единствената единна система за обмен на информация, свързана с кибер инциденти е тази на мрежата от центрове за реакция (от типа на CERT/CSIRT)[209], която се координира от ENISA (Европейската агенция за информационна и мрежова сигурност). Мрежата е създадена в изпълнение и в съответствие с „Директивата МИС“, която в член 12 дефинира създаването на мрежата от центрове за реагиране при компютърни инциденти. Целта на мрежата е „да допринася за развитието на доверието (“confidence and trust”) между държавите-членки и за насърчаване на бързо и ефективно оперативно сътрудничество“. Мрежата е съставена от посочени от държавите-членки на ЕС центрове CSIRT/CERT (известни от Закона за киберсигурност като ЕРИКС – „Екип за Реакция при Инциденти с Компютърната Сигурност“), както и центъра за

[204] https://www.sei.cmu.edu/

[205] https://cmmiinstitute.com/

[206] https://www.sei.cmu.edu/news-events/news/article.cfm?assetId=453248

[207] https://www.isao.org/resource-library/tools/stix-taxii-and-cybox/

[208] https://www.misp-project.org/

[209] https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

киберсигурност към ЕК - CERT-EU. Европейската комисия участва в мрежата като наблюдател. ENISA има за задача активно да подкрепя сътрудничеството, да предоставя секретариат и активна подкрепа за координация на инцидентите при поискване. Мрежата на CSIRT осигурява форум, в който членовете могат да си сътрудничат, да обменят информация и да изграждат доверие. Членовете ще могат да подобрят работата по трансграничните инциденти и дори да обсъждат как да реагират по координиран начин на конкретни инциденти (от сайта на ENISA). Приети са обща таксономия и стандарт (протокол) за споделяне на информация във връзка с кибер инциденти и събития между центровете CSIRT и органите (агенциите) за правоприлагане и Европол, представлявана от EC3[210]. На тази база се поддържа и обща статистика за докладваните инциденти. Този документ не регламентира процедурите за обмен на информация (или реакция), но има установени такива в методиката за създаване на центрове CERT/CSIRT. „Прототипът“ на CERT е в Университета Карнеги Мелън (Институт по софтуерно инженерство), където и в момента продължават да се разработват методики и модели за постигане на кибер устойчивост (cyber resilience), както и стандарти и препоръки за разработване на сигурен софтуер (secure coding), изследват се новите предизвикателства и слабости на технологии, сложни системи (системи от системи) – както за целите на бизнеса и обществото, така и за нуждите на отбраната и националната сигурност (в предната секция са описани някои от тези стандарти)[211].

Този механизъм за обмен на информация при кибер инциденти вече работи, но ефективно осигурява информация на техническо ниво най-вече. За целите на справяне с инциденти от голям мащаб, оценка на въздействието и нивото на тревога, или „разбиране на ситуацията“ (situational awareness) на ниво ЕС, към обявеният през септември 2017г. Пакет за киберсигурност, ЕК добави и План (Blueprint) за „координиран отговор на инциденти с киберсигурността от голям мащаб и кризи и с трансграничен характер“. Документа е отправена следната препоръка:

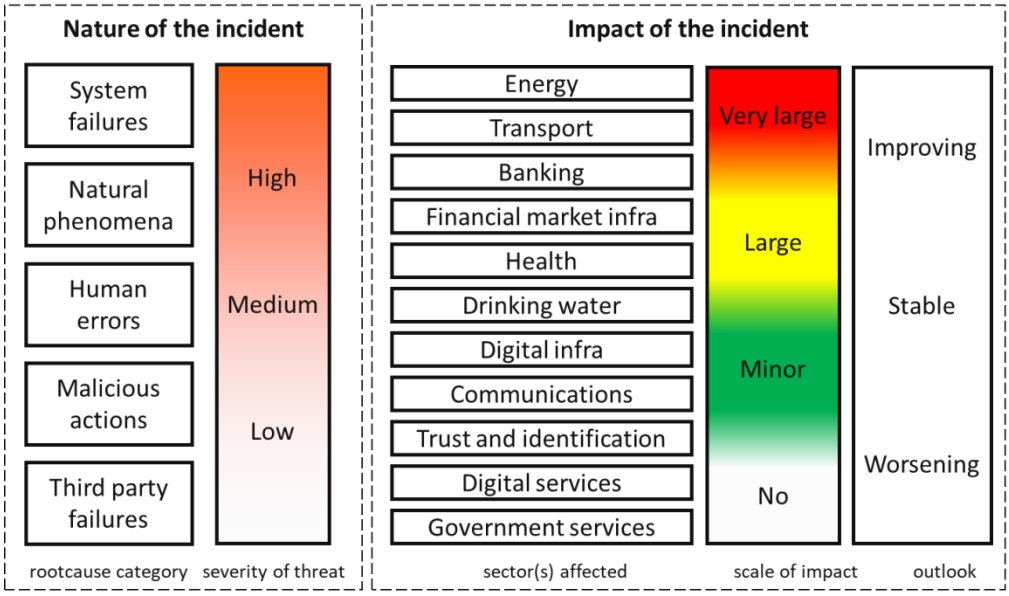
„**Препоръка (7)** Със съдействието на ENISA и въз основа на предишната работа в тази област, държавите-членки следва да си сътрудничат при разработването и приемането на обща таксономия и образец за „доклад за ситуацията“, за да опишат техническите причини и въздействия от инциденти, свързани с киберсигурността, и да развият оперативното сътрудничество при кризи. В тази връзка държавите-членки следва да вземат предвид текущата работа в рамките на Групата за Сътрудничество относно насоките за уведомяване за инциденти и по-

[210] https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

[211] https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21274

специално аспектите, свързани с форматите на националните съобщения.“ Както и:

„…Осъзнаването и разбирането на ситуацията в реално време, … е от жизненоважно значение за вземането на добре информирани решения. Осъзнаването на ситуацията от всички заинтересовани страни е от съществено значение ефективен координиран отговор. Това включва елементи относно причините, както и въздействието и произхода на инцидента....“ и зависи от *„обмена на информация между съответните страни в подходящ формат, като се използва обща таксономия за описване на инцидента и по съответен сигурен начин“.*



Фигура 26. Таксономия към Blueprint

По време на Българското Председателство на Съвета на ЕС, беше разработена и приета през юни 2018 г. първата версия на Таксономията[212], която е представена схематично на Фигура 26 (и по-подробно в документа на ЕК, който подлежи на развитие и стандартизация, както и формално описание в машинен формат, налични като прототип в платформата на MISP[213]).

Предназначението на таксономията, както и на целия План Blueprint, е да бъде интегриран механизма за справяне с кибер-инциденти от голяма

[212] http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

[213] https://github.com/MISP/misp-taxonomies/tree/master/nis

мащаб и кризи в общия механизъм на ЕС за справяне с кризи, който се осъществява от *EEAS Crisis Response Mechanism*[214] и *Integrated Political Crisis Response arrangements (IPCR)*[215].

На национално ниво, в България, заложеният в Националната стратегия за киберсигурност (2016 г.) модел за координация и взаимодействие през мрежата НКОМКС, и с изграждане на Национален кибер ситуационен център, който да поддържа мулти-секторна национална киберкартина напълно съответства с духа и механизма, препоръчан на Европейско ниво (и доказан като работен във водещите държави, САЩ). Препоръката към изграждането им е да се следват възможно най-пълно препоръките и изискванията за интеграция от ЕК и НАТО, за да се постигне синхрон и пълноценно взаимодействие между центровете и съответните организации и в България, и не на последно място – да могат да бъдат ангажирани и секторни, публично частни, академични и бизнес центрове за обмен на информация (предвидени в Стратегията, но нерегламентирани със Закона за киберсигурност).

Отчитайки виталната важност на киберпространството, цифровата зависимост и изместването на живота и дейността на обществото в този „пети домейн“, НАТО и ЕС интензифицираха сътрудничеството и взаимодействието, съобразно характера и приоритетите на двете организации. След приетата през 2016 г. съвместната декларация между ЕС и НАТО за сътрудничество в областта на киберсигурността, последваха редица съвместни инициативи. Основна база за формализиране на това сътрудничеството, както и преминаването от стратегическо към оперативно и техническо ниво, е синхронизиране на разбирането за заплахите и уточняване на критерии, терминологии, както и минималните изисквания и стандарти за киберсигурност. Основа за това са:

- разпознаването на киберпространството като пети домейн;
- прилагането на Директивата за МИС от всички държави-членки (доколкото „съществените услуги“ са общ обект на тревога, заплахи и защита, и тяхната сфера и мащаб на въздействие е далече по-широка и непредсказуема от традиционните критични инфраструктури);
- обмен на информация за заплахи инциденти (некласифицирана);
- съгласуване на позиции при инциденти и кризи, както и възможни източници на атаки (attribution);

[214] https://eeas.europa.eu/topics/crisis-response_en

[215] https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/

- стратегията за „възпиране и разубеждаване“ в киберпространството (Deterrence and Dissuassion), възприета от НАТО и вече ЕС.

Алтернативни модели за развитие на системата за кибер сигурност и използване на иновативни технологии в България

До 2016 г. националната система за кибер сигурност се развива еволюционно, като с появата на нови заплахи и предизвикателства отговорността за неутрализиране, защита и реакция при проявата им се възлага на едно или повече от съществуващите ведомства (министерства, държавни или изпълнителни агенции). В рамките на отделения му бюджет, всяко ведомство изгражда способности за изпълнение на поставените му задачи, участва в процесите на формулиране на политики за киберсигурност и отговаря за съответните оперативни дейности.

През 2014 г. бе разработена Концепция „Киберустойчива България 2020" на основата на която през 2016 г. бе приета националната стратегия за кибер сигурност „Киберустойчива България 2020", която предписва принципи и механизми за оперативно взаимодействие и сътрудничество и координация в развитието на способности за кибер сигурност както между публични организации, така и между публични и бизнес организации и академичния сектор[216].

Законът за киберсигурност, приет от Народното събрание на 31 октомври 2018 г. в голяма степен отразява основните положения от стратегията[217]. Практическата им реализация изисква взимането на съответстващи организационни и ресурсни решения и ще отнеме значително време, особено предвид намеренията за съкращаване на администрацията[218]. Междувременно, не трябва да се изключва възможността от появата на нови заплахи за кибер сигурността, нови технологични възможности и/или политически виждания за организацията на националната система за кибер сигурност.

Прилагането на научен подход за изследване и анализ на алтернативни организационни решения позволява по-добре да бъдат разбрани предимствата и недостатъците на възможните решения и, съответно, да бъде намерена най-добрата траектория за развитие на националната система за кибер сигурност в рамките на ограничените човешки и финансови ресурси.

---

[216] Национална стратегия за кибер сигурност „Киберустойчива България 2020", приета от МС на Република България на 13 юли 2016 г.

[217] Закон за киберсигурност, приет от НС на 31.10.2018 г., Държавен вестник, бр. 94 от 13.11.2018 г.

[218] Министрите имат две седмици да направят предложения за съкращения в администрациите си. Дневник, 5.12.2018 г., https://www.dnevnik.bg/bulgaria/2018/12/05/3357047_ministrite_imat_dve_sedmici_da_napraviat_predlojeniia/.

Тази част от доклада представя базовите алтернативни модели, критериите за тяхното оценяване и използвания метод за тяхното ранжиране. Представените тук и в следващия раздел резултати са част от дисертационното изследване, провеждано от инж. Васил Ризов под ръководството на проф. Тодор Тагарев, което ще бъде завършено в началото на 2019 г.

Базови алтернативни модели за организация на националната система за киберсигурност

Алтернативните организационни модели се различават главно по равнището на координация между отделните ведомства с отговорности за защита на кибер сигурността и степента на централизация (или разпределеност). Това са съответно двете оси на изследваното пространство от възможни алтернативи, представени на Фигура 27.

Разработени са шест базови модела, обозначени съответно като:

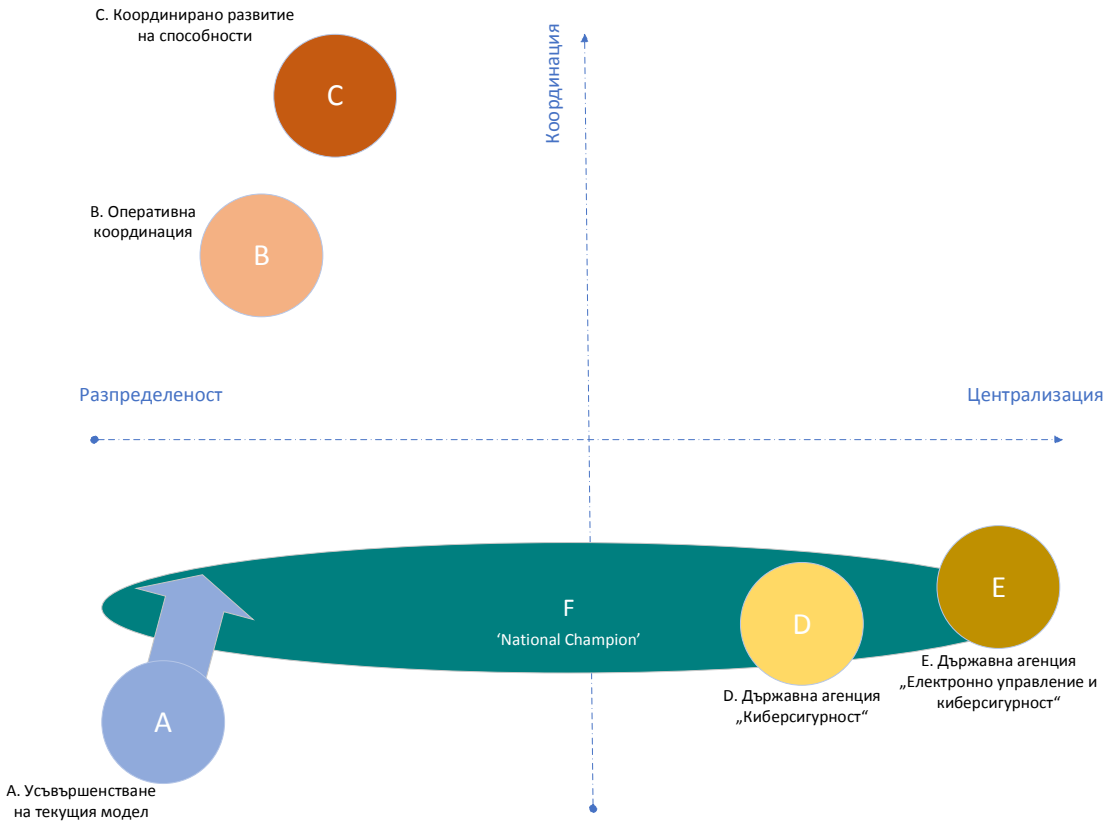
A. Усъвършенстване на текущия модел
B. Оперативна координация
C. Координирано развитие на способности
D. Държавна агенция „Киберсигурност“
E. Държавна агенция „Електронно управление и киберсигурност“
F. Аутсорсинг към водеща фирма (“National Champion”).

Преди да бъдат описани модели е необходимо да се поясни, че координацията (а и въобще функционирането на системата за сигурност) може да бъде разгледана на две равнища:

- **оперативно**, на което организациите от системата за сигурност използват наличните ресурси за наблюдение на обстановката, ранно предупреждение, защита на определени активи (напр. компютърни мрежи, информация), реагиране при атака, възстановяване на работоспособността и отстраняване на негативните последствия от атака, разкриване на причините, идентифициране на извършители др.; и
- при **развитие на способности за киберсигурност** чрез използване на налични и предоставени човешки, материални и финансови ресурси, въвеждане на стандартни оперативни процедури, стандарти и други общи изисквания към квалификацията на персонала, придобиване и изграждане на технически средства и системи, образование, квалификация и учения и т.н.

Шестте разработени модела са наречени „базови“, тъй-като описват само някои главни характеристики. Реалната реализация на избран модел може да бъде осъществена след неговото детайлно разработване и адаптиране към съответната нормативна, организационна и културна среда.

Предполага се например, че при всеки от моделите се реализира публично-частно партньорство, търси се начин за противодействие на т.н. хибридни и други заплахи. Тези въпроси не се разглеждат в настоящото изследване.



Фигура 27. Базови алтернативни модели

A. Усъвършенстване на текущия модел

Модел А отразява текущия модел на организация на националната система за киберсигурност (преди да бъдат реализирани съответните положения от Националната стратегия за киберсигурност „Киберустойчива България 2020“ от 2016 г. и Закона за киберсигурност (2018 г.) с възлагане на отговорности на отделни ведомства по някои от областите на кибер

сигурността (например, противодействие на кибер престъпността – ГДБОП-МВР, защита на критичната инфраструктура – ДАНС, защита на информационната инфраструктура на публичната администрация – ДАЕУ, службите за сигурност – защита на собствените информационни инфраструктури и противодействие на кибер шпионаж и др.). Моделът се усъвършенства постепенно, например чрез разработване и съгласуване на процедури за обмен на информация и взаимодействие между две или повече ведомства с отговорности в областта на кибер сигурността, въвеждане на квалификационни изисквания за съответни длъжности в администрацията, разкриване на съответни специалности във висши учебни заведения, организация на курсове, сертифициране на ключов персонал и т.н.

B. Оперативна координация

Модел B отразява текущия модел за организация на националната система за киберсигурност с добавяне на предвидени в Националната стратегия и Закона за киберсигурност механизми за оперативна координация. Организациите с ключови отговорности в различните области на кибер сигурността си взаимодействат оперативно за целите на наблюдение, създаване и поддържане на обща картина на киберпространството, ранно предупреждение, координирана реакция при „мащабен“ кибер инциденти (криза), отстраняване на последствията и разследване на причините за инцидента и установяване на извършителите.

За тази цел се създава и централен орган за оперативна координация – „Национален кибер ситуационен център“.

C. Координирано развитие на способности

Този модел надгражда Модел B, като към оперативната координация се добавя координирано използване на ведомствени и общо предоставени ресурси за създаване на способности, в т.ч. за научни изследвания и технологично развитие, прилагане на технически и процедурни мерки за повишаване на защитеността на мрежи и информационни ресурси, тестване, сертификация, стандартизация, квалификация, организация и провеждане на учения и др.

За целта се създава „Национална координационна мрежа за киберсигурност“, която формулира и предлага на Съвета по сигурността (или на „Съвет по киберсигурност“) към Министерския съвет общи мерки, политики и приоритети, в т.ч. по бюджетни и инвестиционни въпроси.

При модели B и C системата за киберсигурност остава разпределена, но с нарастваща координация между отговорните ведомства и създаване на

малки централизирани звена – щатно (кибер ситуационен център) и нещатни (мрежа, съвет) – които да подпомагат оперативната и ресурсната координация.

D. Държавна агенция „Киберсигурност“

Създава се нова държавна агенция, която подпомага Съвета по сигурността при формиране на националните политики по киберсигурност, координира и осъществява дейностите по реализиране на тези политики. Държавна агенция „Киберсигурност“ (ДАК) поема оперативни и контролни функции по гарантиране на киберсигурността, в т.ч. противодействие на кибер престъпност и кибер шпионаж, действия за кибер отбрана и защита на критични информационни инфраструктури и стратегически обекти, и криптографска сигурност.

В ДАК се концентрират най-добрите специалисти в администрацията по информационна, мрежова, комуникационна и криптографска сигурност.

ДАК изпълнява функциите на национален център за реагиране на компютърни инциденти (CIRC) и поддържа екип за реагиране (CERT) за нуждите на всички организации.

Модел D предполага развитие на системата за киберсигурност в посока централизация, съчетана със специализация по въпросите на сигурността в киберпространството. ДАК категорично се позиционира като част от националната система за сигурност.

E. Държавна агенция „Електронно управление и киберсигурност“

Моделът предвижда съществуващата Държавна агенция „Електронно управление“ да поеме и функциите на агенция по Модел D, които да бъдат добавени към функциите и задачите, определени в закона за електронно управление и устройствения правилник на агенцията. Възлагат се допълнителни (нови) функции на съществуващите организационни звена и се създават нови организационни звена, които да поемат допълнителните функции и задачи.

При този модел най-добрите специалисти в администрацията в областта на информационните технологии се концентрират в една агенция, изпълняваща „граждански“ задачи и задачи по защита на националната сигурност.

F. Аутсорсинг към водеща фирма (“National Champion”)

Изпълнението на основни оперативни функции в гарантирането на киберсигурността се възлага на водеща фирма с висококвалифициран персонал с достъп до класифицирана информация. Същевременно, със своята експертиза, фирмата подпомага формирането на политики и взимането на съответни инвестиционни/бюджетни решения за развитието на способности за киберсигурност.

Критерии за сравняване алтернативни организационни модели

В изследването се използват пет критерия за оценяване на алтернативните организационни модели: оперативна ефективност; ефикасност; устойчивост; адаптивност; и взаимодействие.

1. *Оперативна ефективност*

В този комплексен критерий се отчита очакваното равнище на ситуационна осведоменост, защитеност, капацитет за ранно предупреждение, адекватна реакция, отстраняване на последствията, разкриване на причини и извършители; капацитет за управление на основни процеси по гарантиране на кибер сигурността, планиране и насочване на ресурсите по направления и задачи.

2. *Ефикасност*

Ефикасността показва отношението на постигнатия резултат спрямо вложените човешки, финансови и материални ресурси. По-ефикасен е този модел, при който се постигат по-добри резултати при определено равнище на ресурсно осигуряване или, аналогично, гарантиран резултат се постига при по-ниско равнище на разходи.

3. *Устойчивост*

Чрез този критерий се оценява способността на системата за киберсигурност да запази работоспособност в условията на масирана, и отчасти успешна, кибер атака и да възстанови загубени ресурси и оперативност за минимално време. Критерият отчита структурни свойства на системата в съответствие с концепцията за resilience[219].

[219] Терминът се превежда обичайно, вкл. и в стратегията за киберсигурност, като „устойчивост.“ Dobrygowski D., “Cyber Resilience: Everything You (Really) Need to Know,” World Economic Forum, 8 July 2016.

4. Адаптивност

Чрез този критерий се оценява капацитета на даден организационен модел да осигури навременно адаптиране на националната система за киберсигурност към промени в средата – нови заплахи, използване на възможностите, предоставени от нови технологии, икономически, демографски и образователни промени и др. Чрез критерия се отчита доколко даден модел позволява гъвкавост (agility) и въвеждане на иновации.

5. Взаимодействие

Чрез последния, пети критерий се оценява капацитета на даден организационен модел да осигури на взаимодействие между структури, специализирани по въпроси на киберсигурността, с други организации от системата за сигурност, съюзници и партньори и при решаване на други, „гранични“ проблеми на сигурността, например защита на критични инфраструктури, радикализация и тероризъм, противодействие на хибридни заплахи (пр. пропаганда), защита на финансовата и банкова система.

Метод за ранжиране на алтернативи

Оценяването на алтернативните организационни модели се извършва по метода AHP (Analytic Hierarchy Process), разработен от американския математик Томас Саати в началото на 80-те години на XX век[220]. Методът представлява модел на естествените човешки разсъждения при решаване на задачи за избор чрез йерархии от критерии и е апробиран в редица изследвания в социологията, екологията и икономиката.

Ранжирането на базови алтернативни организационни модели се извършва на основата на индивидуални експертни оценки. За извличане на експертните мнения е използвана деветстепенна скала за сравняване на алтернативи (критерии, модели и др.) по двойки.

Sharkov G., “From Cybersecurity to Collaborative Resiliency,” Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, 24 October 2016, pp. 3-9, https://doi.org/10.1145/2994475.2994484.

NIST, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, SP 800-160 Vol. 2 (draft), National Institute of Standards and Technology, 21 March 2018, https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft.

[220] Thomas L. Saaty T., Mathematical Principles of Decision Making: The Complete Theory of the Analytic Hierarchy Process (Pittsburg, PA: RWS Publications, 2010).

За всеки един от разработените критерии, последователно се представят предпочитанията за всяка двойка алтернативни модели. Накрая експертите оценяват степента на важност във всяка двойка критерии.

За всяка група сравнения по двойки – между алтернативни модели по даден критерий или между критерии – се оценява консистентността на оценките с използване на максималната собствена стойност на матрицата на оценките[221], която не трябва да превишава 10 %.

В индивидуални интервюта, всяко с продължителност между 1 и 1.5 часа, до завършването на изследването са извлечени оценките на 48 експерти – от администрацията и други органи на държавното управление (24 – заемащи или заемали съответни длъжности), академичния сектор (18) и фирми (6). Статистически резултати от оценките са представени в следващия раздел на отчета.

РАНЖИРАНЕ НА АЛТЕРНАТИВНИТЕ МОДЕЛИ ЗА РАЗВИТИЕ НА СИСТЕМАТА ЗА КИБЕР СИГУРНОСТ И ИЗПОЛЗВАНЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ

Този раздел представя резултатите от индивидуални интервюта с експерти и от допълнително проведени консултации и дискусии с експерти от администрацията, индустрията и академичния сектор.

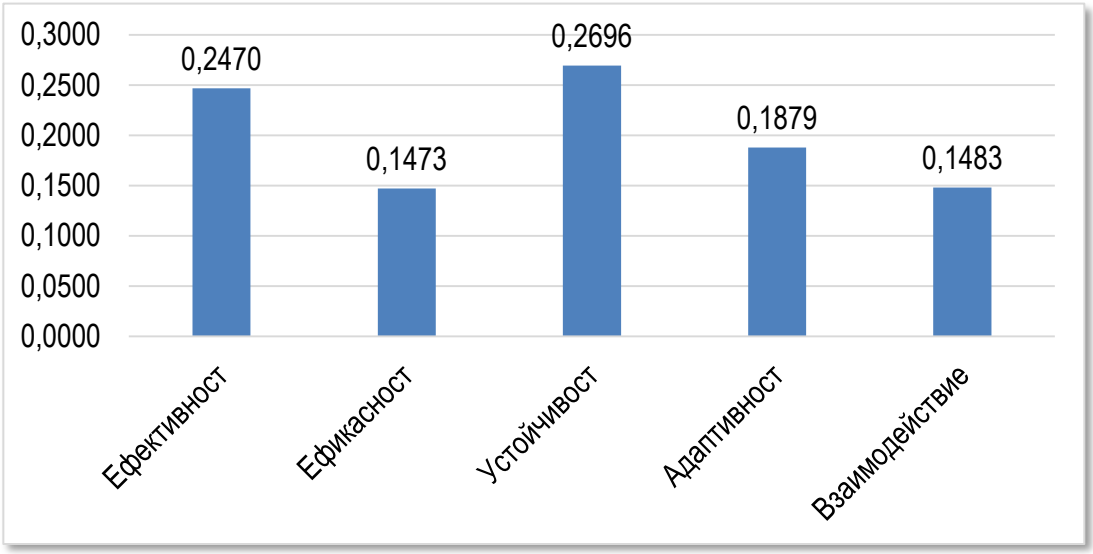
Фигура 28 представя критериалната база за ранжиране на алтернативни организационни модели. Теглото на всеки отделен критерий е определено чрез осредняване на оценките на всички участвали експерти. Най-важно значение се отдава на критерий „Устойчивост“ (27 %), следван от критерий „Ефективност“ (24.7 %) и „Адаптивност“ (18.8 %).

Предпочитането на критерий „Устойчивост“ е най-ясно изразено сред експертите от академичната общност, които поставят на второ място критерий „Адаптивност“ и едва на трето място критерий „Ефективност“ (вж. Фигура 29).

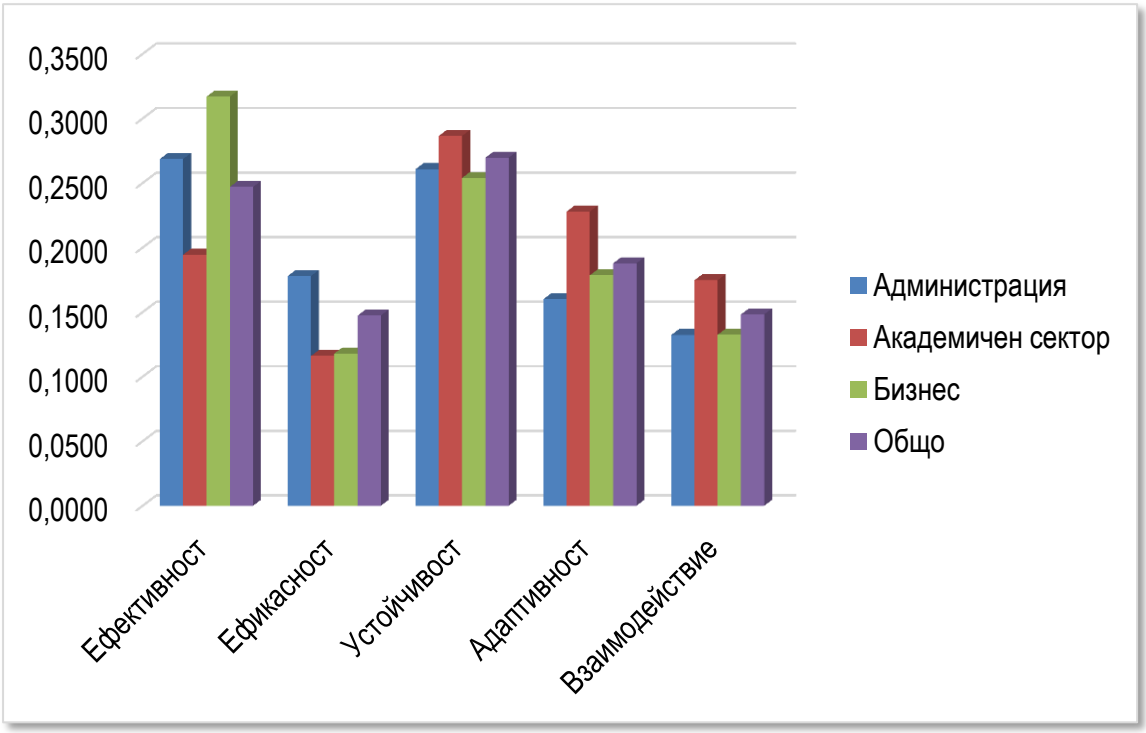
Критерий „Ефикасност“ е с най-малка тежест според оценките на всички интервюирани (14.7 %), но експертите с административен опит го поставят на трето място с тегло от 17.8 %. Този резултат може да се интерпретира по следния начин: Преобладаващото експертно мнение е, че към момента намирането на подходящо решение на проблемите на киберсигурността и ускореното развитие на съответни способности трябва

[221] Mu E., M. Pereyra-Rojas, “Understanding the Analytic Hierarchy Process,” in Practical Decision Making, Springer Briefs in Operations Research (Cham: Springer, 2017), 7-22, https://doi.org/10.1007/978-3-319-33861-3_2.

са се разглеждат приоритетно, а на цената на това решение не трябва да се отдава твърде голямо значение.



Фигура 28. Осреднени тегла на критерии сред всички интервюирани експерти



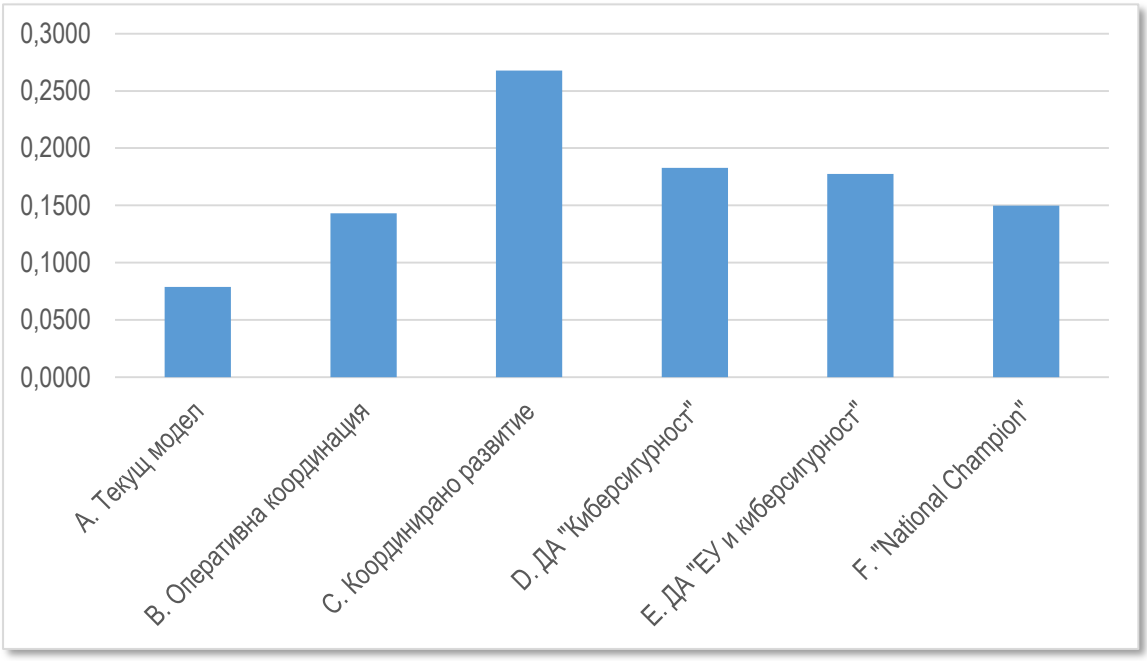
Фигура 29. Осреднени тегла на критерии по групи интервюирани експерти

Според осреднената оценка на всички участвали експерти, най-предпочитан е модел C „Координирано развитие на способности“ (26.8 %), следван от модел D „Държавна агенция Киберсигурност“, но със значително по-нисък резултат (18.3 %) и модел E „Държавна агенция ‘Електронно управление и киберсигурност’“ (17.7 %). Обобщените резултати са представени на Фигура 30.

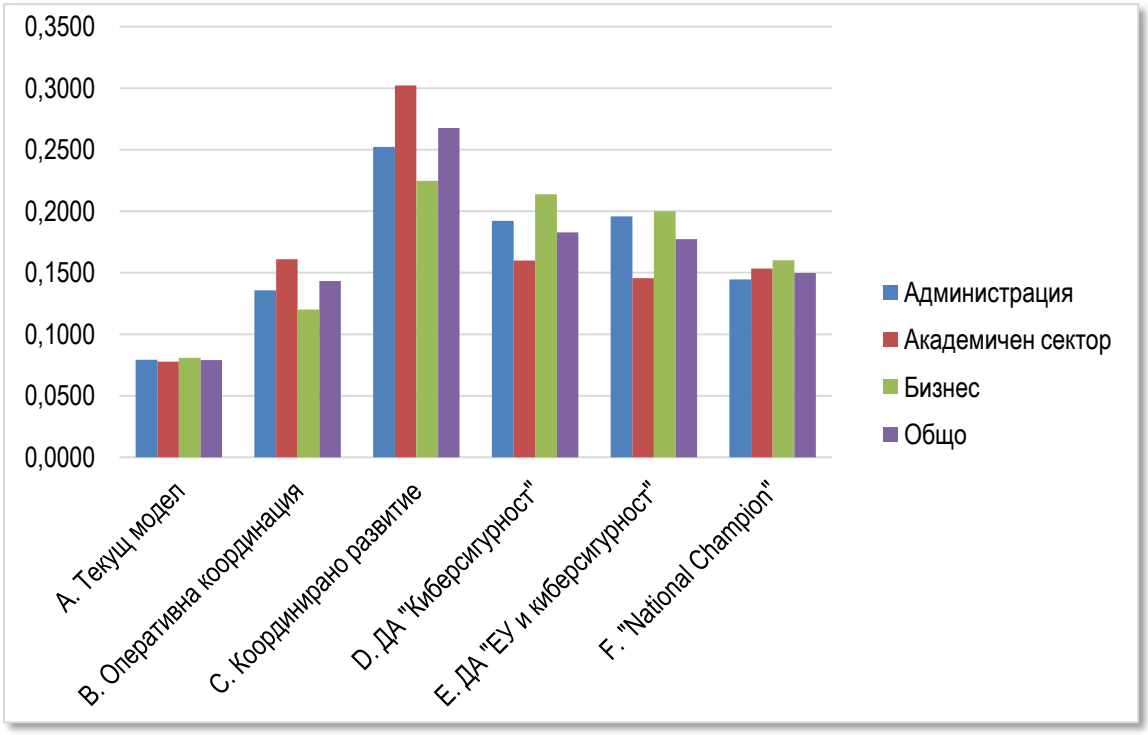
Може да се отбележи още, че като цяло организационното развитие в посока координация между отделни организации се предпочита пред развитието в посока централизация. Сумарно модели B и C получават 41 % предпочитание, в сравнение с 36 % общо за модели D и E.

Това предпочитание се наблюдава сред трите групи експерти, макар и изразено в различна степен (вж. Фигура 31). Най-голямата наблюдавана разлика е между експертите с административен опит и тези от академичния сектор, като първата група класира по-високо централизираните модели (39 % общо за модели D и E, при общо 30.5 % за двата модела от експертите от академичния сектор).

Може да се отбележи още, че между двата централизирани модела D и E предпочитан, макар и в малка степен, е този на специализирана агенция за киберсигурност (модел D).



Фигура 30. Предпочитани организационни модели по осреднени оценки на всички интервюирани експерти



Фигура 31. Предпочитани организационни модели по групи експерти

Сред интервюираните са 10 експерти с опит на висши управленски позиции – министър, заместник-министър и еквивалентни. Техните осреднени оценки не се различават качествено, но тежестта на критерии „Устойчивост“, „Ефективност“ и „Адаптивност“ са по-ясно изразени (съответно с 29.1 %, 26 % и 20.5 %). И тази група експерти дава най-малка тежест на критерий „Ефикасност“ (11.8 %), което потвърждава извода за необходимостта от належащи инвестиции в системата за киберсигурност.

В тази група предпочитанието към модел С е малко по-ясно изразено (27.1 %), а на второ място сред предпочитаните модели е модел Е с 20.7 %.

Общи изводи по отношение на базовите организационни модели:

- Текущият модел, дори при хипотезата за постепенното му усъвършенстване, е класиран най-ниско в общата оценка и във всяка от трите групи експерти. Само в 9 оценки текущият модел не е класиран на последно място, като нито един от експертите не го поставя сред първите три предпочитани модела.
- Най-важно значение при оценяване на алтернативни организационни модели се дава на критериите „Устойчивост“ и „Ефективност“, а при академичната извадка критерий „Адаптивност“ е с по-високо тегло от това на критерий „Ефективност“.
- Модел С, заложен в националната стратегия за киберсигурност, е най-предпочитан. Общо развитието в посока по-добра координация (оперативна и при развитие на способности) се предпочита пред централизацията в националната система за киберсигурност.
- По отношение на централизираните модели (D и E) известно предимство се дава на модела на специализирана агенция по киберсигурност (модел D).

Относно внедряването на иновационни технологии, и изобщо капацитета за иновации, по-подходящи са модели, които са адаптивни. Самият критерий „Адаптивност“ включва капацитета за иновации като свой същностен елемент.

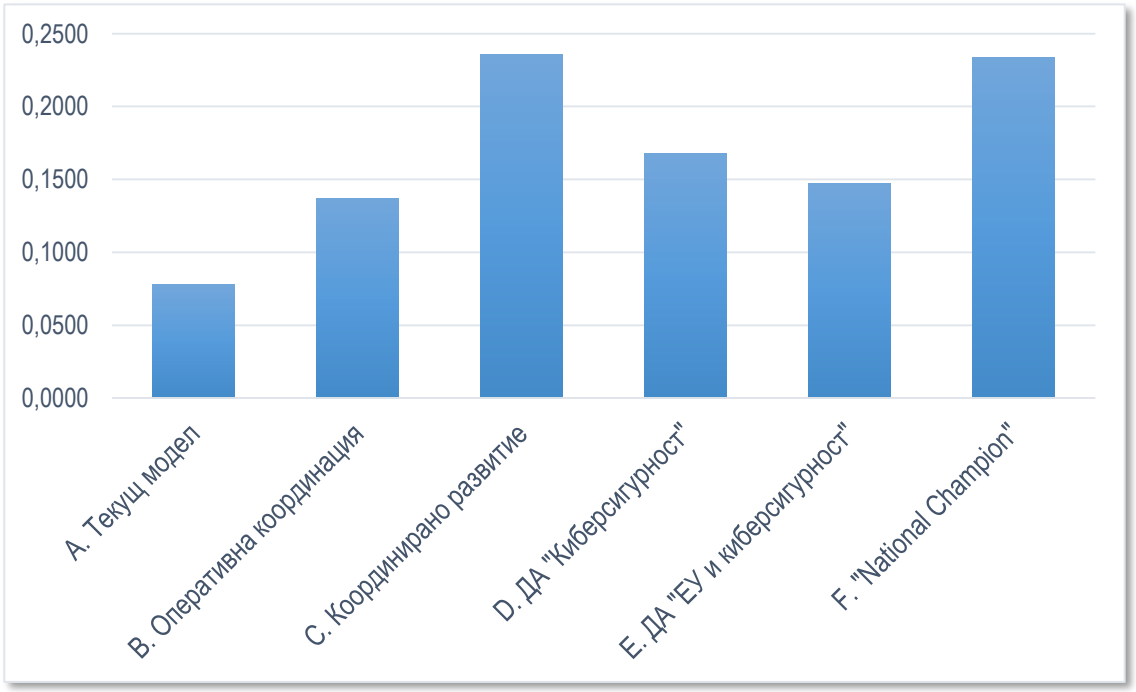
По-критерий „Адаптивност“ отново Модел С е най-предпочитан (вж. Фигура 32), но е следван в непосредствена близост с разлика от 0.2 % от фирмения модел (модел F). Като цяло, организационното развитие в посока нарастваща координация е по-силно предпочитане от развитието в посока централизация.

ОПИСАНИЕ НА ПРЕДПОЧИТАНИЯ МОДЕЛ ОТ ЕКСПЕРТИТЕ

На базата на проведените интервюта и начални изводи се препоръчва провеждане на задълбочено изследване за дефиниране на архитектурата на предпочитания модел с отчитане на препоръки за използване на добрите страни от други модели, които са приложими към предпочитания вариант.

Такова изследване и проектиране на процеси, организация, необходими технологии и изисквания към персонала, оценка на ресурсните измерения далеч надхвърля обхвата на текущото изследване, но

резултатите в отчета по този договор могат да се използват за основа за дефиниране на обхвата и изискванията на специален проект по описание на предпочитания модел под ръководството на Съвета по кибер сигурност.



Фигура 32. Ранжиране на организационни модели по критерий „Адаптивност“

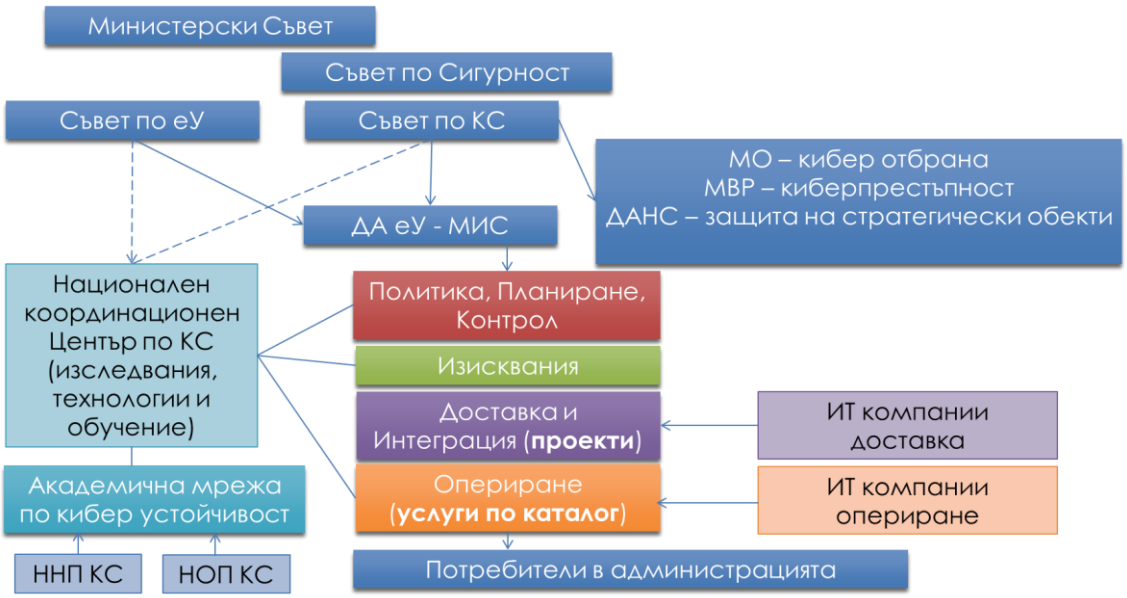
ВИЗИЯ ЗА ОРГАНИЗАЦИЯ ЗА КИБЕР УСТОЙЧИВОСТ НА ПУБЛИЧНАТА АДМИНИСТРАЦИЯ С ИЗПОЛЗВАНЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ

Изследването на различните алтернативи бе насочено към избор на модел, гарантиращ **Максимална кибер сигурност при ограничени ресурси** и критерии:

- Ефективност;
- Ефикасност;
- Устойчивост;
- Капацитет за промяна / гъвкавост;
- Взаимодействие / принос към сигурността в общ план.

Изследваните **алтернативи** от текущо състояние през специализирана агенция до частен оператор с фокус върху ролята на

новите информационни технологии (НИТ) и човешкия фактор потвърждава целесъобразността на заложения в Стратегията и Закона модел, но идентифицира и предизвикателствата в **разбиране на модела по ЗКС** и необходимостта от разработка на направленията за реализация / развитие.



Фигура 33. Модел за развитие на МИС контекста на Стратегията и Закона за кибер сигурност

Развитието на организацията с фокус върху мрежова и информационна сигурност (МИС), представено на Фигура 33 е около еволюцията на ДАЕУ с 4-те основни функции (политика, изисквания, интеграция, опериране) във взаимодействие с академичен сектор и индустрия в рамките на ръководната структура на МС, Съвет по Сигурността на МС, Съвет за е-Управление, Съвет по Кибер Сигурност.

Идентифицираните инвариантни приоритети по използване на НИТ и развитие на човешкия потенциал се предлагат като основа на Визията по усъвършенстване на организацията за кибер сигурност. Тези приоритети / инициативи са:

- Научни изследвания / сертификация на технологии;
- Обучение и сертификация на персонал;
- Взаимодействие “Администрация-Академия-Индустрия”;
- Международно взаимодействие в ЕС/НАТО еко система “кибер сигурност”.

Системата за кибер устойчивост в държавната администрация включва процеси, организации, технологии и хора, които се развиват в съответствие със Стратегията и Закона, като най-динамичната част са технологиите и те създават сериозни предизвикателства пред хората. В този контекст е важно да се установят такива процеси и организации, които в максимална степен позволяват да се използват възможностите на технологиите при наличния персонал и постоянното му усъвършенстване.

Важно е при усъвършенстване на организацията за кибер сигурност да се утвърдят принципите на:

- Единна рамка за ръководство и управление на ИТ ресурсите (COBIT – Control Objectives for Information and related Technologies);
- Архитектурен подход за стратегическо планиране (BSc – Balanced Score Cards) управление на промяната (ADKAR – Awareness, Desire, Knowledge, Ability, Reinforcement);
- Управление на портфолио от програми и проекти (MSP – Management Successful Programs, PRNINCE II);
- Управление на услуги (ITIL IT Infrastructure Library) – остойностени и платени от потребителите;
- Оптимално използване на академичния сектор за изследвания и обучение (годишни / многогодишни научни / обучителни програми);
- Оптимален аутсорсинг към индустрията за проекти и услуги (годишни / рамкови договори за доставки и услуги);
- Модел на зрялост на организацията / кибер сигурността (CMMI – Capability Maturity Model Integration).

Изследването по проекта дефинира редица препоръки и демонстрира предпочитание към модела, застъпен в Стратегията и Закона, но предизвикателството е реализацията на този модел в рамките на преходен период от 3 години при добро стратегическо планиране и управление на промяната.

Прилагайки рамката за балансирана система за показатели за развитие се очертава следното съдържание на основните четири квадранта на системата за кибер сигурност (Фигура 34):

- Принос към качеството на е-Правителството и другите аспекти на цифровизация на държавната администрация
  - Съгласие по индикаторите за киберсигурност и връзката им с качеството на е-Управлението и другите цифрови процеси в държавната администрация
  - Интеграция на въпросите по киберсигурността при стратегическото планиране в държавната администрация

- Партньорство с потребителите на системата за кибер сигурност – това са всички административни органи и оператори на съществени услуги по закона за кибер сигурност
  - Изграждане на механизъм за консултация с потребителите при участие на индустрията и академичния сектор при разширен формат
  - Създаване на система за измерване и подобряване на удовлетвореността на потребителите от работата на системата за киберсигурност
- Усъвършенстване на процесите за кибер устойчивост в системата, както и на съответните организации в RACI (Responsible, Accountable, Coordinated, Informed) матрицата на процесите.
  - Институционализация на ролята Главен информационен мениджър (ГИМ) / мениджър по киберсигурност (МКС) и съответните съвети от ниво административен орган до ниво МС
  - Изграждане на мрежа за координация на национално и международно ниво (ЕС, НАТО)
- Внедряване на нови технологии и усъвършенстване / растеж на персонала в системата.
  - Институционализиране на партньорството между администрация, индустрия и академичен сектор в изследванията и технологиите
  - Институционализиране на партньорството между администрация, индустрия и академичен сектор в подготовката и развитието на специалисти по кибер сигурност и висши мениджъри в администрацията

Промяната и продължаващото подобрение става чрез Стратегически план / План за преход обединени чрез балансирана система от показатели и ключови инициативи. Фокус върху използването на НИТ и оптимално реализиране на човешкия потенциал.

Фокусът на настоящият проект в най-голяма степен засяга четвъртият квадрант, въпреки, че в дефиниция на алтернативите се отчитат и целите в другите 3 квадранта. Този четвърти квадрант силно зависи от академичния сектор – капацитета му за изследвания и обучение по киберсигурност, както и от готовността на индустрията, съвместно с академичния сектор да разработва нови технологии и осигури ротация на персонала между администрация, академичен сектор и индустрия с цел максимална реализация на човешкия капитал.

Фигура 34. Показатели в балансираната система по 4-те квадранта: обществен интерес, потребители, процеси, усъвършенстване

Именно в този контекст след избор на предпочитана алтернатива като процеси и организация на системата за кибер устойчивост, развитието на Визията се съсредоточава на модела на взаимодействие между администрация, академичен сектор и индустрия, механизмите на международно взаимодействие и в частност рамката в ЕС, както и две фундаментално важни програми:

- Национална програма **за научни изследвания** по киберсигурност (в контекста на цялостно развитие на ефективни, ефикасни и кибер устойчиви ИТ системи / организации), която да позволи:
  - бързо внедряване на нови технологии и оптимизация на процеси и организации в системата;
  - разработка на пътни карти за развитие на тези технологии;
  - тестване и сертифициране на тези технологии.
- Национална програма **за обучение** по кибер сигурност (индивидуално и колективно – учения) с механизъм за сертификация на персонала, която да позволи:

- унифициран подход към компетентностите;
- обучение, базирано на изследвания;
- паралелно обучение в множество институции на базата на „обучение на обучаващите" и единен сертификат за квалификация.

Тази визия определя необходимостта от представителство на академичния сектор и индустрията в различните формати за консултации и вземане на решения, вкл. на ниво Съвет по кибер сигурност към МС, както и надолу по мрежата от екипи за действие по киберсигурността.

Реализацията на визията ще изисква консолидация на администрацията по въпроси на кибер сигурността чрез ролята на ГИМ, създаване на консолидирано представителство на академичния сектор (чрез съвет на програма за изследвания и програма за обучение), както и единно представителство от страна на индустрията на базата на различните ИТ асоциации.

На базата на консолидацията около постигане на целите в Балансираната система от показатели може да протекат и следващите два етапа – рационализация и оптимизация на системата в рамките на избраната алтернатива за система за киберсигурност.

Визията определя организацията за киберсигурност като екосистема с възможност за промяна при развитие на рисковете, технологиите и други елементи на средата с капацитет за адаптация като в елементите – правителство, оператори, академичен сектор индустрия, така и на секторно, национално и международно ниво.

ОСИГУРЯВАНЕ НА ИНСТРУМЕНТИ ЗА ПРОМЯНА ЧРЕЗ ИНОВАТИВНИТЕ РЕШЕНИЯ В ДЕЙНОСТТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ПУБЛИЧНИЯ СЕКТОР

Едно от важните изисквания е промяната да води до непрекъснато усъвършенстване, но и непрекъсваемост на работа на системите, зависещи от организацията за киберсигурност. Естествено промените, особено в началото, могат да доведат до възникване на нови и повишена вероятност за съществуващи рискове, затова цялостната система за управление на риска следва да се изгражда изпреварващо по отношение на промените.

Инструментите за промяна са стратегически инициативи, подкрепящи една или няколко от целите в Балансираната система от показатели. Тези стратегически инициативи са подкрепени от портфолио от проекти, чието професионално управление, заедно със специални „проекти" по промяна на

културата и стратегическа комуникация изискват професионално управление, паралелно с текущата оперативна дейност на организацията (макар и виртуална в началото) за кибер сигурност.

Голяма част от стратегическите инициативи ще са свързани с внедряване на нови технологии, сертифицирани чрез Програмата на научни изследвания, както и въвеждането на нови длъжности в резултат на програмата за обучение на персонала.

Общото ръководство на включените в програмата за промяна / трансформация обезателно е от първия ръководител на организацията за кибер сигурност, но отделните инициативи са отговорност на различни служители в рамките на това общо управление на портфолиото и на риска.

Модел на взаимодействие между ПА, академичен и бизнес сектори за ефективност, ефикасност и кибер устойчивост на ИТ системите / организациите

В основата на модела е първо консолидация на звената в академичния сектор в мрежа от центрове на компетентност, както и консолидирано представителство на индустрията, като на тази основа се предлага създаването на консултативен съвет към Съвета по киберсигурност на МС.

Консултативния съвет, макар и не споменат в Закона, може да бъде създаден с РМС и да осигури много аспектно (всички заинтересовани страни) управление / консултиране на развитието на организацията за кибер сигурност.

Консолидацията на академичните звена ефективно може да се постигне чрез Национална програма за изследване и Национална програма за обучение със съответна система за ръководство и управление, от която да се излъчи участието в консултативен съвет към Съвета по киберсигурност на МС.

Консолидацията на индустрията логично става чрез асоциации от които да се излъчи участието в консултативен съвет към Съвета по киберсигурност на МС.

Модел на международно взаимодействие за ефективност, ефикасност и кибер устойчивост на ИТ системите / организациите в публичния сектор на България

Роля на Регламент на ЕК и Съвета за създаване на Европейски център за промишлени, технологични и изследователски експерти познания

в областта на кибер сигурността и Мрежа от национални координационни центрове в контекста на проекта по Х2020 за създаване на Европейска мрежа от центрове на компетентност с хъб за иновации и операции в Брюксел е да създаде рамка за развитие на екосистема за изследвания и технологии, която да се развива както отгоре на долу, така и отдолу нагоре.

Този модел се разглежда преди всичко в сферата на изследванията и технологиите, като в посока отгоре надолу изисква включването на България в Европейски център за промишлени, технологични и изследователски експерти познания в областта на кибер сигурността при активирането му през 2021 година, а дори преди това номиниране на Национален координационен център на базата на консолидацията на академичния сектор и ИТ индустрията в сферата на киберсигурността.

По този начин се постига синергия между всички участници, както са представени на Фигура 33.

Изисквания към Национална научна програма „Ефективност, ефикасност и кибер устойчивост на ИТ системи / организации“

МОН стартира 11 национални научни програми (ННП) през 2018 година, които заедно с проектите по ОП ОНИР и НФНИ създават добра рамка за развитие на изследвания и консолидиране на академичната общност около значими проблемни области. Киберсигурността в контекста на ефективно, ефикасно и кибер устойчиво управление на информационните ресурси определено е ключова област, която заслужава да бъде подкрепена от Национална научна програма, която ще консолидира и националната мрежа от академични звена в тази област и ще позволи ангажирането ѝ с проблеми и възможности, идентифицирани от администрацията и индустрията.

Към момента работен пакет 3 „Информационна сигурност” в ННП ИКТ покрива ограничени аспекти на кибер сигурността.

Проведеното изследване определя следните направления за съставяне на многогодишна програма за работа и система за управление на програмата:

- Среда за кибер сигурност – рискове и заплахи;
- Политики и процеси за постигане на кибер сигурност;
- Организационни аспекти на кибер сигурността (административен орган, национален, международен);
- Технологии за кибер сигурност и сертификацията им (вкл. блокчейн, изкуствен интелект);
- Роля на човешкия фактор за кибер сигурността и обучение на персонала;

- Учения по кибер сигурност като услуга;
- Правни и икономически аспекти на кибер сигурността.

Изисквания към сертификационна програма за ИТ лидери и административни ръководители за Главни Информационни мениджъри / Мениджъри на кибер устойчивостта „Ефективност, ефикасност и кибер устойчивост на ИТ системи / организации“

Анализът на различни бакалавърски, магистърски, докторски и общо квалификационни програми в ограниченото по време и ресурс изследване ни позволява да направим следните препоръки в областта на изисквания към сертификационна програма за ИТ лидери и административни ръководители:

- Необходимо е дефиниране на минималните изисквания за специалистите по кибер сигурност и общо за служителите в администрацията с разработка на обучение и сертификация за входно ниво;
- Базовото образование в бакалавърски и магистърски програми следва да отговаря на компетентностите, определени в ЕС;
- Квалификационното обучение на специалистите следва да отговаря на изисквания определени от ДАЕУ;
- Разработването и реализацията на утвърдените програми следва да се реализира от академичната общност чрез Национална програма под ръководството на Съвета по кибер сигурност;
- Периодичните брифинги и тестове за специалисти по кибер сигурност и общо за служители в администрацията следва да се извършват ежегодно;
- Проверката на нивото на готовност и координация по определени въпроси / сценарии следва да се осъществява чрез учения поне веднъж годишно;
- Обучението следва да се обвърже с изследванията за нови технологии и свързаните с тях промени в процеси и организация.

УПРАВЛЕНИЕ НА ПРОМЯНАТА ЗА ПОВИШАВАНЕ НА КИБЕР УСТОЙЧИВОСТТА В ДЕЙНОСТТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ПУБЛИЧНИЯ СЕКТОР

Избраната методика за това изследване, отчитайки ограниченото време и финансиране, което лимитира кръга на въвлечени експерти и дълбочината на прилагане на избраните методи включва следните стъпки:

1) Анализ на средата по метода PEST.
2) Дефиниране на основни измерения за разработване на алтернативи.
3) Синтез на алтернативи и техния SWOT анализ.
4) Оценка и избор на алтернатива по метода AHP.
5) Описание на предпочитаната алтернатива в съответствие с архитектурата на организацията за кибер сигурност на е-Управлението.
6) Определяне на стратегия за реализация на стратегията като Балансирана система от показатели (BSc).
7) Дефиниране на стъпки за промяна по метода ADKAR.

Изборът да се извърви целия път по такъв обхватен проект е именно с цел да се изработят основата на настоящата визия и да се определят задачи за последващи изследвания по детайлно планиране и управление на прехода от текущото състояние, към това определено във визията.

Това позволява да се идентифицират инициативи, инвариантни на институционалния избор за вариант за организацията / системата за кибер сигурност / устойчивост в държавната администрация, и да се работи паралелно по подготовка на промяната, заедно с оформяне на крайното решение за облика на системата.

Като се съсредоточи върху постигането на петте цели по долу, моделът ADKAR може да се използва за ефективно планиране на промените на индивидуално и организационно ниво:

- **Осъзнаване** (на необходимостта от промяна);
- **Желание** (да участвате и подкрепите промяната);
- **Знания** (как да променяте);
- **Способност** (за прилагане на необходимите умения и поведение);
- **Укрепване** (за поддържане на промяната).

Промяната в рамките на 3 години изисква диагностика за готовността на системата да бъде променена от текущо към целево състояние и подготовката ѝ за приложение на плана за промяна по модела ADKAR (Фигура 35). След оценката и подготовката (в рамките на първата половина

на първата година, като етап 0 – подготвителен), промяната включва следните 3 етапа:

1) Структурна консолидация – година 1 (втора половина);
2) Рационализация – година 2;
3) Оптимизация – година 3.

Фигура 35. Елементи на оценка и подготовка за управление на промяната на организацията за кибер сигурност

Стратегията за преход следва да отчете следните препоръки:

- Установете доверие с всички заинтересовани страни (в това число Индустрия и Академичен сектор);
- Изградете партньорство с клиентите;
- Вдъхновете хората в организацията с ясна визия;
- Демонстрирайте стратегическата гъвкавост;
- Изградете единството на ръководството;
- Осигурете гъвкавост в насочване на ресурсите;
- Формирайте отношение „Мога да го направя“ и „Просто го направи“ при промяна на културата.

Управление на промяната (по Котър) е процес от 8 стъпки:

1) Чувство за неотложност
2) Ръководен екип
3) Визия и стратегия

4) Ефективна комуникация
5) Отстраняване на препятствията
6) Краткосрочни победи
7) Налагане на вълна след вълна от промени
8) Нова култура за устойчивост на ново поведение

Този процес се разполага в трите етапа по-горе и се подкрепя от резултатите на ADKAR-диагностиката и подготовката на средата.

Независимо колко упорито се опитваме да останем последователни, емоциите играят огромна роля в нашето поведение и като знаем петте етапа на приемане на промяната, можем да очакваме реакциите на служителите си и да планираме своя отговор (и график) предварително. Етапите са: отричане, гняв, договаряне, депресия и приемане.

Именно в този контекст е важно да отчетем, че усилията за управление на промените са успешни, когато се създаде нова култура в организацията и у заинтересованите страни / клиенти. Стратегическата комуникация – външна и вътрешна – е критичният фактор за развитието и укрепването на новата култура. Този аспект се разглежда отделно от цялостното управление на промените, поради важността и цялостния му характер. По същия начин, по който трябва да измерваме удовлетворението на клиентите, за да стимулираме промяната към външния свят, се нуждаем от правилно измерване на развитието на организационната култура и зрялост, за да стимулираме вътрешните промени. Вътрешната и външната стратегическа комуникация са насочени към укрепване на положителните постижения и оформяне на промените в областите, в които все още имаме проблеми. Основен урок: това усилие трябва да се превърне в отделна стратегическа инициатива и в същото време да се интегрира с други ключови инициативи като инструмент за поддържане на обратна връзка и активно оформяне на средата.

С приемането на Закон за киберсигурност на 31.10.2018 текат сроковете за изграждане на ключови елементи от организацията за кибер сигурност / устойчивост, а настоящото изследване предлага и редица други линии на развитие, които следва да се интегрират в единен план за управление на промяната и пълна реализация на Стратегията за кибер сигурност „Кибер устойчива България 2020“ (която подлежи на актуализация основно в контекста на забавеното ѝ изпълнение и променена среда, както и необходимост да се развие във времето към хоризонт 2025/2030).

ЗАКЛЮЧЕНИЕ

Независимо от краткия период (под 3 месеца) и ограничено финансиране на базата на ясно формулираните от ИПА изисквания в техническата спецификация за изследването, екипът успя да осъществи и шестте предвидени дейности, да проведе анкета с широк кръг експерти, да организира две консултации – по резултатите от първата част на изследването (първа глава и елементи от втора и трета глава), както и заключителна валидация на резултатите с участие на представители на всички основни институции по Закона за кибер сигурност и Заявителя (ИПА).

Ползотворното сътрудничество с ИПА позволи резултатите от изследването да се представят публично на международна конференция на института на 12 и 13.12.2018 г. на тема „Кибер сигурност в публичната администрация“ (София).

Основните изводи

✓ С приемането на Концепцията „Кибер устойчива България 2020” през 2014 г., последвана от Стратегията за кибер сигурност „Кибер устойчива България 2020” през 2016 г. и Закона за КС през 2018 г. се преодолява изоставането на България в НАТО и ЕС на ниво документи от общата архитектура на организацията за кибер сигурност (Фигура 1).

✓ Избраният модел в Стратегията и Закона имат подкрепата на експертите и сега важното е, след 4 години фокусирани върху документи да постигнем поне ниво на зрялост 3 по избрания модел за следващите 3 години – 2019-2021(22) г.

✓ Реализацията на Стратегията / Закона е сериозно трансформационно усилие за промени в процеси, организация, технологии и хора. Липсата на единна програма за приложение на Стратегията и Закона е проблем, като част от самата програма е организацията за ръководство и управление на изпълнението ѝ, ресурсно осигуряване в периода 2019-2021 г.

✓ Необходима е национална програма за изследвания и технологии / сертификация по кибер сигурност, която изпреварващо по отношение на програмата за прилагане на Закона да осигури необходимото разбиране на технологични, организационни и други аспекти на организацията за кибер сигурност.

✓ Човешкия фактор се очертава като най-критичен в сравнение с финанси, достъпност до технологии, дори желанието / готовността за промени в процесите и организацията и това изисква единно управление на процеса на подготовка и сертификация на специалисти.

✓ Решаване на проблемите, свързани с технологии и хора изисква иновационен модел за взаимодействие между администрация, академичен сектор, индустрия.

✓ Преодоляване на проблемите в сферата на кибер сигурността за България може да бъде подпомогнато чрез развитие на сътрудничеството с НАТО (NCIA) и ЕС (ENISA), както и на двустранна и регионална база.

ПРЕДЛОЖЕНИЯ

✓ Изследването предлага обща архитектура за анализ на организацията за кибер сигурност, която може да се използва за извършване на задълбочен одит и оценка на степента на зрялост – необходима стъпка преди прехода към целевия модел.

✓ Използваният подход за разработка и избор на алтернативи за организация на системата за кибер сигурност следва да се приложи по-задълбочено за дефиниране в детайли на избрания модел.

✓ Предлаганият модел за Модел за развитие на МИС контекста на Стратегията и Закона за кибер сигурност може да се приложи за създаване на „коалиция“ за промяна на системата – например консултативен съвет от индустрията и академичния сектор към Съвета по кибер сигурност.

✓ За подобряване на ефективността и ефикасността на изследванията и обучението е необходимо да се изгради национална мрежа от центрове на експертиза, както и федерирана мрежа от кибер полигони между администрация-академия-индустрия с добро управление от Национален координационен център на компетентност по кибер сигурност (в съответствие и с обсъждания Европейски регламент).

✓ ДАЕУ следва да обвърже наредбата за минималните изисквания с програма за сертификация на технологии и програма за сертификация на персонал в сферата на МИС, като взаимодейства с академията и индустрията у нас, но и на ниво НАТО и ЕС.

✓ За развитие на организацията за кибер сигурност / МИС е важно да се разработи подробна Балансирана система от показатели.

✓ Преходът следва да се извърши по интегриран план за управление на промяната с подготвителен и три основни етапа при използване на единен подход.

Екипът изказва специална благодарност на директора на ИПА – г-н Павел Иванов и координатора на проекта от ИПА – г-жа Елена Димкина, както и на всички експерти, участвали в анкетата, кръглата маса и работната среща за валидация на резултатите.

Краткото време за изследването и краткия срок за събиране на екипа бяха сериозни предизвикателства. Голямата заетост на участниците в екипа създаде трудности в управление на проекта, дори при използване наистина на най-адекватния метод в такива условия SCRUM.

В този контекст и предвид важността на темата, предлагаме работата да продължи с отделен проект през 2019 г. за постигане на следващо ниво на анализ на събраните данни и предложения от участниците в анкетата и кръглата маса / среща за валидация, както и да се предвиди специален проект на ИПА за създаване на Национална програма за обучение и сертификация по кибер сигурност в Публичната администрация (вкл. с провеждането на регулярни учения).

Друга част от предложенията предлагаме да бъдат обсъдени с ДАЕУ, МОН, МО, МВР, ДАНС и СС- МС за набелязване на мерки по подобряване на организацията за кибер сигурност и използване на иновативни технологии в България в контекста на членството ни в НАТО и ЕС, желаното лидерство в региона на Балканите и Черноморието.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ

[1] Brussels Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 11-12 July 2018, Press Release (2018)074, accessed on 2.11.2018.

[2] Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, 20 May. 2012, Press Release (2012) 062, Issued on 20 May 2012, pp. 12-13.

[3] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, Official Journal of the European Union, L 239/36, 19.9.2017.

[4] Council of the European Union, Action Plan for implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 12 December 2017.

[5] Council of the European Union, Annual Report on the Implementation of the Cyber Defence Policy Framework, available from, http://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf, accessed on 5.11.2018.

[6] Council of the European Union, Council Conclusions on Cyber Diplomacy, available from: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf, accessd on 5.11.2018.

[7] Council of the European Union, Council conclusions on malicious cyber activities – approval, Brussels, 16 April 2018, http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf, accesed on 5.11.2018.

[8] Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - Council conclusions (20 November 2017).

[9] Council of The European Union, Draft Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available from: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011357%202013%20INIT, accessed on 5.11.2018.

[10] Council of the European Union, EU Cyber Defence Policy Framework, Brussels, 18 November 2014.

[11] Council of the European Union, Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017.

[12] Cyber Defence Pledge 08 Jul. 2016, Press Release (2016) 124 Issued on 08 Jul. 2016.

[13] Deshpande A., K. Stewart, L. Lepetit, S. Gunashekar: Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report prepared for the British Standards Institution (BSI), May 2017, 34 p.

[14] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[15] Dobrygowski D., "Cyber Resilience: Everything You (Really) Need to Know," World Economic Forum, 8 July 2016.

[16] European Commission, EU Cybersecurity plan to protect open internet and online freedom and opportunity, Brussels, 7 February 2013.

[17] European Parliament, 2014-2019, REPORT on cyber defence (2018/2004(INI)), European Commission, Bruselss, 25.5.2018. COM/2018/435.

[18] Fridgen, G., F. Guggenmos, J. Lockl, A. Rieger, A. Schweizer, N. Urbach: Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process. Reports of the European Society for Socially Embedded Technologies: vol. 2, no. 13, ISSN 2510-2591, https://doi.org/10.18420/blockchain2018_10

[19] Harnessing the Blockchain Revolution: CompTIA's Practical Guide for the Public Sector. Research Report, July 2018. https://www.comptia.org/resources/harnessing-the-blockchain-revolution-comptia-s-practical-guide-for-the-public-sector

[20] http://www.natoschool.nato.int/, accessed on 15.10.2018.

[21] http://www.ndc.nato.int/, accessed on 15.10.2018.

[22] https://ccdcoe.org/, accessed on 15.10.2018.

[23] https://cert.europa.eu/cert/plainedition/en/cert_privacy.html, accesed on 5.11.2018.

[24] https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/4369, accessed on 28.10.2018.

[25] https://www.eda.europa.eu/what-we-do/activities/activities-search/captech-components, accessed on 28.10.2018.

[26] https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx, accessed on 15.10.2018.

[27] https://www.ncia.nato.int/Pages/homepage.aspx, acessed on 15.10.2018.

[28] https://www.nciss.nato.int/, accessed on 15.10.2018.

[29] https://www.sto.nato.int/publications/Pages/default.aspx, accessed on 22.10.2018.

[30] Ishizaka A., Ph. Nemery: Multicriteria decision analysis: methods and software. Wiley, 2013, 328 p.

[31] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final.

[32] Karanjia B., A. G. Karanth, S. Veerapaneni, S. Goswami, A. Sharma, M. Boda: Blockchain in Public Sector: Transforming government services through exponential technologies. Deloitte Touche Tohmatsu India LLP, January 2018, 32 p.

[33] Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 Nov. 2010, Press Release (2010) 155, Issued on 20 Nov. 2010, p. 11.

[34] Mu E., M. Pereyra-Rojas, “Understanding the Analytic Hierarchy Process,” in Practical Decision Making, Springer Briefs in Operations Research (Cham: Springer, 2017), 7-22, https://doi.org/10.1007/978-3-319-33861-3_2.

[35] Multi-criteria analysis: a manual. Department for Communities and Local Government: London, January 2009, ISBN: 978-1-4098-1023-0

[36] NATO (2011). Defending the Networks: The NATO Policy on Cyber Defence.

[37] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM/2017/0477 final - 2017/0225 (COD).

[38] Quatation of Antonio Missiroli, NATO assistant secretary general for emerging security challenges. “Nato’s full operational capability in terms of cyber security is expected by 2023,” in panel discussion on the future of NATO’s cyber policy at the 2018 European Cybersecurity Forum in Krakow, https://www.computerweekly.com/news/252450425/Nato-to-be-fully-operational-in-cyber-space-by-2023, accessed on 22.10.2018.

[39] Saaty T., Mathematical Principles of Decision Making: The Complete Theory of the Analytic Hierarchy Process (Pittsburg, PA: RWS Publications, 2010).

[40] Sharkov G., “From Cybersecurity to Collaborative Resiliency,” Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, 24 October 2016, pp. 3-9, https://doi.org/10.1145/2994475.2994484.

[41] Signing of Memorandum of Understanding on Cyber Defence, available on: https://www.nato.int/cps/ie/natohq/photos_136551.htm, accessed on 15.10.2018.

[42] Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, SP 800-160 Vol. 2 (draft), National Institute of Standards and Technology, 21 March 2018, https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft.

[43] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 Sep. 2014, Press Release (2014) 120, Issued on 05 Sep. 2014, pp. 15-16; NATO Policy on Cyber Defence, endorsed by Allied Defence Ministers in June 2014.

[44] Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, 09 Jul. 2016, Press Release (2016) 100 Issued on 09 Jul. 2016, pp. 15-16.

[45] Актуализирана стратегия за национална сигурност на Република България, приета с Решение на Народното събрание от 14.03.2018 г.

[46] Директива 2013/40 на Европейския парламент и на Съвета относно атаките срещу информационните Системи

[47] European commission, Joint communication to the European Parliament, the Council, the European economic and social committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 07.02.2013.

[48] Закон за Държавна агенция „Национална сигурност“

[49] Закон за електронната идентификация, в сила от 21.11.2016 г.

[50] Закон за електронните съобщения

[51] Закон за електронния документ и електронния подпис

[52] Закон за електронното управление

[53] Закон за защита на класифицираната информация

[54] Закон за киберсигурност, приет от Народното събрание на 31.10.2018 г., обн. ДВ. бр.94 от 13.11.2018г.

[55] Закон за управление и функциониране на системата за защита на националната сигурност, в сила от 01.11.2015 г.

[56] Иновационна стратегия за интелигентна специализация на Република България 2014-2020 г.

[57] Министрите имат две седмици да направят предложения за съкращения в администрациите си. Дневник, 05.12.2018 г., https://www.dnevnik.bg/bulgaria/2018/12/05/3357047_ministrite_imat_dve_sedmici_da_napraviat_predlojeniia/.

[58] Национална стратегия за кибер сигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г.;

[59] Оперативна програма „Иновации и конкурентоспособност“ 2014-2020 90

[60] Правилник за дейността, структурата и организацията на Държавна агенция "Електронно управление", приет с постановление № 274 от 28 октомври 2016 г.

[61] Предложение за Регламент на Европейския парламент и на Съвета за създаване на Рамковата програма за научни изследвания и иновации „Хоризонт Европа“ и за определяне на нейните правила за участие и разпространение на резултатите.

[62] Предложение за регламент на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове

[63] Програма „Цифрова България 2020“

[64] Проект на Постановление на Министерския съвет за приемане на Правилник за дейността, структурата и организацията на Държавно предприятие „Единен системен оператор“, публикуван за обществено обсъждане на 09.02.2017 г., приключило обществено обсъждане на 13.03.2017 г.

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО ПУБЛИЧНА
АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ

ПРИЛОЖЕНИЯ КЪМ ДОКЛАД

ОТ ПРОВЕЖДАНЕ НА ИЗСЛЕДВАНЕ ЗА УКРЕПВАНЕ НА АДМИНИСТРАЦИЯТА

НА ТЕМА:

КИБЕРСИГУРНОСТ И ВЪЗМОЖНОСТИ ЗА ПРИЛОЖЕНИЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ

НЛКВ – БАН,
София, 2018 г.

Проект „Работим за хората“ - укрепване капацитета на институциите за посрещане на предизвикателствата на съвременните публични политики“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ПРИЛОЖЕНИЕ 1:
КЛЮЧОВИ ТЕРМИНИ В НАЦИОНАЛНАТА СТРАТЕГИЯ ЗА КИБЕРСИГУРНОСТ „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ“

Националната стратегия за кибер сигурност „Киберустойчива България 2020” за първи път предлага систематизирани определения за основните термини и понятия в областта на кибер сигурността. В същото време за някои от използваните термини са предложени повече от едно определение. На първо място това са определения на **двете основни понятия** в областта на кибер сигурността – *кибер пространство* и *кибер сигурност*.

Кибер пространство

Интерактивна среда от електронни мрежи и информационна инфраструктура използвана за създаване, унищожаване, съхранение, обработка, обмяна на информация, управление на обекти, системи и услуги.

Кибер пространство (2) – сферата, в която информационната среда, съставена от независими мрежи на информационни системни инфраструктури, включително интернет, телекомуникационни мрежи, компютърни системи, вградени процесори и контролери, се използват за обработване, съхраняване и пренасяне на информация и дейности на потребители.

Кибер сигурност

Състояние, определено и измерено чрез нивото на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги.

(Според ISO 27000) – опазване на конфиденциалността, интегритета (целостта) и наличността на информацията (триада на информационната сигурност – КИН, или CIA - Confidentiality, Integrity, Availability)

(ЕС) – Под кибер сигурност обикновено се разбират предпазните мерки и действия, които могат да бъдат приложени за предпазване на кибер пространството както в гражданската, така и във военната област, от заплахи, които са свързани с неговите независими мрежи и информационна инфраструктура или могат да нарушат работата им. Целта на кибер сигурността е да се съхрани наличността и целостта на мрежите и инфраструктурата, както и поверителността на информацията, която се съдържа в тях.

Дефинирани са инфраструктурите, представляващи особено важна част от националната икономика и общество, и основната среда на дейностите по кибер сигурност.

Критична инфраструктура (КИ)

Система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни негативни последици за Република България в резултат на невъзможността да се запазят тези функции.

Критична комуникационна и информационна инфраструктура (ККИИ)

Системи, услуги, мрежи и инфраструктури, които са жизнено важна част от националната икономика и общество и осигуряващи важни стоки и услуги, деструктивното въздействие върху които би могло да има сериозно влияние на жизнено важни функции на обществото. Критична информационна инфраструктура са както мрежите, каналите, така и системите за управлението и поддържането им.

Предложени са определения и на основните нежелани дейности/събития в кибер пространството.

Кибер престъпление

Действия, насочени към и/или използващи кибер пространството, които се определят като престъпни в националното и/или международното законодателство.

Кибер престъпност (ЕС)

Обхваща традиционни престъпления (напр. измами, фалшифициране и кражба на самоличност), престъпления, свързани със съдържанието (напр. онлайн разпространение на детска порнография или подбуждане към расова омраза), и престъпления, които са възможни само при компютри и информационни системи (например атаки срещу информационни системи, предизвикване на отказ на услуга и зловреден софтуер).

Кибер атака

Злонамерена дейност, която цели да разруши, да осигури контрол над компютърна среда/инфраструктура, да наруши интегритет на данни или откраднe контролирана информация.

(НАТО) – действия, предприети за нарушаване, отхвърляне, влошаване или разрушаване на информация, намираща се в компютър и/или компютърна мрежа, както и на самите компютри и/или компютърни мрежи.

(ISO 27000) – опит за разрушаване, разкриване, променяне, забрана, кражба ли получаване на неупълномощен достъп до или реализация на неупълномощено използване на актив.

Кибер инцидент

Неоторизирани или неочаквани дейности в КИС, при които автоматизираните мерки не са достатъчни за предотвратяване на негативни въздействия, но за които експертите по кибер защита могат да предупредят.

(НАТО) – неочаквано събитие в кибер пространството, което, с или без криминален умисъл, би могло да промени кибер сигурността чрез фактическо или потенциално излагане на опасност на конфиденциалността, целостта или наличността на информационната система или на информацията, която системата обработва, съхранява или пренася, нарушаване или потенциално нарушаване на политиките за сигурност, процедурите за сигурност или политиките за приемливо използване.

(ISO 27000) – събитие или поредица от нежелани или неочаквани събития, свързани със кибер сигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията.

Кибер война

Всеки политически мотивиран конфликт в кибер пространството, характеризиращ се с кибер атаки срещу компютърните и информационните системи на противника.

Кибер война (2)

Военни действия, водени във виртуалното пространство със средства и методи на информационните технологии. В по-широк смисъл, това представлява поддръжката на военни операции, провеждани в традиционните оперативни пространства – сухопътно, морско, въздушно и космическо – чрез действия, извършвани във виртуалното пространство.

Хибридна заплаха

Идентифицирано намерение и способност от държавен или недържавен субект, който може да използва хибридна стратегия. Оценява се, че за да използва хибридна стратегия, един недържавен субект

притежава способността да прилага всички, или почти всички елементи на силата, характерни по-скоро за една суверенна държава.

Хибриден модел на водене на война

Използва се за обозначаване на съвременни конфликти, обединяващи конвенционални и неконвенционални действия, кибер атаки, психологическо и икономическо въздействие, кампании за дезинформация, инфилтрация на информационната среда, създаване на паника, финансиране на нарочно създадени политически субекти, с цел промяна на външнополитическата линия на набелязаните противници и други действия за постигане на политически и стратегически цели. Хибридният модел е специфична проява на дадена хибридна стратегия, използвана от конкретен противник.

Определени са също субектите и дейностите за противодействие на нежелани събития и гарантиране на нормално протичане на процесите в кибер пространството.

Computer Emergency Response Team (CERT)

Организация, която изучава уязвимостите в кибер пространството и подпомага жертви на хакерски атаки, осигурява 24/7 услуги, споделя информация за повишаване на кибер сигурността и координира отговори на заплахи на кибер сигурността (известни в различни организационни форми – CSIRT, CIRC и др.).

Кибер отбрана

Интегрирана система, свързана с изпълнението на всички мерки по защитата на комуникационно-информационните системи на въоръжените сили от кибер атаки за осигуряване постигането на военно-стратегическите цели.

Посочени са и определения на термини с общо приложение в областта на сигурността, като е посочено тяхното съдържание в контекста на Стратегията за кибер сигурност.

Устойчивост (Resilience, NIST)

Способност, свойство (на организацията) бързо да се адаптира и да се възстановява от известни или неизвестни промени в околната среда чрез цялостно и последователно реализиране на управлението на риска, управление при извънредни ситуации и планиране на непрекъснатост на дейностите/операциите.

Уязвимост

Неустойчивост на информационната система, на вътрешния контрол и процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата.

Заплаха

Факт или събитие с потенциал, който може да нанесе сериозни вреди на дейността на организации, активи, хора или даже на държавата чрез неоторизиран достъп, разрушаване, разкриване и промяна на данни, и/или отказ от услуги. (ISO 27000: потенциална причина за нежелан инцидент, който може да причини вреда на дадена система или организация).

Риск

Потенциалната възможност дадена заплаха да бъде реализирана, като се експлоатира уязвимостта на активите, за да се причини вреда.

Нарушение

Неоторизирано действие, което преодолява механизмите за сигурност на системите.

ПРИЛОЖЕНИЕ 2:
КЛЮЧОВИ ТЕРМИНИ В ЗАКОНА ЗА КИБЕРСИГУРНОСТТА

Със *Закона за киберсигурност, приет на 31 октомври 2018 г.* в българското законодателство се въвеждат изискванията на Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза. В параграф 3 от Допълнителните разпоредби на проекта се предлага систематизирано съдържанието на основните термини по смисъла на закона в областта на обществените отношения, които той регулира. Съществен принос на проекта на закон са легитимните определения на **двете основни понятия** в областта на кибер сигурността – *киберпространство и киберсигурност*.

Киберпространство

Глобална мрежа от системи за компютърна обработка, електронни съобщителни мрежи, компютърни програми и данни.

Киберсигурност

Предпазни мерки и действия, които могат да бъдат приложени за предпазване на кибер пространството както в гражданската, така и във военната област от заплахи, които са свързани с неговите независими мрежи и информационна инфраструктура, или могат да нарушат работата им. Кибер сигурността обхваща три основни стълба: мрежова и информационна сигурност, правоприлагане и кибер отбрана.

Следват предложени в закона правни дефиниции на основни дейности и понятия в кибер пространството, обхващащи един доста по-широк кръг от термини.

Онлайн място за търговия

Цифрова услуга, която дава на потребители и/или търговци – по смисъла на определенията, съдържащи се съответно в чл. 4, параграф 1, букви „а” и „б” от Директива 2013/11/ЕС на Европейския парламент и на Съвета (18), възможността да сключват договори за онлайн продажби или услуги с търговци или на уебсайта на онлайн мястото за търговия, или на уебсайт на търговеца, използващ електронни услуги, предоставяни от онлайн мястото за търговия.

Онлайн търсачка

Цифрова услуга, която дава възможност на ползвателите на интернет да извършват търсене по правило на всички уебсайтове или уебсайтове на

даден език въз основа на запитване по всякакви теми под формата на ключова дума, израз или друг вид въведени данни, в отговор на което тя подава интернет връзки, съдържащи информация, свързана с исканото съдържание.

Система за имена на домейни (Domain Name System – DNS)

Йерархично разпределена мрежова система за именуване на домейни, която разпределя заявки за имена на домейни.

Регистър на имена на домейни от първо ниво

Субект, който извършва и управлява регистрацията на имената на интернет домейни в специален домейн от първо ниво (top-level domain — TLD).

Цифрова услуга

Услуга по смисъла на чл. 1, параграф 1, буква „б" от Директива (ЕС) № 2015/1535 на Европейския парламент и на Съвета (17) от категориите, посочени в приложение № 2 към закона.

Цифрова инфраструктура

Инфраструктура, която включва точка за обмен в интернет, доставчици на DNS услуги и регистри на имената на домейни от първо ниво.

Компютърна услуга 'в облак'

Цифрова услуга, която дава възможност за достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно.

Съществени услуги

Услуги, чието предоставяне зависи от електронни съобщителни мрежи или от информационни системи и чието прекъсване може да окаже значително увреждащо въздействие върху предоставянето на социални или икономически дейности в:

а) един от следните сектори: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода, цифрова инфраструктура, или

б) една от следните цифрови услуги: онлайн място за търговия, онлайн търсачка и компютърни услуги в облак.

Технически стандарт

Правило по смисъла на чл. 2, параграф 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно Европейска стандартизация.

Спецификация

Техническа спецификация по смисъла на чл. 2, т. 4 от Регламент (ЕС) № 1025/2012.

Точка за обмен в интернет

Мрежово средство, което дава възможност за свързване на повече от две независими автономни системи преди всичко с цел улесняване на обмена на интернет трафик. Чрез точка за обмен в интернет се осъществява свързване само на автономни системи. Свързването чрез точка за обмен в интернет не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин.

Мрежа и информационна система

а) електронна съобщителна мрежа по смисъла на чл. 2, буква „а" от Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно обща регулаторна структура за електронни комуникационни мрежи и услуги (Рамкова директива) (ОВ, L 108, 24.4.2002);

б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработва автоматично цифрови данни, или

в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от букви „а" и „б", с цел обработване, използване, защита и поддръжка.

Специално внимание в закона е отделено на определянето на основните нежелани дейности/ събития в кибер пространството.

Отказ от услуга

Кибер атака, при която извършителят се стреми да направи машина или мрежов ресурс, недостъпен за предназначените си потребители, временно или за неопределено време да наруши услугите на хост, свързан с интернет. Отказ от услуга обикновено се осъществява чрез наводняване на целевата машина или ресурс с излишни искания в опит да се претоварят

системите и да се предотврати изпълнението на някои или на всички легитимни искания.

Зловреден софтуер

Софтуер, който умишлено е включен или вмъкнат в система с цел нанасяне на вреда.

Зловреден интернет трафик

Аномалии на интернет трафика, предизвикани от хардуерни или софтуерни повреди на интернет пакети със злоумишлено модифицирани опции.

Определени са видовете инциденти в кибер пространството, като класификацията им се определя по Методика на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) в зависимост от типа на атаката. Определенията на същите са градирани по степента на негативно въздействие както върху публичния сектор, така и върху бизнеса и предоставянето на услуги на гражданите.

Киберинцидент

Събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията.

Киберинцидент със среден приоритет

Киберинцидент, който има сериозно въздействие върху средна организация или който представлява значителен риск за голяма организация или за по-широко/местно управление.

Киберинцидент с висок приоритет

Киберинцидент, който има сериозно въздействие върху голяма организация или върху по-широко/местно управление или който представлява значителен риск за предоставянето на съществените услуги на голяма част от българското население или върху икономиката на Република България.

Киберинцидент със значителен приоритет

Киберинцидент, който оказва сериозно въздействие върху дейността на правителството, върху предоставянето на съществени услуги на голяма

част от българското население или върху икономиката на Република България.

Мащабен киберинцидент

Когато са регистрирани инциденти със среден приоритет в мрежите и информационните системи на повече от 4 от субектите по чл. 2, с висок приоритет в мрежите и информационните системи на повече от два от субектите по чл. 2 и с висок приоритет на повече от един от субектите по чл. 2 (от закона).

Инцидент със „значително увреждащо въздействие

Определя се, като се вземат предвид следните показатели:

а) брой ползватели, разчитащи на услугите, предоставяни от субекта;

б) зависимост на други сектори – от посочените в Приложение 1 от Закона, от услугата, предоставяна от субекта;

в) въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност;

г) пазарният дял на субекта;

д) географският обхват, що се отнася до областта, която би била засегната от даден инцидент;

е) значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга;

ж) когато е целесъобразно се вземат предвид и характерните за сектора показатели, за да се определи дали даден инцидент би имал значително увреждащо въздействие.

Киберзаплаха

Възможността за злонамерен опит да се повреди или прекъсне компютърната мрежа, системата, услугите и данните.

Кибератака

Опит за разрушаване, разкриване, променяне, забрана, кражба или получаване на неупълномощен достъп до/или неупълномощено използване на актив.

Киберпрестъпление

Престъпни деяния, които се определят като такива в националното законодателство и/или в международното законодателство, насочени към и/или използващи киберпространството.

Риск

Потенциалната възможност дадена заплаха да се осъществи, като се експлоатира уязвимостта на активите, за да се причини вреда.

Уязвимост

Неустойчивост на информационната система, на вътрешния контрол и на процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата.

Определени са също субектите, отговорни за противодействие при нежелани събития и дейностите за гарантиране на нормално протичане на процесите в кибер пространството.

Екип за реакция при инциденти с компютърната сигурност

Организация, която изучава уязвимостите в кибер пространството и подпомага жертви на кибер атаки, осигурява проактивни и реактивни услуги, споделя информация за повишаване на кибер сигурността и координира отговори на заплахи на кибер сигурността (известни в различни организационни форми – CSIRT, CERT и др.)

Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност

Международна група, включваща националните екипи за реагиране при инциденти с компютърната сигурност от държавите членки и екипите за реагиране при инциденти с компютърната сигурност на Европейския съюз.

Действия при инцидент

Всички процедури, подпомагащи установяването, анализа и ограничаването на инцидент, както и реагирането на такъв инцидент.

Киберотбрана

Комплекс от способности за защита и активно противодействие на кибер атаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на страната и въоръжените сили във военно положение, извънредно положение или положение на война и върху стратегическите обекти от значение за националната сигурност.

Информационната защита

Комплекс от организационни, юридически, технически и технологични мерки за мониторинг, активна превенция, намаляване влиянието на уязвимости, споделяне на информация за тях, включително отстраняване на последствията от тези заплахи.

Мрежова и информационна сигурност

Способността на мрежите и информационните системи да издържат при дадено равнище на увереност на действия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.

Устойчивост

Способност, свойство (на организацията) бързо да се адаптира и да се възстановява от известни или неизвестни промени в околната и вътрешната среда чрез цялостно и последователно осъществяване на управлението на риска, управление при извънредни ситуации и планиране на непрекъснатост на дейностите/операциите.

Национална стратегия относно сигурността на мрежите и информационните системи

Рамка, включваща стратегически цели и приоритети в областта на сигурността на мрежите и информационните системи на национално равнище.

Посочени са органите, на които са възложени (или на които предстои да бъдат възложени) със закон или друг нормативен акт от съответния ред, отговорности за предоставяне на цифрови услуги и за осъществяване на дейности по гарантиране на сигурността в кибер пространството.

Доставчик на DNS услуги

Субект, предоставящ Система за имена на домейни (DNS) услуги по интернет.

Доставчик на цифрови услуги

Юридическо лице, предоставящо цифрова услуга.

Национален компетентен орган

Орган, отговарящ за изпълнението на задачите, свързани със сигурността на мрежите и информационните системи на операторите на съществени услуги и доставчиците на цифрови услуги съгласно този закон.

Национално единно звено за контакт

Звено за контакт, което отговаря за координацията на въпросите, свързани със сигурността на мрежите и информационните системи, и за трансграничното сътрудничество на равнището на Европейския съюз.

Представител

Физическо или юридическо лице, установено в Европейския съюз, което е изрично определено да действа от името на доставчик на цифрови услуги, който не е установен в Европейския съюз, и към което националният компетентен орган или екип за реагиране при инциденти с компютърната сигурност може да се обърне вместо към доставчика на цифрови услуги във връзка със задълженията на доставчика на цифрови услуги по Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194 от 19 юли 2016 г.).

Административен орган

Понятието, определено в § 1, т. 1 от Допълнителните разпоредби на Закона за електронното управление.

Група за сътрудничество

Група, съставена от представители на държавите членки, на Европейската комисия и на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).

Длъжностно лице

Понятието, определено в чл. 93, т. 1 от Наказателния кодекс.

Лица, осъществяващи публични функции

Понятието, определено в § 1, т. 11 от Допълнителните разпоредби на Закона за електронното управление.

Оператор на съществени услуги

Публичен или частен субект от посочените в Приложение №1 от закона категории, който отговаря на критериите, определени в чл. 2, ал. 2 на закона за кибер сигурност.

Организация, предоставяща обществени услуги

Понятието, определено в § 1, т. 14 от Допълнителните разпоредби на Закона за електронното управление.

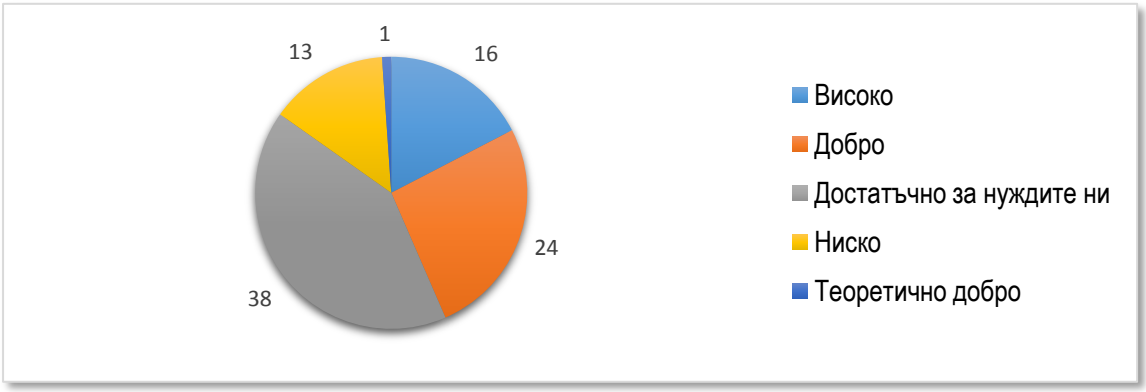
ПРИЛОЖЕНИЕ 3:
РЕЗУЛТАТИ ОТ ОНЛАЙН ИЗСЛЕДВАНЕ С ЕКСПЕРТИ ПО КИБЕР СИГУРНОСТ

ГРУПА 1: Състояние и развитие на човешкия ресурс

Моля, посочете каква е Вашата позиция в организацията

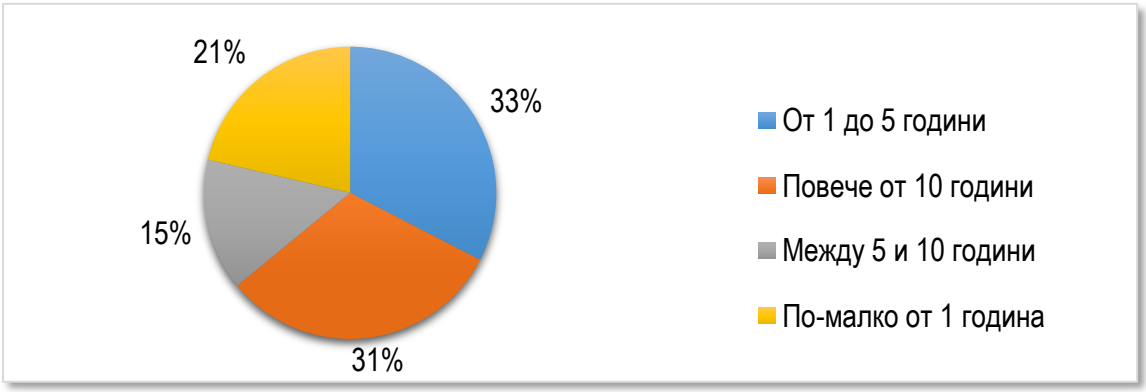
Анкетираните участници заемат ръководни, експертни и изследователски длъжности.

Моля, посочете Вашето ниво на експертиза в областта на кибер сигурността



41% от анкетираните смятат, че нивото им на експертиза в областта на кибер сигурността отговаря на нуждите на организацията, в която работят. 18% смятат, че нивото им е високо и 26% смятат, че нивото им е добро.

Моля, посочете продължителността на Вашия опит като експерт в областта на кибер сигурността.



Най-често опитът на анкетираните в областта на кибер сигурността е или между 1 и 5 години (33%) или над 10 години (31%).

Обобщение на коментарите

✓ Желание за ясно дефиниране на структурата на проблема, върху който се работи. Да се проследява ефективността от действията на всеки един екип.

✓ По-строга регулация и задължения за спазване на Нормативната база. Повече информиране на ръководителите на администрациите, не само звената и отделите.

✓ Съгласуваност между ДАЕУ, министерства и всички ведомства за изграждане на Единен модел за кибер сигурност на публичните организации, което ще е условие и за успешен модел за електронното управление.

✓ Необходимост от пътна карта за изпълнение на стратегията и яснота как ще се прилага закона в пълния му обем.

✓ Необходимост от разработване на ведомствена рамка, която да вмени отговорности.

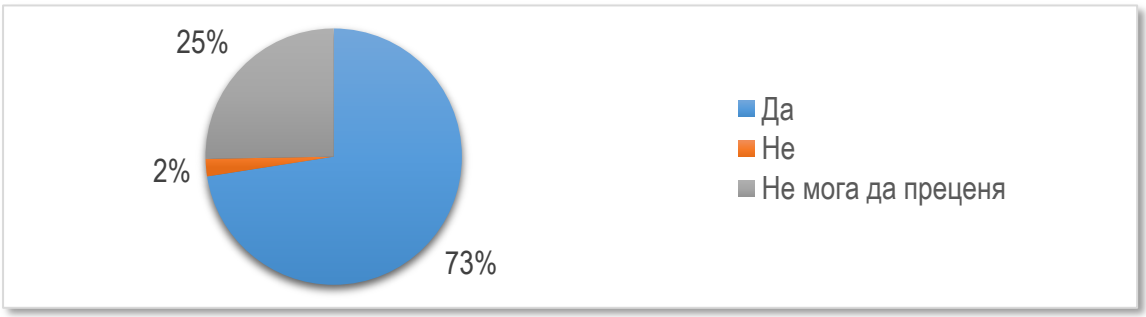
✓ Адекватно финансовото заплащане на служителите, които се занимават с киберсигурност.

✓ Засилване обучението и осведомеността на всички потребители без значение от заеманият пост в държавната администрация.

✓ Подобряване на електронните услуги.

✓ Подобряване на комуникацията между ведомствата, визирайки електронния достъп до информация, както за публична такава, така и за класифицирана.

Смятате ли, че са необходими промяна и развитие в набирането, обучението, подготовката на кадрите, задържането им и извличането на поуки от практиката в областта на кибер сигурността в България?

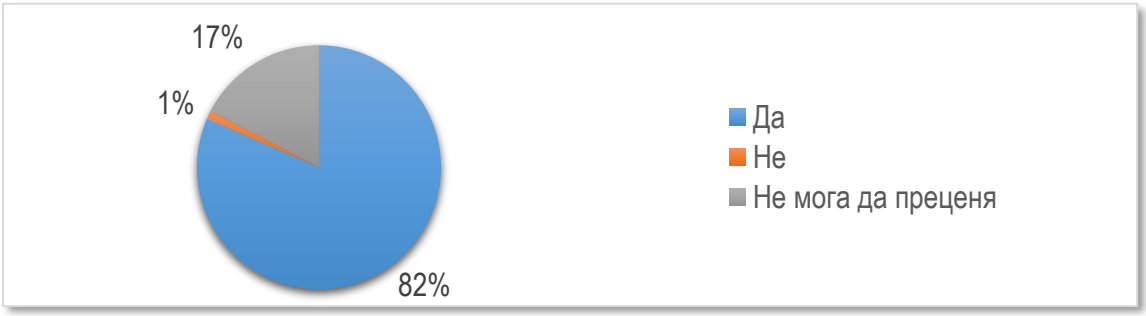


В огромното си мнозинство експертите смятат, че са необходими промени в набирането, обучението, подготовката на кадрите, задържането им и извличането на поуки от практиката в областта на кибер сигурността. Конкретните предложения: „Трябва да завършват сертификации за това, а и да има такава специалност в техническите висши учебни заведения“; „Кадрите трябва да се набират според конкретната задача, а не да бъдат "швейцарски ножчета"“; „Модно е да се преподава киберсигурност от хора, които никога не са работили в тази област. Няма ясно дефинирани способности, които се изграждат. Обучението е неосигурено с технологии и платформи. Лекциите, които се заимстват от западни и източни източници, не са осигурени с възможност за практическа работа и проверка. Инвестициите меко казано не постигат своята цел, което говори за неправилното им насочване“; „Създаване на специализирани звена за обучение и "на място"“; „Фокус върху обучението и задържането на кадрите“.

Освен това, в поредица от въпроси експертите бяха помолени да посочат дали са необходими промени в нормативната база, стратегиите, концепциите, доктрините и организацията на системата за киберсигурност. В повечето случаи малко над половината от изследваните лица посочват, че такива промени са необходими. Освен това, те дават конкретни предложения какво да се промени. Ето някои примери: „Процедури за взаимодействие между организации“; „Ясни правила за публично-частно партньорство“; „Доктринални въпроси за взаимодействие в рамките на НАТО и ЕС“; „Процедури за действие при различни сценарии. Процедура за преглед и актуализация на стратегията“; „Трябва да има ясно определени лица, екипи и отговорности. Да им се поставят цели. При непостигане на целите – да има промени в екипите. По този начин за сравнително кратък

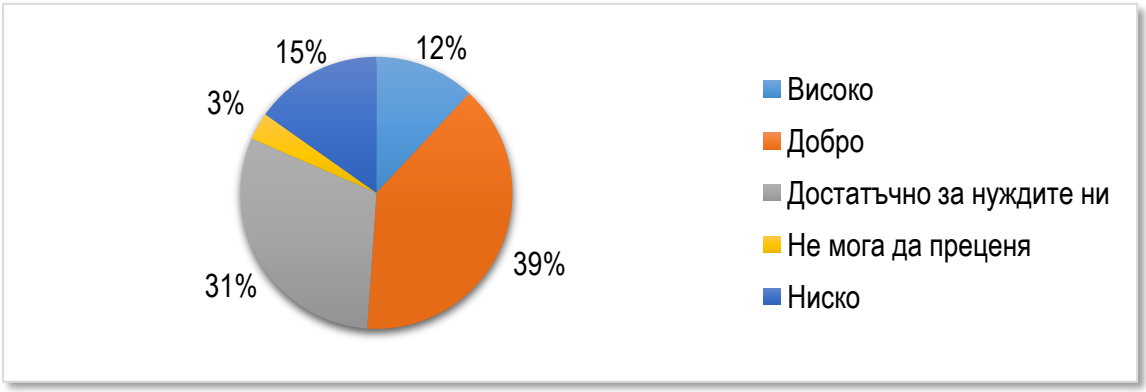
период ще формират работещи екипи и държавната администрация ще се освободи от неработещи структури и псевдо експерти“.

Смятате ли, че е необходимо да се отдели специално внимание на ролята на човешкия фактор в областта на кибер сигурността в България?



Отново огромното мнозинство от експертите подчертават ключовата роля на човешкия фактор в киберсигурността. Показателно е, че само 1 човек не счита, че човешкият фактор е ключов. Препоръки: „Дългосрочна стратегия за осигуряване на необходимия човешки потенциал“; „Подбор, обучение, сертификация, ротация между публична администрация, индустрия, академичен сектор, НАТО и ЕС, проверка за лоялност“; „Важно е да се оценяват поведението, нагласите и настроенията на потребителите в киберпространството с цел предвиждане на техните действия и очаквания“; „Технологиите за киберсигурност са с много къс жизнен цикъл. Могат да се придобиват сравнително бързо и лесно. Трудното е да се изгради и развива човешкият потенциал. Трябва да се определят какви специалисти са ни нужни да се гарантира "здравословния" излишък от специалисти във всяка една определена област на киберсигурността“; „Човешкият фактор е най-рисков; той е част от системата; основна уязвимост дори и при най-защитените системи“; „Като най-слабо звено във всяка организация изисква специално внимание най-вече по отношение на обучение с цел повишаване на компетенциите на служителите и спазване на добри практики в областта на киберсигурността“.

Как определяте нивото на експертност на персонала, който отговаря за сигурността във Вашата организация?



Нивото на експертиза на персонала, който отговаря за сигурността в организацията, в повечето случаи се определя като достатъчно добро и добро (70%), а в 15% от случаите се определя като ниско.

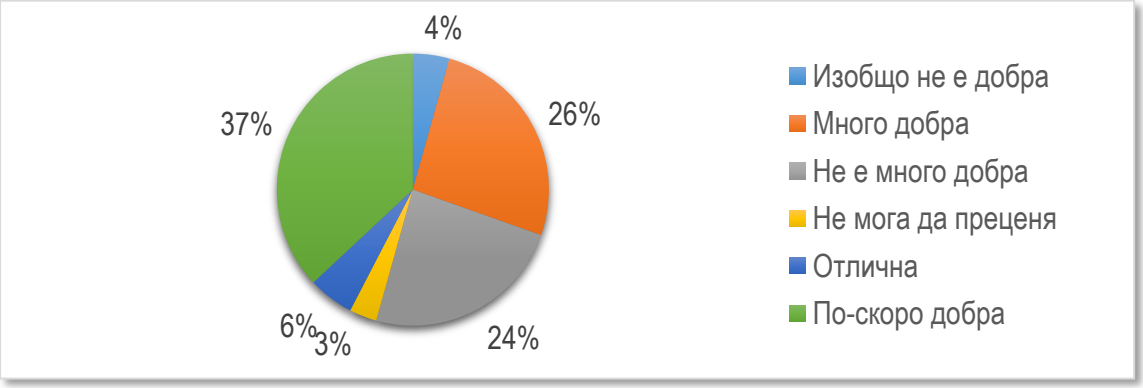
Кога за последно е проведено обучение по кибер сигурност във вашата организация?

Проучването показва, че в голяма част от случаите (55%) такива обучения не са правени. Под **Друг отговор** (14%) се включва:

- ✓ Преди 3 години
- ✓ През последната година
- ✓ През последните 6 месеца
- ✓ Провежда се в момента.
- ✓ Такива обучения са провеждани само на администраторите на информационни системи.

ГРУПА 2: Текущо състояние на оборудването и ресурсите

Моля, посочете как оценявате защитата/сигурността на системите на Вашата организация



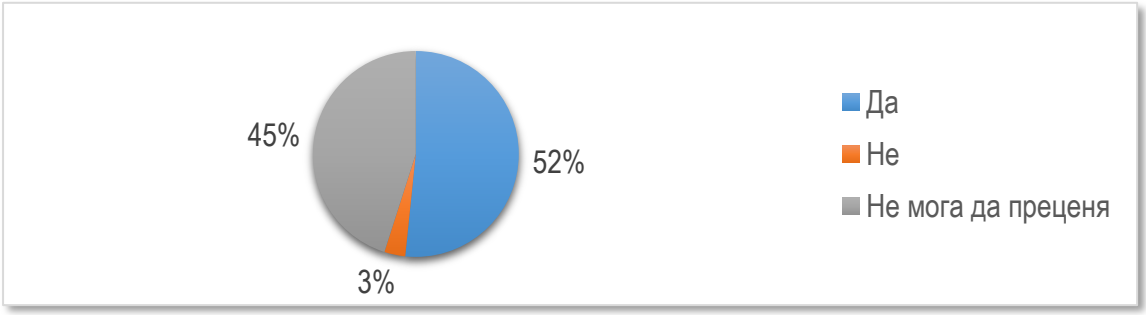
Данните показват твърде голямо разнообразие в отговорите. Повече от половината експерти дават оценки „По-скоро добра“ – 37%, „Много добра“ – 26%. Около една четвърт смятат, че защитата/сигурността на системите на тяхната организация е „Не много добра“. Единични експерти дават оценки като „Отлична“ и „Изобщо не е добра“.

Моля, посочете и обосновете трите най-важни проблема в момента в областта на кибер сигурността в България

Респондентите са имали възможност да посочат повече от един верен отговор. Като най-сериозни проблеми на киберсигурността експертите определят недостатъчния капацитет (знания и умения) на ИТ

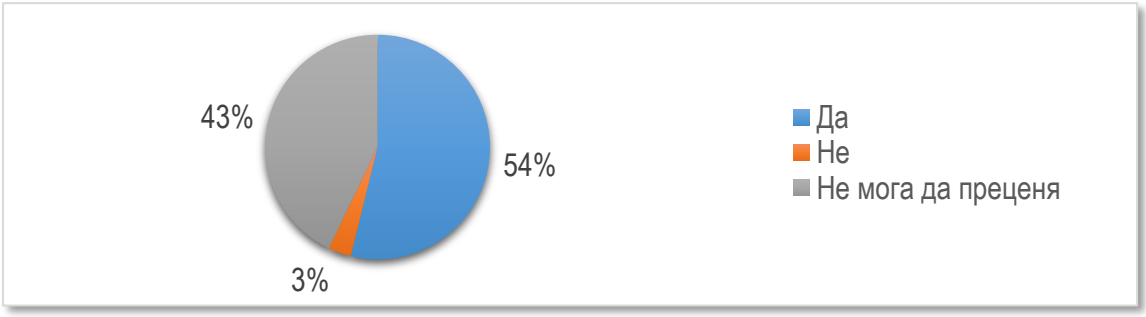
персонала. На следващо място с почти еднакъв дял са посочени качеството на информационните системи в администрацията и недостатъчните средства, които се отделят за киберсигурност. На трето място са посочени известни пропуски в нормативната база и практиката на прекалено аутсорсване на ИТ услуги, в някои случаи водещо до лошо качество. Единични експерти смятат, че липсва разбиране сред ръководния състав, че проблемът се омаловажава или че се работи на парче.

Смятате ли, че са необходими промени в технологичното осигуряване на звената в областта на кибер сигурността в България?



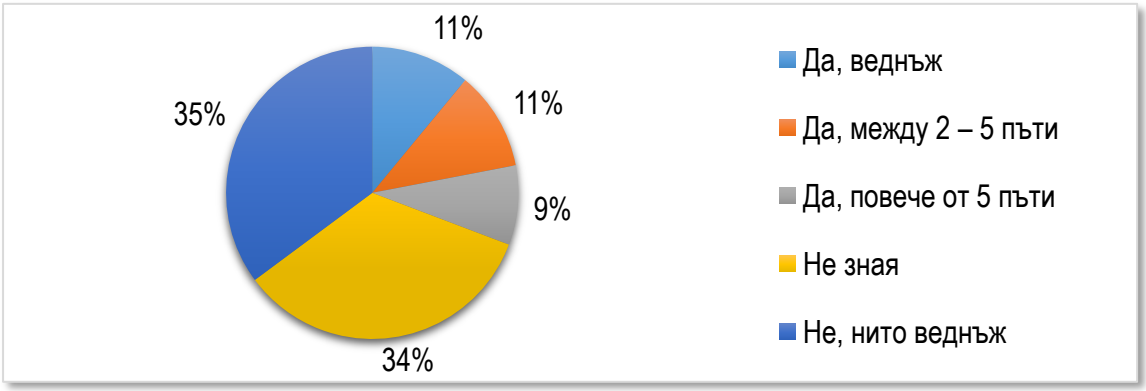
Повече от половината експерти отговарят положително на въпроса (52%). Прави впечатление големият дял отговори „не мога да преценя“. Очевидно голяма част от изследваните експерти не са компетентни в областта на технологичното осигуряване на звената в областта на кибер сигурността.

Смятате ли, че са необходими промени в ресурсното осигуряване на звената в областта на кибер сигурността в България?



Повече от половината експерти (54%) отговарят положително на въпроса. И тук прави впечатление големият дял отговори „не мога да преценя“, вероятно по същата причина.

Вашата организация била ли е подложена на атака от тип разпределен отказ от услуга (DDoS) през последната година?

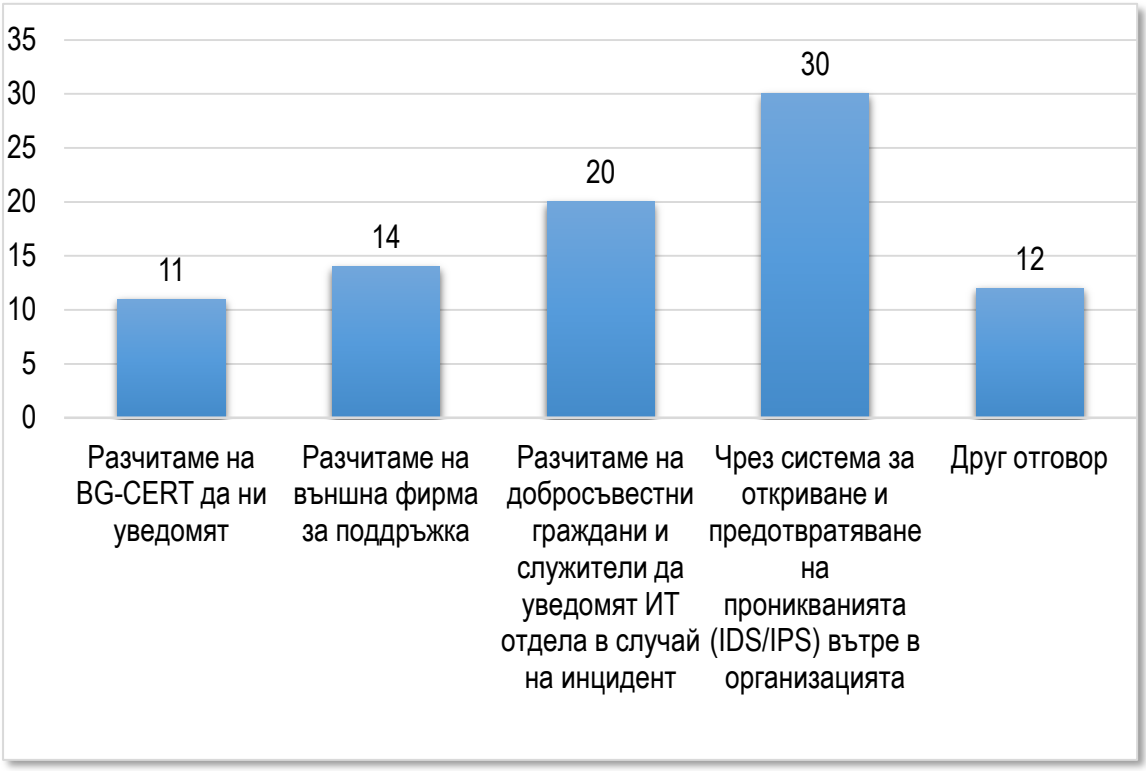


Процентът на атакуваните за последната година с DDoS атака организации е 31%. В 34% те не са атакувани, а за останалите 35% от случаите тази информация не е известна за анкетирания служител.

Годишният бюджет за 2018 г., предназначен за поддържане на сигурна и защитена информационна и комуникационна инфраструктура, е:

В 49% от случаите бюджетът за текущата година, предназначен за поддържане на сигурна и защитена информационна и комуникационна инфраструктура е същият като предходната година. В 10% от случаите такъв бюджет изобщо не се предвижда дори и за поддръжка на съществуващите системи.

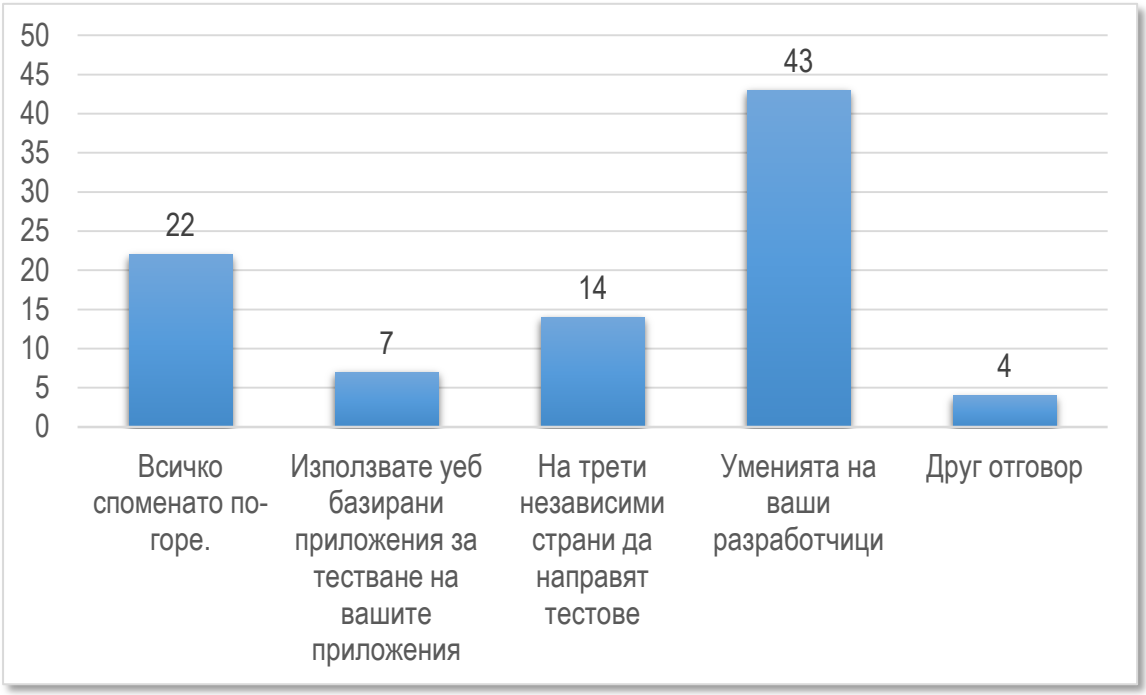
Как получавате уведомления за пробив в сигурността на вашите системи?



Респондентите са имали възможност да посочат повече от един верен отговор. В повечето случаи се поддържа система за откриване и предотвратяване на проникванията вътре в организацията. Под **Друг отговор** се включва:

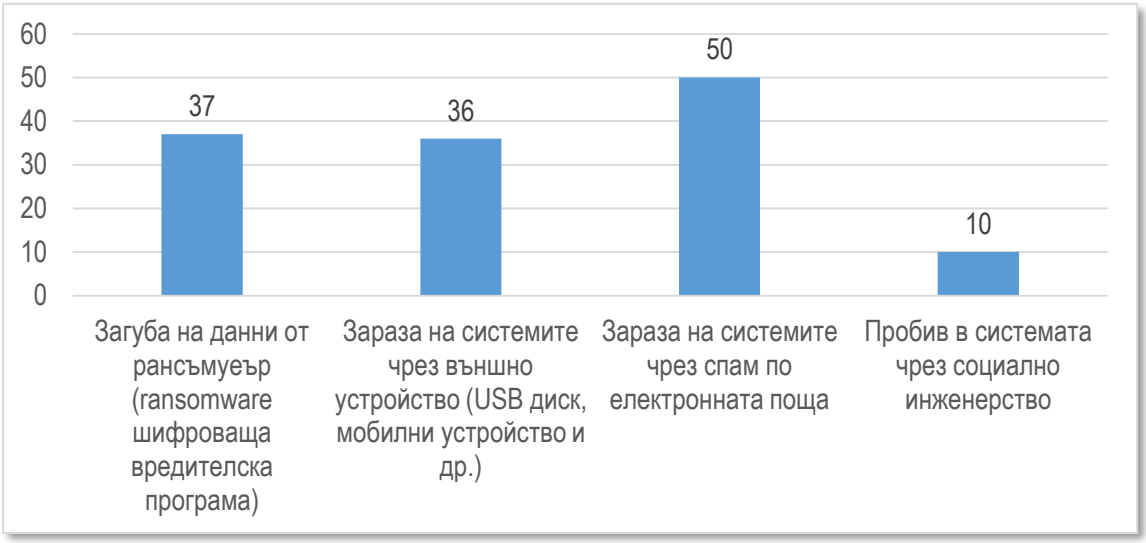
- ✓ на базата на личните умения и опит персонала, който отговаря за поддръжката;
- ✓ наблюдаване на трафика;
- ✓ ежедневно наблюдение на системите.

За качеството на предлаганите от вас уеб ресурси и уеб приложения разчитате на:



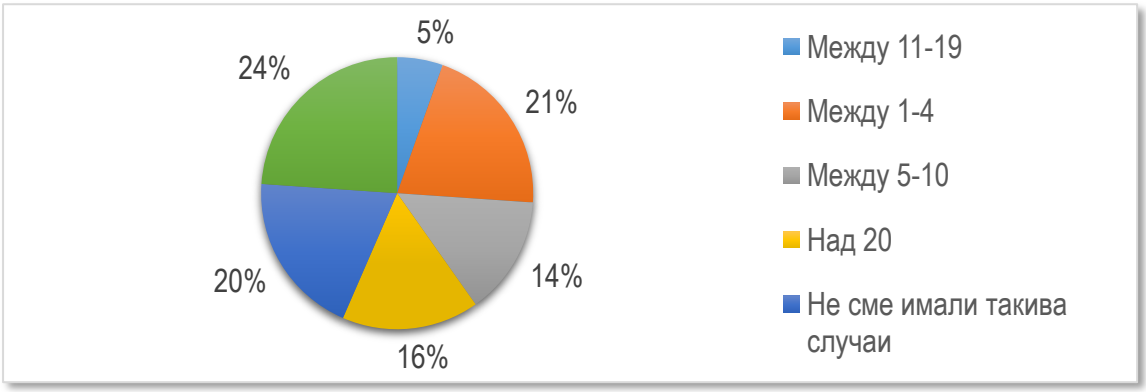
Този въпрос позволява повече от един отговор. В повечето случаи се разчита на уменията на собствени разработчици. В немалко случаи се използва комбинирания подход, където се използват както вътрешни, така и външни независими източници.

Сблъсквала си се е Вашата организация с някой от следните проблеми?



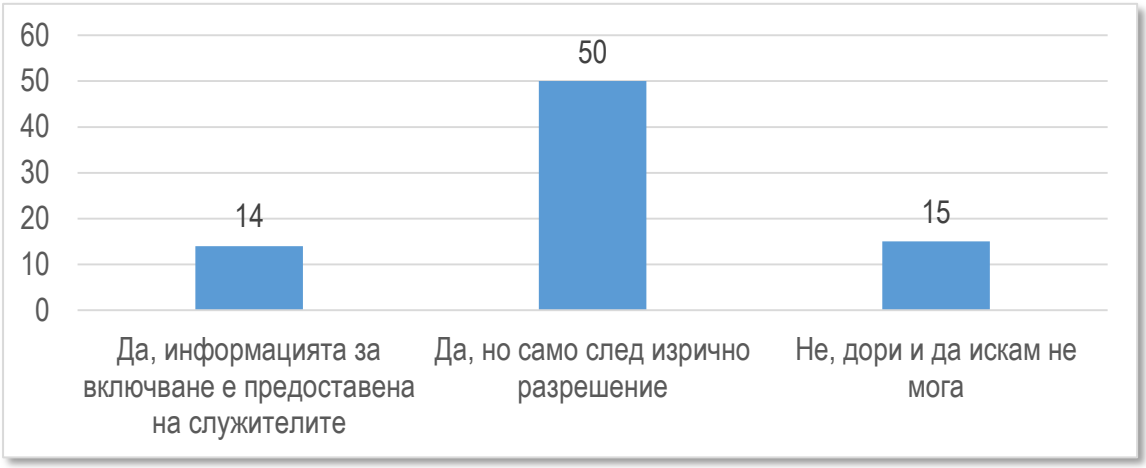
На този въпрос може да се даде повече от един отговор. Най-често срещаните проблеми по отношение на успешни атаки са зараза чрез спам и рансъмуеър.

С колко кибер заплахи сте се сблъскали за последната година?



Най-често потребителите са се сблъсквали с кибер атака от 1 до 10 пъти за последната година (35%). На второ място (над 20%) са се сблъсквали повече от 10 пъти. Само 20% заявяват, че не са имали такива случаи, а 24% от тях не са информирани.

Имате ли възможност да свързвате външни за организацията устройства към Вашата мрежа?



Възможността да се свързват външни устройства към мрежата на организацията, но само след изрично разрешение е посочена от половината анкетирани.

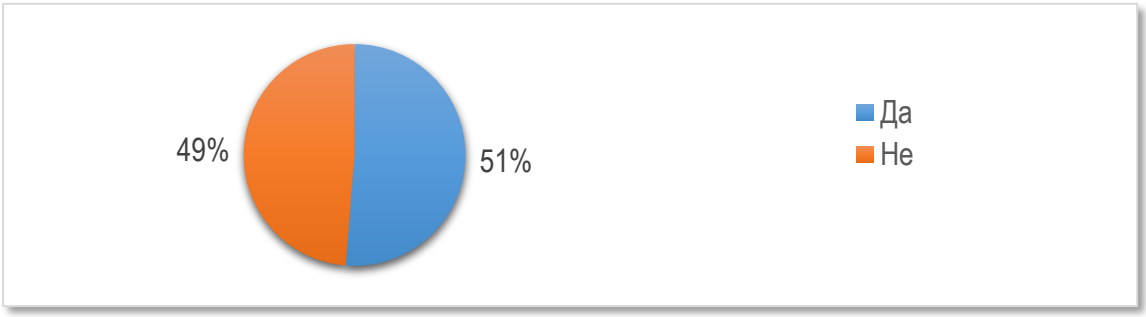
Използвате ли криптография за защита на данните?

Над 2/3 от анкетираните използват криптография за защита на данни в определени случаи. Трябва да се отбележи, обаче, че 9% твърдо използват криптографията за данни, които не се ползват. 16% не използват криптография, тъй като намират процедурата за сложна, а 8% от анкетираните не намират смисъл от ползването на криптография.

Кой реагира в случаи на кибер атака?

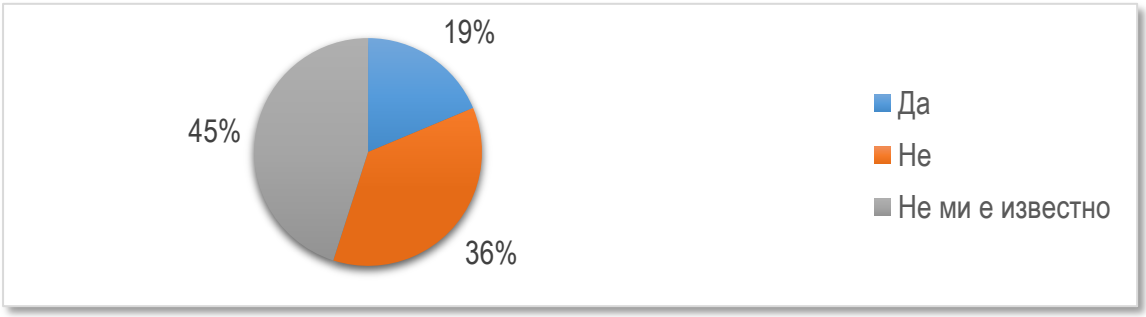
Близо 2/3 от анкетираните имат собствена структура за реакция от кибер атаки. Не малък е броят (25%) на организациите, които ползват услугите на външна частна фирма. Те са почти два пъти повече от тези, които разчитат на външни държавни организации, специализирали се в тази област.

Имате ли разработени планове/процедури за реагиране в случай на кибер заплаха?



Респондентите са раздвоени. От резултатите се вижда, че не се очертава ясна тенденция по отношение на разработването на планове и/или процедури за реагиране в случай на кибер заплаха. Почти половината нямат разработени такива процедури и планове.

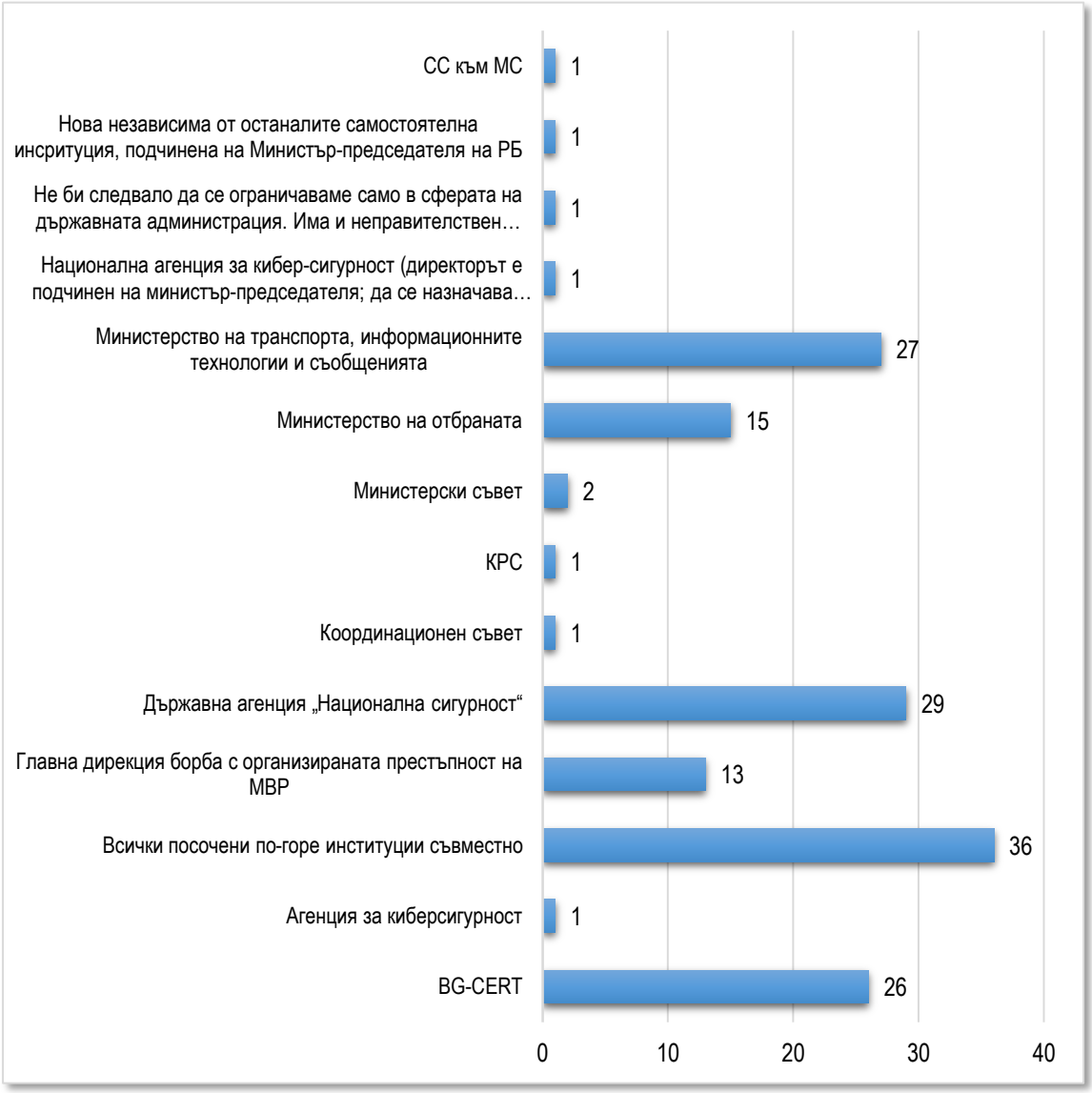
Налага ли се изтриване на информация от бази данни, които следва да бъдат достъпни и за трети страни?



Над 1/3 не извършват такава дейност. Около 1/5 посочват, че я извършват. Високият процент (45%) „Не ми е известно“ говори за това, че вероятно не извършват изтриване на информация или нямат такава, която да е достъпна и за трети страни.

ГРУПА 3: Управление и политики

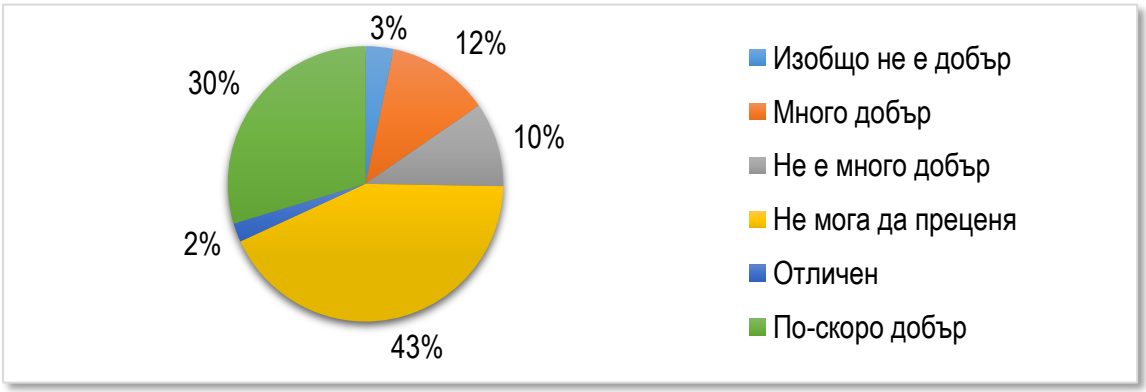
Коя институция/и в държавата следва да има водеща роля по въпросите на кибер сигурността според Вас?



Респондентите са имали възможност да посочат повече от един верен отговор. Мнението им е категорично, че всички държавни институции следва да работят заедно и в синхрон, за да се гарантира кибер сигурността. Необходим е интегриран подход за работа, като се отчита ролята на индустрията, науката и управлението. На следващо място, с почти еднакъв дял отговори, са посочени BG-CERT, ДАНС и Министерство

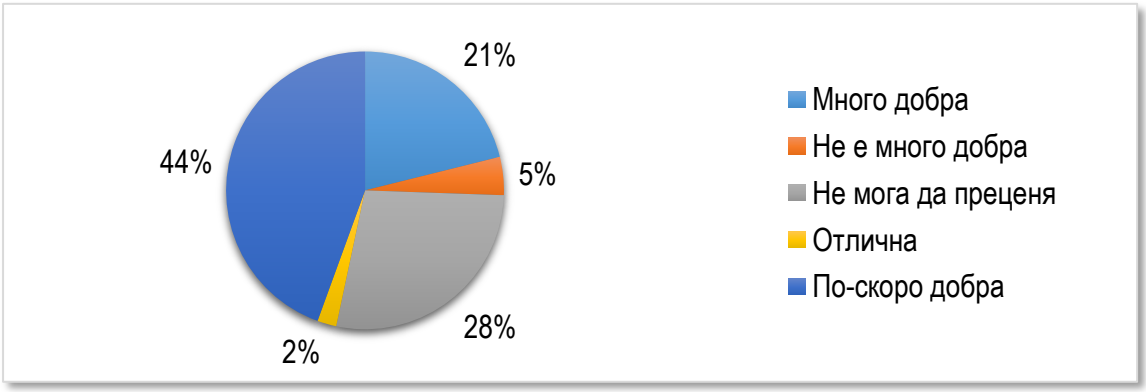
на транспорта, информационните технологии и съобщенията. Сравнително висок дял от експертите посочват и МО като институция, която трябва да има водеща роля в кибер отбраната. Данните показват, че експертите не смятат за необходимо да се създават нови държавни структури, които да отговарят за кибер сигурността. Вместо това те препоръчат да се подобри взаимодействието и сътрудничеството между съществуващите.

Моля, посочете как оценявате проекта за Закон за кибер сигурност, който е пред второ четене в Парламента?



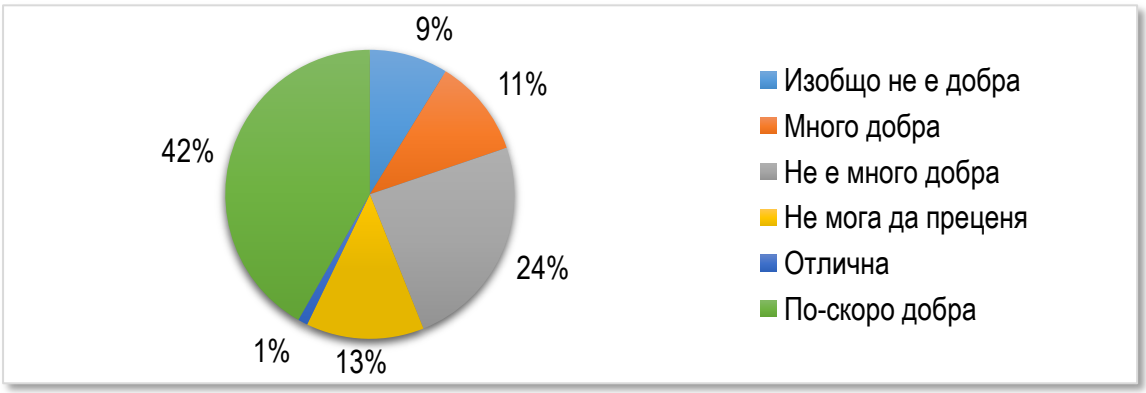
Изследването е проведено преди приемането на Закона за киберсигурност. Данните показват твърде голямо разнообразие в оценките. Близо една трета го оценяват като „По-скоро добър“ – 30%. Още 12% определят Закона като „Много добър“, а 10% като „Не много добър“. Единични експерти дават оценки като „Отличен“ и „Изобщо не е добър“. Прави впечатление сравнително големия дял отговори „Не мога да преценя“ – 43%. Очевидно част от изследваните експерти не са се запознали с проекта на Закон за кибер сигурност.

Моля, посочете как оценявате директивата на ЕС за мрежова и информационна сигурност



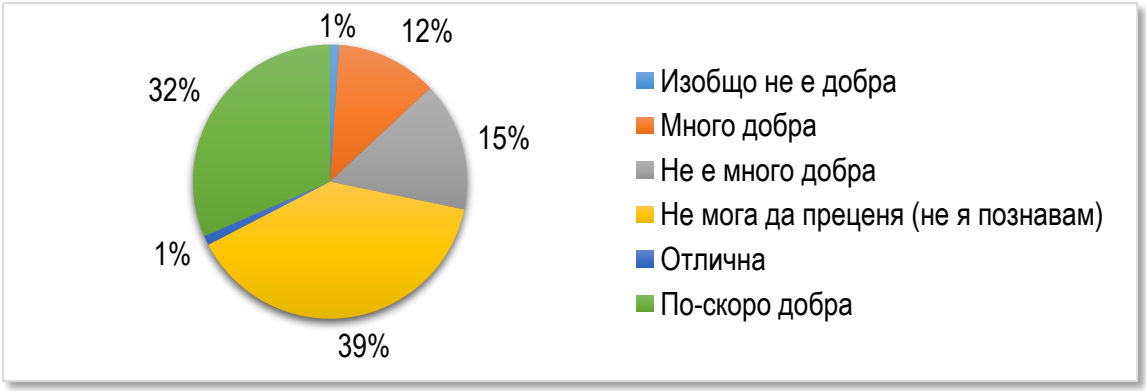
Повече от половината експерти дават оценки „По-скоро добра“ – 44%, „Много добра“ – 21%. Единични експерти дават оценки „Отлична“ или „Изобщо не е добра“. Повече от една четвърт (28%) нямат мнение по въпроса.

Моля, посочете как оценявате регламента GDPR и приложението му в България



Данните показват, че няма единно мнение по въпроса и известна липса на информация. Повече от половината експерти дават оценки „По-скоро добър“ – 42%, „Много добър“ – 11%. Единични експерти дават оценка „Отличен“. Около една трета смятат, че регламентът „Изобщо не е добър“ (9%) и „Не е много добър“ (24%). Над една десета (13%) нямат мнение по въпроса.

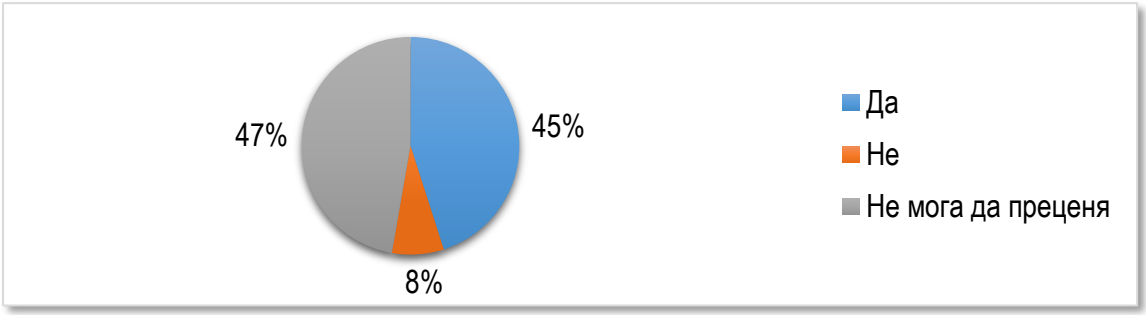
Моля, посочете и обосновете Вашата оценка за действащата Стратегия за киберсигурност „Киберустойчива България 2020“



Данните, представени на тази графика будят тревога, защото твърде голям дял от участниците в изследването, които са експерти в киберсигурността (39%), посочват, че не познават Стратегията за киберсигурност „Киберустойчива България 2020“.

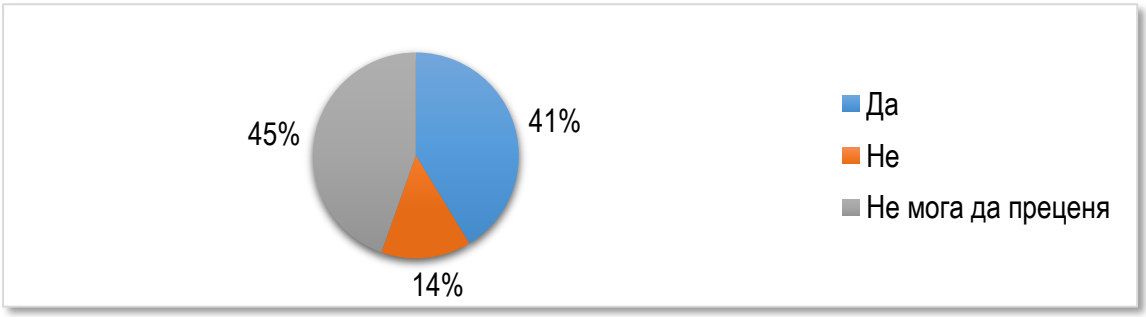
Под половината експерти дават оценки „По-скоро добра“ (32%) и „Много добра“ (12%). Единични експерти дават оценки „Отлична“ или „Изобщо не е добра“. Заслужава внимание и фактът, че близо 15% оценяват Стратегията като „Не много добра“. Очевидно са необходими действия за запознаване на експертната общност със Стратегията за киберсигурност „Киберустойчива България 2020“ и евентуална нейна актуализация.

Смятате ли, че са необходими промени и развитие в концепции, стратегии, доктрини и процедури в областта на кибер сигурността в България?



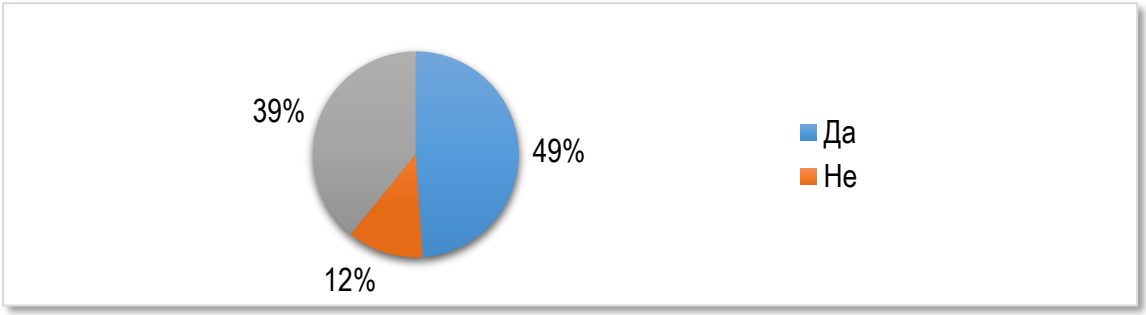
Данните показват, че няма единно мнение по въпроса и сериозна липса на информация. Близо половината експерти отговарят положително на въпроса (45%), а на обратното мнение са само 8%. Голям е делът отговори „не мога да преценя“ (47%). Очевидно част от изследваните експерти не са компетентни в областта на развитие на концепции, стратегии, доктрини и процедури в кибер сигурността.

Смятате ли, че са необходими промени в нормативната база в областта на кибер сигурността в България?



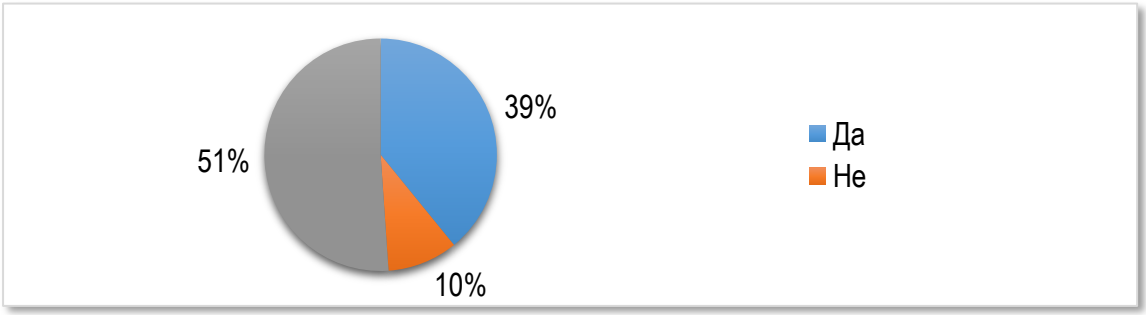
Данните отново показват, че няма единно мнение по въпроса и сериозна липса на информация. Значителна част експерти отговарят положително на въпроса – 41%. На обратното мнение са 14%. Отново почти половината (45%) нямат мнение по въпроса, вероятно по същата причина.

Смятате ли, че са необходими промени в организационната структура на звената в областта на кибер сигурността в България?



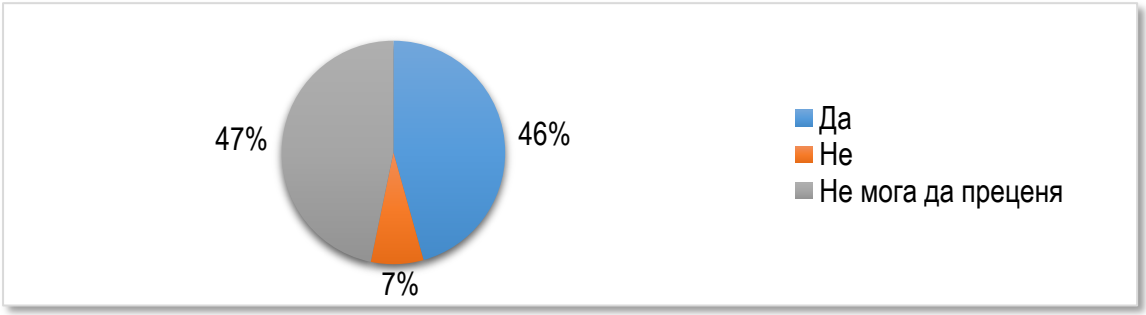
Данните отново показват, че няма единно мнение по въпроса и сериозна липса на информация. Близо половината експерти отговарят положително на въпроса – 49%. На обратното мнение са 12%. Значителна част над една трета – 39% нямат мнение по въпроса. Очевидно част от изследваните експерти не са компетентни в областта на организацията на кибер сигурността.

Смятате ли, че са необходими промяна и усъвършенстване на механизмите за прозрачност и отчетност в областта на кибер сигурността в България?



Данните отново показват, че няма единно мнение по въпроса и сериозна липса на информация. Значителна част над една трета – 39% от експертите отговарят положително на въпроса. На обратното мнение са 10%. Повече от половината – 51% нямат мнение по въпроса. Очевидно част от изследваните експерти не са компетентни в областта на механизмите за прозрачност и отчетност в областта на кибер сигурността.

Смятате ли, че са необходими промяна за повишаване на капацитета при стратегическо планиране и управление на промяната в областта на кибер сигурността в България?

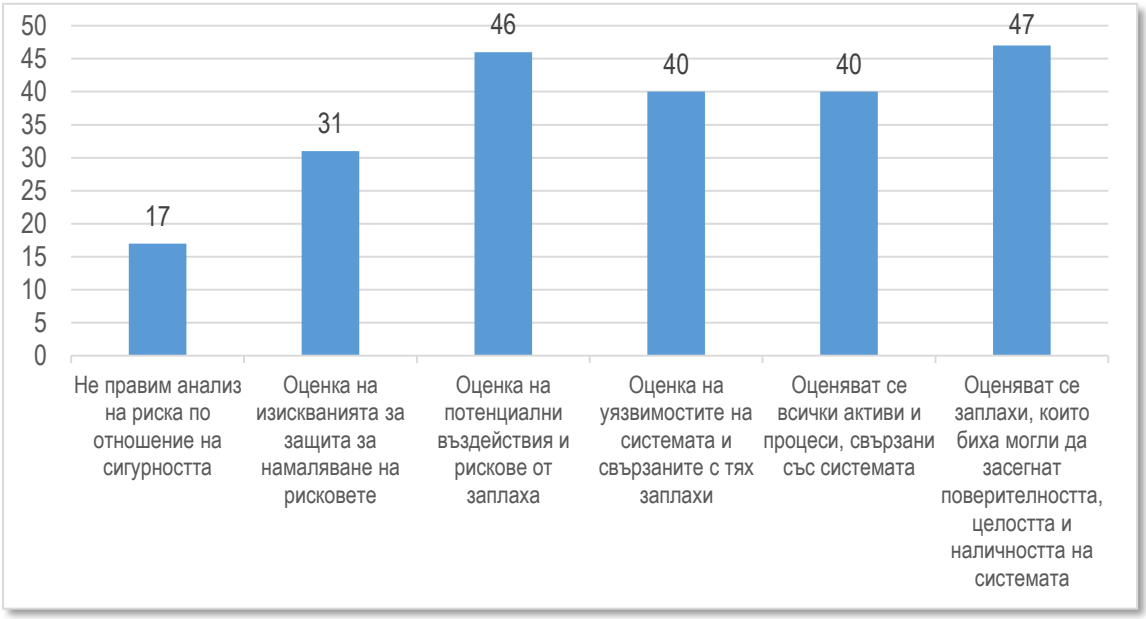


И тази графика показват, че няма единно мнение по въпроса и сериозна липса на информация. Близо половината експерти отговарят положително на въпроса – 46%. На обратното мнение са едва 7%. Близо половината – 47% нямат мнение по въпроса. Очевидно част от изследваните експерти не са компетентни в областта на стратегическо планиране и управление на промяната в областта на кибер сигурността

Има ли Вашата организация разработени и разписани системни политики за сигурност?

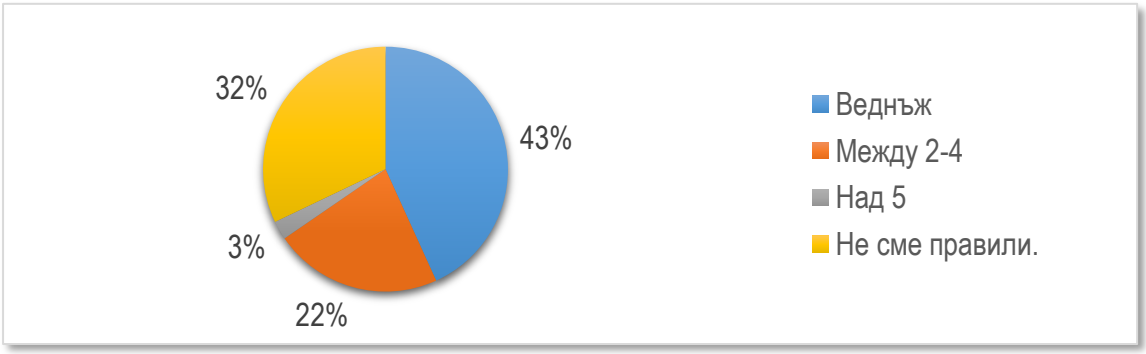
Почти половината (48%) имат разработени стандартни политики за сигурност, които се актуализират при необходимост. Почти 1/4 посочват, че редовно актуализират тези документи. 16% от анкетираните нямат такива политики. Не малък дял от анкетираните (12%) посочват, че не знаят дали има разработени такива политики в тяхната организация.

Кои от посочените елементи са включени в оценката на риска по отношение на сигурността?



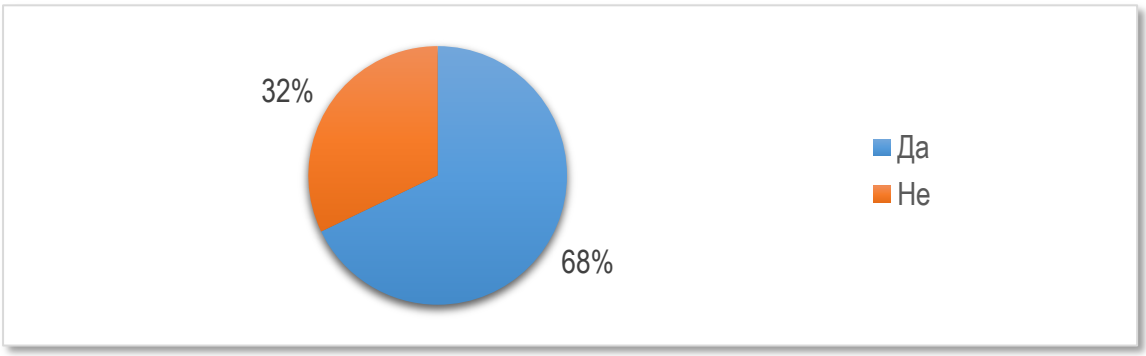
На тази въпрос може да се отговори с повече от един отговор. С почти еднакъв дял анкетираните посочват, че правят оценка на потенциални въздействия и рисковете от заплаха и оценяват заплахите, които биха могли да засегнат поверителността, целостта и наличността на системата, когато правят оценка на риска на техните системи. На второ място, с много близък дял, се посочва, че в тази оценка се включва оценката на уязвимостите и на всички активи и процеси, свързани със системата. Важното е, че 17 респондента са посочили, че не правят оценка на риска по отношение на сигурността.

Колко пъти сте правили оценка на риска за последната година?



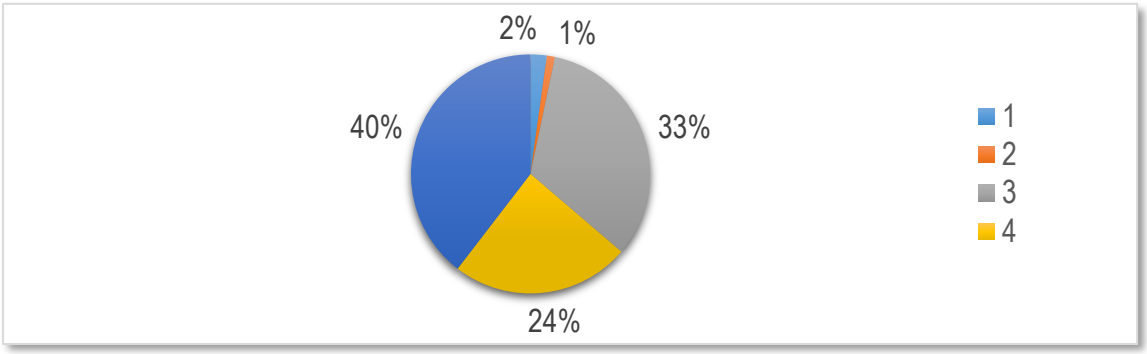
Най-често оценка на риска се прави веднъж годишно (43%). Почти 1/3 от респондентите (което е тревожен факт) заявяват, че не правят оценка на риска. В останалите случаи респондентите заявяват, че такава оценка се прави повече от 2 пъти в годината.

Според Вас трябва ли всички електронни услуги във Вашата организация да бъдат управлявани централизирано?



Повече от 2/3 посочват, че електронните услуги, които предлагат, трябва да са управлявани централизирано.

Според Вас колко е важно централизираното управление на електронни услуги?



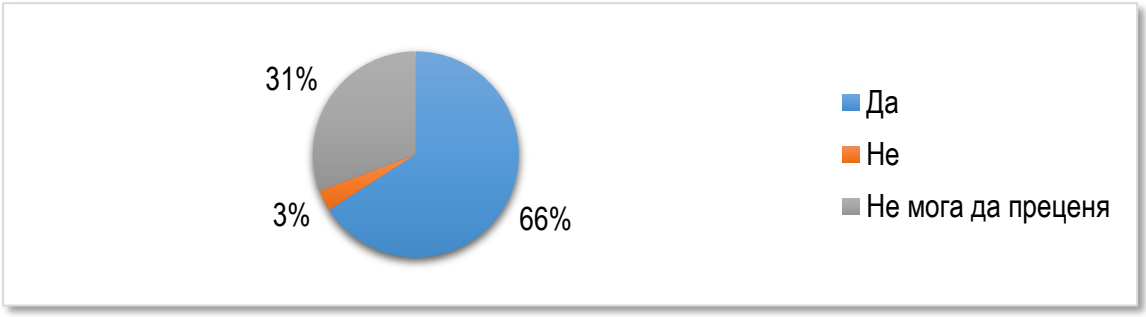
На този въпрос респондентите дават оценка от 1 (най-ниска) до 5 (най-висока) за степента на важност да има централизирано управление на електронни услуги в организацията, която представляват. 64% от тях дават висока степен на важност (оценка 4 и 5) на този въпрос. Само 3% от респондентите смятат, че централизираното управление на електронни услуги е с ниска степен на важност (оценка 1 и 2). Немалък е процентът (33%) на респондентите, които дават средна оценка на важност на този въпрос (степен 3).

ГРУПА 4: Взаимодействие между трите основни сектора: държава, академия и индустрия.

Моля, посочете и обосновете кои са според Вас трите най-важни области, които изискват научни изследвания в областта на кибер сигурността

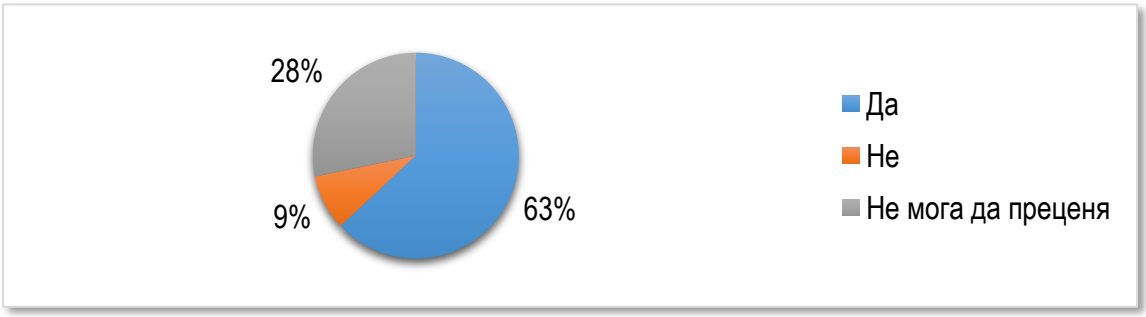
Респондентите са имали възможност да посочат повече от един верен отговор. С най-голям дял отговори, като област, в която има потребност от допълнителни изследвания, е посочена ролята на човешкия фактор в киберсигурността. Определено експертите смятат, че е необходим интегриран подход към кибер сигурността, който да включва човека в центъра на системата, новите технологии, софтуерни иновации, организационни и нормативни промени и др. Наред с това, като важни изследователски области се определят защитата от вируси и зловреден софтуер, ефективното и ефикасно управление на информационните ресурс и изграждането на облачни инфраструктури. Третата група области, които се нуждаят от допълнителни научни изследвания, са изкуственият интелект, проектирането на системи и системите за персонална идентификация. Сравнително по-нисък е интересът към блокчейн технологиите, вероятно поради тяхната по-слаба популярност.

Смятате ли, че са необходими промяна и усъвършенстване на взаимодействието между институциите в областта на кибер сигурността в България?



Усъвършенстването на взаимодействието между институциите в областта на кибер сигурността е един от най-сериозните проблеми. Близо две трети посочват този проблем. Две трети от експертите отговарят положително на въпроса. На обратното мнение са едва 3%. Близо една трета нямат мнение по въпроса. Предложенията на експертите са: „Съветът по сигурността и националният център следва да осигурят истинско взаимодействие, като се добавят и академичен сектор, индустрия, съюзници“; „Обмен на информация и координиране на действията“; „Ясна рамка кой какво споделя с кого. Обичаят всеки да разбира от всичко води до размиване на отговорности, липса на ефективни способности, бавна реакция или пълна липса/неадекватност“; „Цялостна нова концепция на взаимодействие – в момента липсва каквото и да е“.

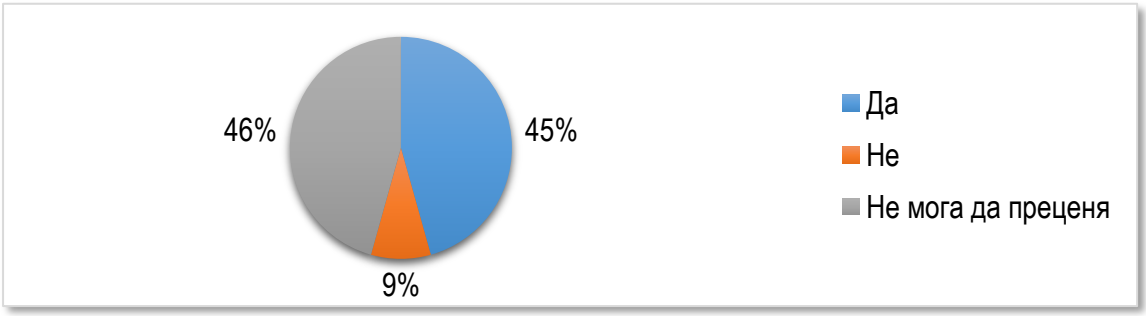
Смятате ли, че са необходими промяна и усъвършенстване на взаимодействието между институциите в областта на кибер сигурността в България и академичния сектор/индустрията?



Данните, представени на тази графика, до голяма степен повтарят тези на предходната. Близо две трети (63%) посочват необходимост от

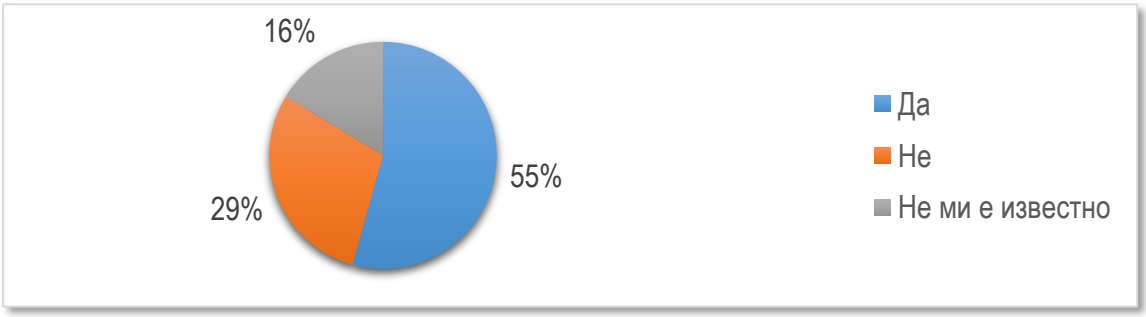
усъвършенстване на взаимодействието. На обратното мнение са 9%. Близо една трета (28%) нямат мнение по въпроса.

Смятате ли, че са необходими промяна и усъвършенстване на взаимодействието между звената в областта на кибер сигурността в България с тези в НАТО и ЕС?



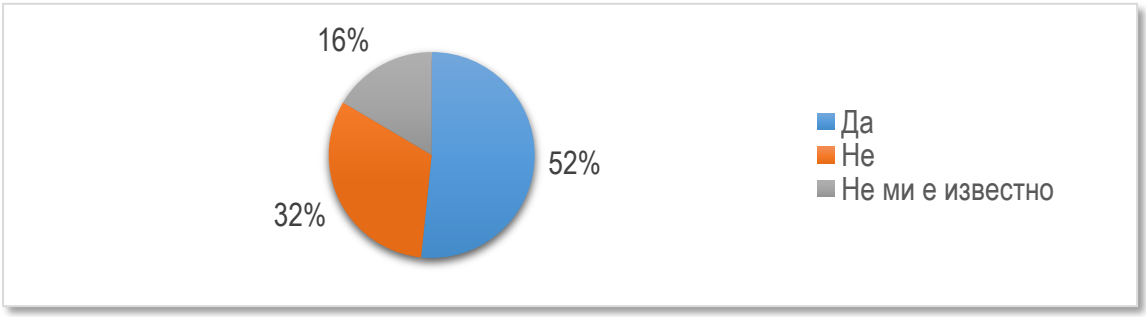
Данните на графиката показват, че няма единно мнение по въпроса и сериозна липса на информация. Близо половината експерти отговарят положително на въпроса – 45%. На обратното мнение са едва 9%. Близо половината – 46% нямат мнение по въпроса.

Налага ли Ви се във Вашата работа да използвате съвместно с друго ведомство/организация една и съща информация?



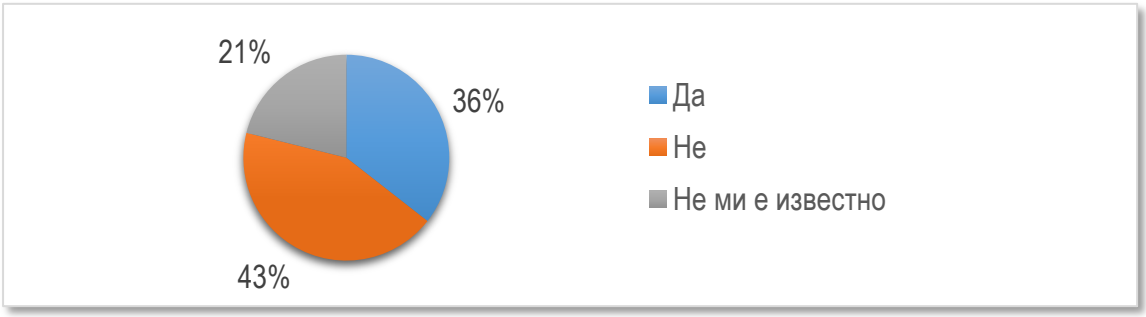
В 55% от случаите се налага използването на една и съща информация с друго ведомство/организация, а в 29% това не се налага.

Оперирате ли с информация, която следва да бъде публично достъпна за одит от други ведомства/организации?



В 52% организациите оперират с информация, която следва да бъде публично достъпна за одит от други ведомства и/или организации, а 32% не оперират с такава информация.

Оперирате ли с информация, която следва да бъде публично достъпна за одит от граждани?

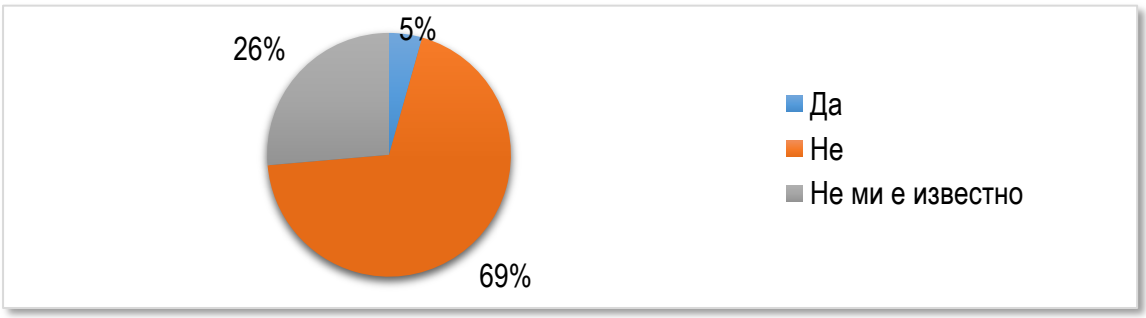


В 43% организациите не оперират с информация, която следва да бъде публично достъпна за одит от гражданите, а 36% оперират с такава информация.

Информацията, която предоставяте на трети страни, изцяло публична ли е или е обект на контрол на достъпа?

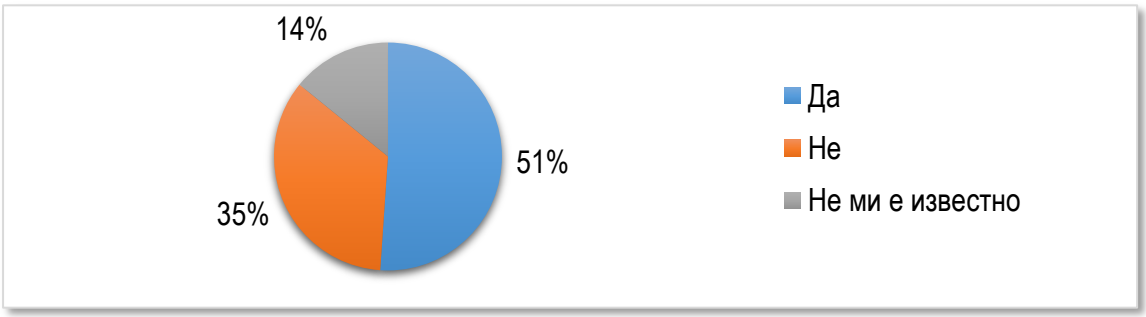
ГРУПА 5: Иновативни технологии

Използва ли се във Вашата организация блокчейн технологията?



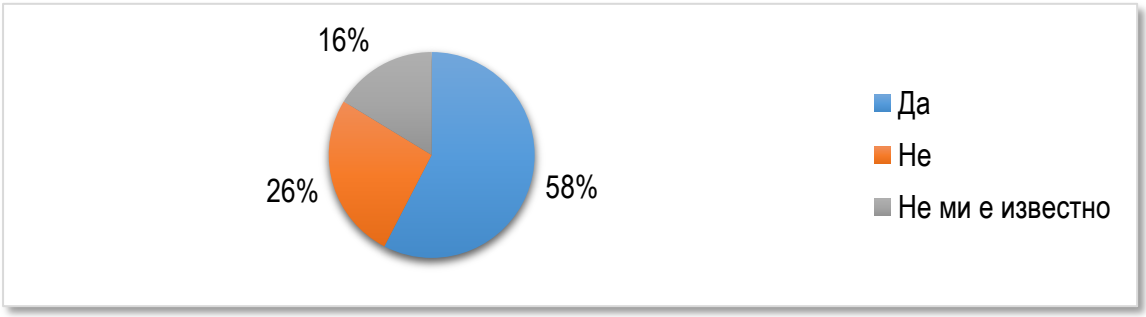
Само 5% от анкетираните заявяват, че използват блокчейн технология в тяхната организация. Останалата част или не използват, или не знаят дали тя се използва.

Използвате ли във Вашата работа разпределени бази данни или разпределени места за съхранение и обработка на информация?



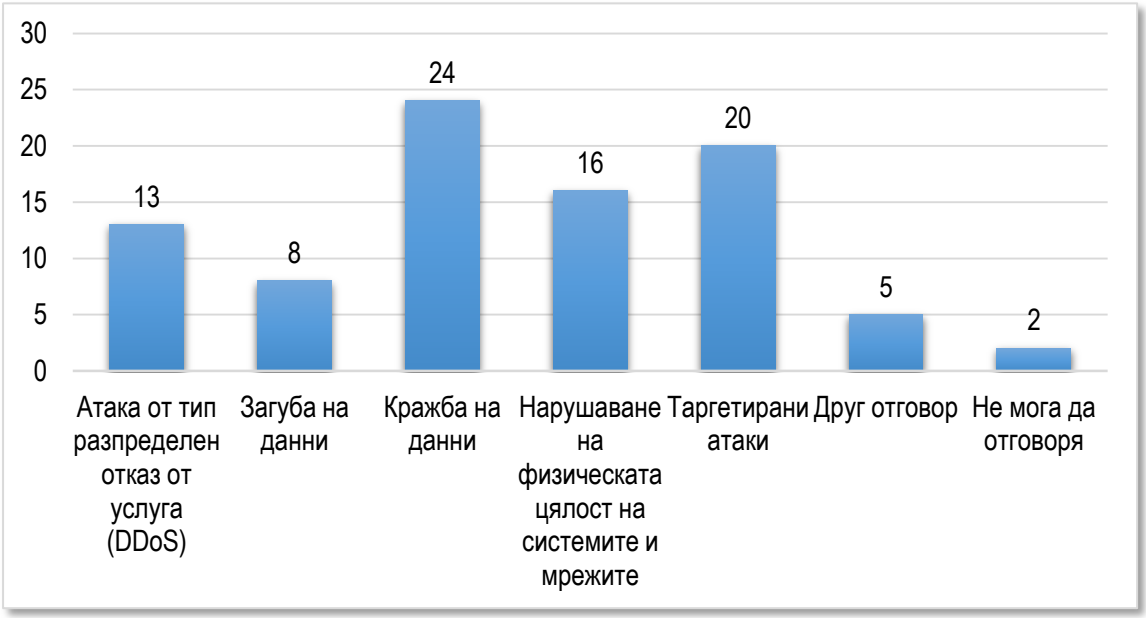
Разпределените бази данни или разпределени места за съхранение и обработка на информация се използват в повече от половината организации. В 35% от случаите не се налага използването на такъв тип бази данни.

Приложими ли са според Вас разпределени бази данни за Вашата организация?



Повече от половината анкетирани (58%) смятат, че в тяхната организация е приложимо използването на разпределени бази данни.

Най-неприятният тип атаки са:



Тук анкетираните могат да дадат повече от един отговор. Повечето от тях смятат, че най-неприятният тип атаки са кражба на данни под всякаква форма, нарушаване на физическата цялост на системите и мрежите и таргетираните атаки. Под **Друг отговор** (14%) се включва:

- ✓ шифроване на данни (рансъмуеър);
- ✓ спам атаки;
- ✓ фишинг.

До каква степен защитата на вашите системи и е-услуги отговаря на изискванията и нуждите на бизнеса, крайните потребители и другите администрации в държавната и местна власт?

Като цяло качеството на защита на организациите, които предлагат е-услуги, отговаря на изискванията и нуждите на бизнеса, крайните потребители и държавната администрация. Степен „Напълно отговаря“ е дадена в 12% от случаите, степен „Отговаря в голяма степен“ е дадено в 33% от случаите и степен „По-скоро отговаря“ е дадено в 26% от случаите.

ПРИЛОЖЕНИЕ 4:
Известни криптовалути

Биткойн

Като първата наложила се в практиката криптовалута, системата Биткойн е важна стъпка в еволюцията на блокчейн технологиите. Самата валута също се нарича биткойн (BTC), но системата поддържа транзакции с много по-малки суми от 1 биткойн – най-малката единица в системата се нарича сатоши, на името на създателя (или създателите). 1 сатоши е 0.00000001 BTC.

Биткойн използва SHA-256 като криптографски хеш алгоритъм, модел на консенсус „Доказателство за работа“, има средно време за „добив“ на блок 10 минути, адаптивна трудност, която се променя на всеки 2016 блока, стартова награда за „добив“ на блок 50 биткойна и двойно намаляване на наградата на всеки 210 000 блока, което се случва на около 4 години (Controlled Supply, n.d.). Както при повечето други криптовалути, цената на 1 биткойн варира и е силно нестабилна.

Етериум

Следващата важна стъпка по пътя на криптовалутите е платформата Етериум. За разлика от Биткойн, Етериум се фокусира върху повече от транзакции и поддържа Тюрингов език за програмиране, чрез който да бъдат имплементирани интелигентни договори. В тази секция разглеждаме само особеностите на Етериум като криптовалута, а в следващата е представен кратък обзор на Етериум като платформа за интелигентни договори.

В платформата Етериум, валутата се нарича етер (“ether”) и се обозначава с ETH, а най-малката деноминация на етер е “wei”, като 1 ETH = 10^18 wei.

Структурата на Етериум като поддържаща платформа на криптовалута е в голяма степен сходна на тази на Биткойн. Основната разлика между двете платформи е, че при Биткойн всеки блок съдържа само хеш-стойността на предходния, докато в Етериум всеки блок съдържа пълното състояние на екосистемата на Етериум преди момента на „добив“ на въпросния блок. Всеки блок съдържа даден брой транзакции, които съдържат изпълним код (който се явява и основа за интелигентните договори). При валидация на „добит“ блок, останалите участници в мрежата проверяват дали кодът на всички транзакции е валиден и може да бъде изпълнен, както и за други параметри в системата (например разход и цена

на „гориво“, обсъдено по-надолу). Тъй като във всеки блок се съдържа пълното предходно състояние на системата, за да бъде възможно ефективното съхранение на големия обем генерирани данни се използва специална структура от данни на име “Patricia tree” (вид дърво) (Buterin, н.д.). Освен това, с цел по-сигурна мрежа, при Етериум се награждава създаването на т.нар. “uncle blocks” –блокове, които са били близко до вграждане във веригата, но не са успели да станат канонични.

Другата съществена разлика между Биткойн и Етериум е, че при Етериум употребата на модела „Доказателство за работа“ е временна и отдавна се планира миграция към модел „Доказателство за залог“. Тъй като към момента тази миграция не е завършена, Етериум няма строго контролирано предлагане – до момента наградата за „добив“ е сваляна неколкократно (от 5 ETH на 3 ETH, от 3 ETH на 0.6 ETH) и предстои въвеждане на хибриден модел между „Доказателство за работа“ и „Доказателство за залог“. Предстои да станат ясни конкретният модел на контролиране на предлагането, както и наградите при „добив“ в бъдещия модел „Доказателство за залог“.

При модела „Доказателство за залог“ вместо да се решава изчислителна задача, набор от „валидатори“ избират следващия блок във веригата. За да стане даден участник в мрежата валидатор, той следва да „заложи“ част от валутата си, като я депозира на специален адрес. Съществуват различни алгоритми за избор на валидатор, който да получи правото да „добие“ следващия блок (Proof of Stake FAQs, n.d.). На избрания валидатор се полага и наградата от „добива“ на блока, ако такава е предвидена. Сред предимствата на модела „Доказателство за залог“, разработчиците на Етериум платформата изтъкват много по-ниския разход на енергия (моделът „Доказателство за работа“ на практика „разхищава“ изчислителен ресурс и енергия), възможност за по-малки награди при „добив“, както и подобрена сигурност спрямо различни видове атаки.

В текущата версия на Етериум е въведена поддръжка и за транзакции със тайни данни на базата на zk-SNARK (Wilcox, 2017), криптографски примитиви, използвани от криптовалутата Zcash (обсъждана по-долу).

Dash/Monero/Zcash

Трите криптовалути Dash, Monero и Zcash са в голяма степен сходни в своята цел, макар и да се различават сериозно в имплементацията ѝ – основната им идея е да предоставят известна анонимност на участниците и конфиденциалност на транзакциите в екосистемата, поради което тук те са групирани заедно.

Исторически, най-ранната подобна криптовалута е Dash, чиято първа версия е публикувана през януари 2014 под името Xcoin (Reuters, 2018).

Валутата предоставя няколко промени спрямо Биткойн, като например възможността за „бързи“ транзакции, както и далеч по-сложна архитектура, при която има „свръх“-възли (“masternodes”), които притежават далеч по-сериозни привилегии и отговорности в системата като предоставянето на услуги за анонимизиране на транзакции чрез „размесване“ на преведената валута от различни транзакции и затрудняване на проследяването им (Prusty, 2017). Друг интересен аспект на Dash е, че свръх-възлите могат да гласуват за финансиране на други проекти, за бюджет на което са заделени 10% от приходите от всяка транзакция в системата.

Едва няколко месеца по-късно е създадена първата версия на Monero – криптовалута, която предлага по-сериозни възможности за анонимизация на транзакциите. Тази функционалност е възможна чрез имплементацията на криптографския протокол CryptoNote, при който получателят има различен адрес при всяка транзакция, а изпращащият е член на група, но не може да бъде различен от останалите участници (Saberhagen, 2013). Това прави проследяването на потоци от валутата експоненциално по-трудно спрямо броя на транзакциите. Monero добавя допълнителното свойство, че размерът на транзакциите също може да бъде скрит чрез разширение на криптографския протокол Confidential Transaction, наречено Ring Confidential Transactions (Noether & Mackenzie, 2016).

Третата важна валута, предоставяща анонимност на транзакциите, която ще разгледаме, е Zcash. За разлика от останалите споменати валути, Zcash използва протокола Zerocash (не е свързан с Zerocoin), при които се поддържат „защитени“ (shielded) транзакции. Вместо транзакциите да се анонимизират чрез разбъркване на сумите или чрез изпращане от група към еднократен адрес, в Zerocash се ползват т.нар. „zero-knowledge Succinct Non-interactive ARguments of Knowledge” (или zk-SNARK) – специален вид криптографски примитиви, които позволяват на всеки наблюдател в блокчейн мрежата да се увери във валидността на дадена транзакция, без да се разкриват параметрите ѝ (подател, адресат и стойност) (Ben-Sasson, et al., 2014). Подобна защита на анонимността е налична за всички транзакции между „защитени“ (буквално “shielded”) адреси в Zcoin екосистемата, докато „прозрачните“ адреси извършват незащитени транзакции. Допълнително предимство на Zcash е частичната съвместимост с Биткойн, бързата и ефективна валидация на „защитени“ транзакции, съразмерима като необходими ресурси със стандартните транзакции, както и възможността при нужда потребител да разкрие параметрите на своите преводи.

ПРИЛОЖЕНИЕ 5:
ОСНОВНИ НАПРАВЛЕНИЯ ЗА ПРИЛОЖЕНИЕ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА

Етериум като среда за интелигентни договори

Както вече споменахме, основната цел на платформата Етериум е да поддържа възможността за имплементация на интелигентни договори. Това е и причината за имплементационните разлики с Биткойн и други криптовалути.

По същество, договорите в Етериум платформата представляват специални адреси в системата, които имат непразно поле за изпълним код (индикиращ, че са договори, а не сметки на потребители). Въпросният изпълним код се изпълнява на т.нар. EVM (Ethereum VM), която представлява стек-базирана виртуална машина, донякъде подобна на JVM, но много по-проста. Самата виртуална машина е специално разработена, така че да не позволява никаква комуникация извън Етериум мрежата с цел защита на участниците в мрежата от зловреден изпълним код. Освен изпълним код, интелигентните договори имат и място за съхранение на данни.

За разлика от традиционните договори, които представляват набор данни, върху който двете страни са се съгласили, интелигентните договори в Етериум платформата са по-скоро автономни агенти, които могат да бъдат „извиквани“ от потребители или други интелигентни договори (Buterin, н.д.).

Всяка транзакция в мрежата на Етериум съдържа изпращащ адрес, криптографски подпис с частния ключ, отговарящ на изпращащия адрес, количество етер, което следва да бъде предадено, данни (възможно е и да липсват), максимален разход на „гориво“ и цена за „горивото“. Въпросното „гориво“ е начинът на платформата да ограничи разхода на изчислителни ресурси от транзакции и интелигентни договори: всяка изпълнена операция от изпълнимия код има цена в „гориво“, също както и съхранението на данни. Употребата на гориво се заплаща, като цената се определя на пазарен принцип – желаещият да направи транзакция включва цената, която е склонен да плати (в етер) за единица „гориво“ в транзакцията. Ако няма желаещи в мрежата да включат тази транзакция в „добит“ блок, тя просто няма да бъде изпълнена. Съществуват множество услуги, позволяващи да се провери текущата пазарна цена на единица „гориво“ (Shwom, 2016).

Когато дадена транзакция е адресирана към интелигентен договор, в „горивото“ за тази транзакция следва да се включи и необходимото „гориво“ за изпълнение на кода на договора-адресат. В мрежата съществуват и специални транзакции на име съобщения, които се изпращат от интелигентен договор към интелигентен договор (Buterin, н.д.).

Самите интелигентни договори за Етериум се разработват на езици от по-високо ниво, тъй като разработката им директно за EVM би била неефективна. Сред поддържаните езици са Solidity (сходен на JavaScript), Serpent (сходен на Python) и LLL (близък до асемблер за EVM).

EOS.IO като среда за интелигентни договори

EOS.IO е блокчейн платформа, фокусирана върху интелигентни договори. Подобренията, които EOS предлага пред Етериум са най-вече с еволюционен характер – вместо специализираната виртуална машина EVM, в EOS се използва WebAssembly – асемблер, който може да бъде генериран от по-широк набор езици от високо ниво; дизайн на по-децентрализиран пазар на изчислителни ресурси и памет и изключително кратък период между блоковете – 500 милисекунди (EOS.IO, 2018).

Приложения на блокчейн в управление на верига за доставките

Едно от основните приложения на блокчейн технологиите отвъд криптовалутите е в управление на веригата на доставките. При сравнение с традиционните електронни системи за управление на веригата на доставките, блокчейн технологиите притежават някои сериозни предимства, например липсата на централна точка, което позволява по-лесна интеграция на B2B (Business-to-Business) системи и, в по-малък мащаб, интеграция на „Интернет на нещата“ (IoT) технологии (Korpela, Hallikas, & Dahlberg, 2017). Пример за конкретно приложение на блокчейн в тази насока е системата на компанията Modum за контрол на доставките на фармацевтични продукти, които трябва да бъдат съхранявани и пренасяни при строго определени температури (modum.io AG, 2017). При този продукт заедно с фармацевтичните продукти се пренася и IoT устройство, което записва температурата по време на транспорт във вътрешна памет. При смяна на собствеността на продуктите, запазените данни се валидират срещу интелигентен договор и резултатите се записват в съответния блокчейн. Съществуват множество други разработки в областта в различна степен на реализация и зрялост, а някои огромни ИТ компании като IBM, Oracle и SAP разработват собствени решения (Forbes, 2018).

Приложения на блокчейн в електронното гласуване

Възможностите за приложение на блокчейн технологиите в електронното гласуване са осъзнати сравнително рано в развитието им – още през 2016, първата по рода си „разпределена автономна организация“, наречена „The DAO” (съкращение от Distributed Autonomous Organization), която оперира като автономен инвестиционен фонд чрез набор интелигентни договори, осигуряващ възможност за гласуване на всички инвеститори с цел избор на бъдещи проекти, в които да бъде инвестирано (Reiff, 2018).

Идеята блокчейн технологиите да бъдат използвани за демократични избори в контекста на държавни институции също не е нова (Ernest, 2014). При подобни приложения съществуват набор допълнителни изисквания към системата за гласуване, които произтичат от социалните аспекти на такива избори, например анонимност на гласа, гарантирано коректно отчитане на гласовете и възможност за промяна на вота (с цел противодействие на контролиран вот). Освен тях, блокчейн технологиите могат да предоставят и допълнителни предимства, например прозрачност, децентрализация и автономност, които да гарантират честни избори, върху които не могат да влияят вътрешни или външни политически фактори поради възможността за независимо преброяване от всеки.

Приложения на блокчейн в хазартни игри

Интелигентните договори намират приложения и в хазартната индустрия, където могат да бъдат използвани за гарантиране на коректно изпълнение на залозите. Пример за подобно приложение е екосистемата от Етериум разпределени приложения (т.нар. „DApps“, набори от интелигентни договори) FansUnite, която позволява спортни залагания, като създава икономически интерес на т.нар. „Оракули“, които предоставят информация за изхода на спортни събития в реалния свят в Етериум, така че залозите да бъдат обслужени от интелигентни договори (FansUnite, 2018).

По-сложен проблем е разиграването на игри със случаен елемент, вътрешен за играта, от типа на предлаганите от казина, поради трудността за едновременно постигане на консенсус върху генератора на случайни събития и непредвидимост на същия генератор. Съществуват имплементации, които се опитват да решат този проблем чрез смесване на различни източници на случайни данни (т.нар. „ентропия“), например действията на всички играчи в платформата, данни за активност и текущи обменни курсове на криптовалути, акции на компании и традиционни валути (Joy Token, n.d.).

Приложения на блокчейн в доказване на време на създаване

Сравнително нишова, но силно ефективна употреба на блокчейн технологиите е за доказване на време на създаване на документ или друг вид електронни данни (т.нар. timestamping). Пример за подобна услуга с отворен код е “Proof of Existence”, която използва Биткойн блокчейнът (Proof of Existence, n.d.). При въпросната схема потребителят предоставя в системата документа, който желае да сертифицира (или дори само стойността на криптографска хеш-функция за този документ), а системата го вгражда като допълнителна информация в Биткойн транзакция. Предвид разпределения характер на блокчейн технологиите и алгоритмите, които се прилагат за постигане на консенсус, измамата е практически невъзможна в подобна екосистема. Подобна услуга може да се използва в известна степен и като нотариус (Kirk, 2013).

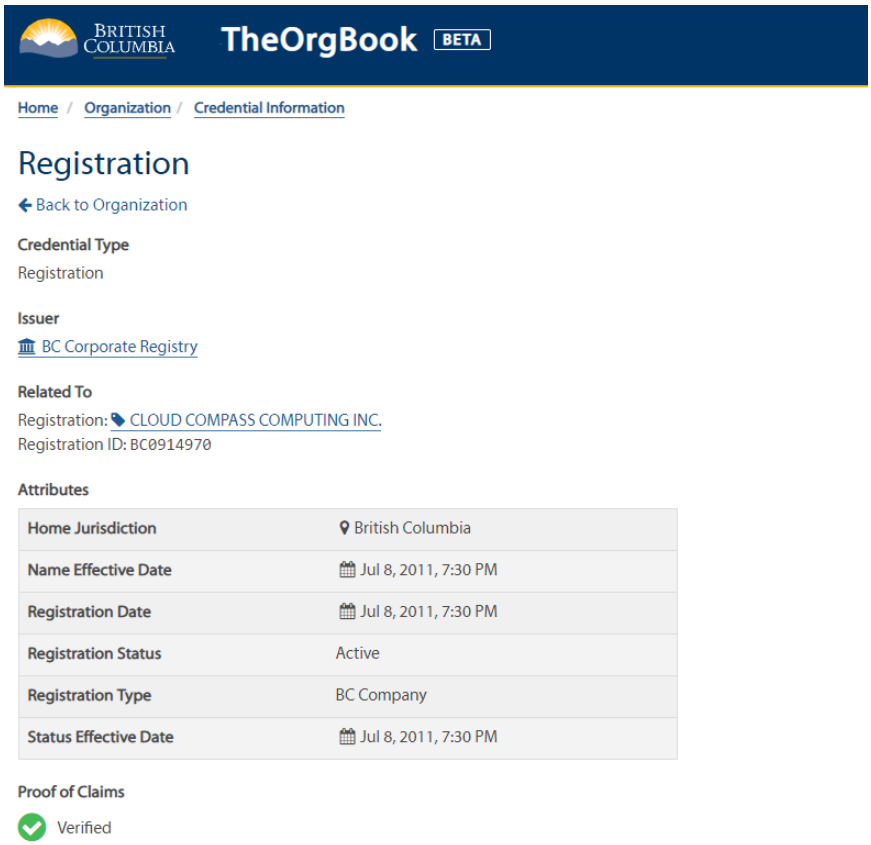
Приложения на блокчейн в одитиране и съхранение на логове

Едно от силно перспективните направления в развитието на блокчейн технологиите е в одитирането и съхранението на логове от АИС. И двете приложения се основават на възможността даден блокчейн да функционира и като разпределена база данни, която е устойчива срещу фалшификации на исторически данни. Пример за технология за съхранението на логове е тази, разработена от компанията LogSentinel, с която е възможно да се използва публична „облачна“ инфраструктура, или да се изгради във вътрешна за организацията инфраструктура, както и възможност да се извършват проверки за съхранените в блокчейна логове (LogSentinel, n.d.).

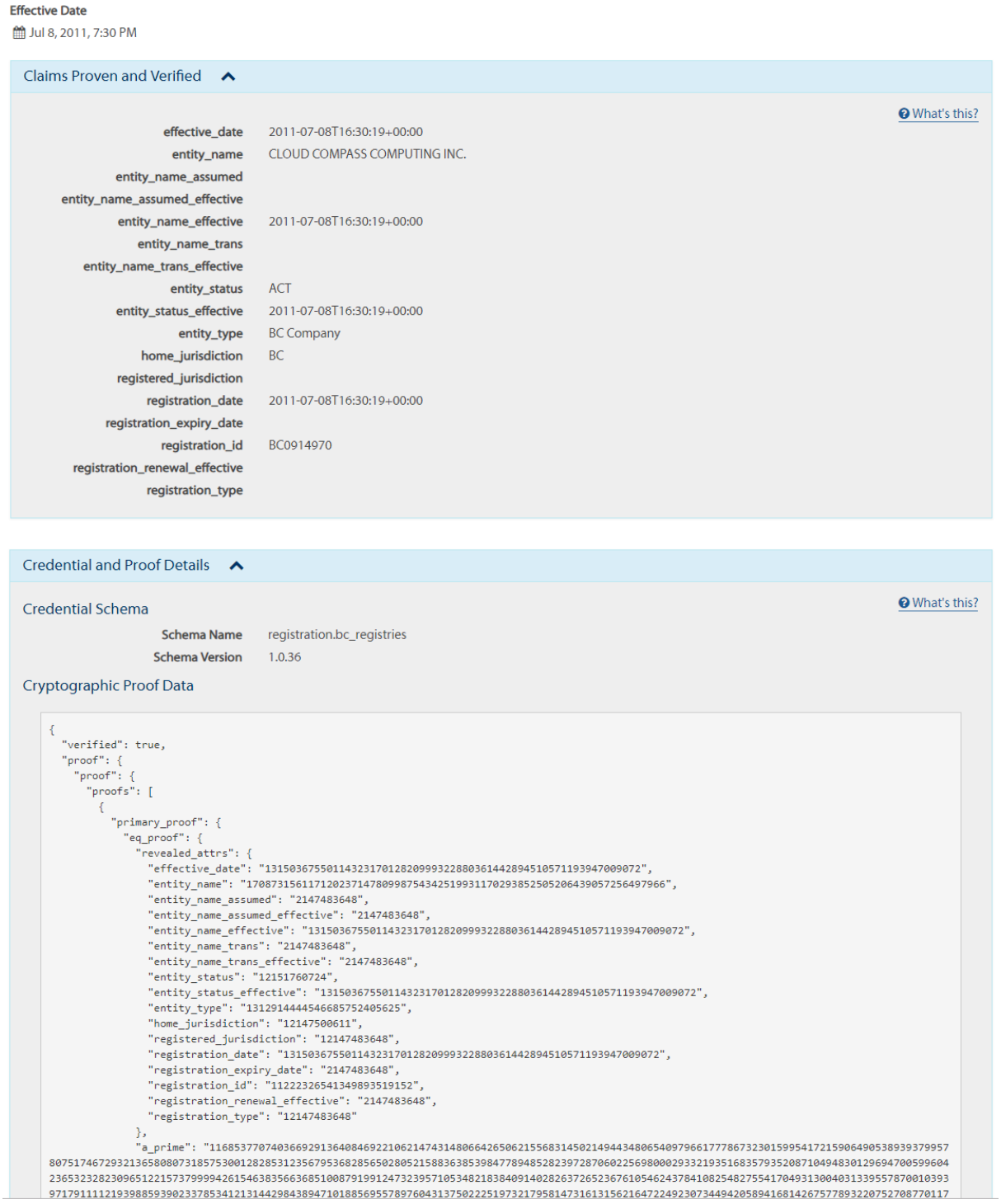
При приложенията за одит се налага употреба на далеч по-сложна и взаимосвързана екосистема, тъй като основното приложение на подобен тип технологии е покриване на законови изисквания, при които често е необходимо данните от одитът да бъдат публични и/или одитът да бъде извършен/потвърден от трета независима страна. При блокчейн технологиите, това може да бъде постигнато и чрез интелигентни договори, които да обработят наличните данни и да извършват и предоставят в реално време резултатите от непрекъснат процес на одит (AuditChain, n.d.).

ПРИЛОЖЕНИЕ 6:
THEORGBOOK

Фигура 36. Първоначален екран на системата



Фигура 37. Обобщени данни за определена компания



Фигура 38. Детайлни данни за определена компания

ISBN 978-619-7262-14-8

Институт по публична администрация
София 1000, ул. „Аксаков“ 1
тел.: 02/940 2556, e-mail: ipa@ipa.government.bg
https://www.ipa.government.bg/