ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“

КАМЕН КАЛЧЕВ
КОСТАДИН ЦВЕТКОВ

КИБЕРСИГУРНОСТ

УЧЕБНИК

София • 2022

Учебникът е създаден с цел удовлетворяване на образователните потребности по дисциплините „Киберсигурност“ и „Защита на информацията в комуникационните и информационните системи“, както и на курса за следдипломна квалификация „Киберсигурност в системите за управление“, водени във Военна академия „Г. С. Раковски“.

Съставянето на учебника е резултат от съвместната работа на полковник професор д-р Камен Калчев (части 1, 2, 3, 4, 5, 6, 7, 8, 9 и 10) и доцент д-р Костадин Цветков (част 11).

Рецензенти
доцент д-р Красимир Димитров
доцент д-р Иван Чакъров

ISBN 978-619-7478-90-7

СЪДЪРЖАНИЕ

1. Въведение в системите за киберсигурност [1]

1.1. Основни определения

Информация –всяко събиране, съхранение, пренасяне, приемане на знания – като факти, данни, възгледи или схващания, под числова, графична или текстова форма, придобити вербално или посредством някаква медия.

Система – събирателно понятие за хардуерните, софтуерните, физическите, административните и организационните мерки, които следва да се разглеждат в единен контекст, когато става дума за сигурност на организирани информационни ресурси.

Информационна система – организирана система в съответствие с определени процедури за ръчно или автоматично събиране, обработване, обмен и разпространение на информация, включваща компютърен и комуникационен хардуер, свързани към тях допълнително оборудване, софтуер, различни способи за представяне на компютърни програми, алгоритми и други спецификации, заложени вътрешно или чрез външен достъп, ръководства и друга документация на хартиен, магнитен, оптичен или друг носител, комуникационни съоръжения, терминали и оборудването им, мултиплекси, точки за включване към мрежи за обмен на информация, параметри за контрол на сигурността, съхранението, технологията, обработката, обмена и разпространението на данни, както и тяхната проверка при цифрово или пакетно комутирано доставяне, както и всички мерки за потребителско идентифициране и верификация.

Система за информационна сигурност е организационно-техническо обединение от сили и средства, стандарти, политики, механизми и процедури, комуникационен и компютърен хардуер, софтуер и фърмуер, които са неделима част от комуникационната и информационната система, предназначена за осигуряване изискванията на държавни и ведомствени нормативни документи по опазване на държавната и служебната тайна чрез защита на данните и ресурсите от случайно или преднамерено разкриване, модифициране, неправомерно използване или унищожаване.

Сигурност на информационната система е способността да се гарантират и защитят наличието, конфиденциалността и целостта на информацията.

Конфиденциалност – основна характеристика на системата за сигурност. Означава възможност за:

- предоставяне на информация единствено от оторизирани лица;
- съхранение в оторизирани физически обекти;
- управление и контрол на разрешените времеви прозорци за съхранение и ползване;
- употреба по оторизиран начин и от оторизирани лица.

Конфиденциалността определя кои са оторизираните субекти, имащи право да притежават и ползват информацията и предоставените ресурси. Тази характеристика позволява подреждане на субектите и информацията в строго йерархична система, наричана нива на конфиденциалност. Само при удовлетворяване изискванията за съответствие на

притежаваните нива на конфиденциалност между субект и информация (информационен ресурс) може да се предостави достъп на едните към другите.

Достъпът до информация се разглежда като способност на даден субект да извършва четене, запис, промяна, копиране, преместване или унищожаване на информация.

Цялост (непокътнатост) – основна характеристика на системата за сигурност, отразяваща способността ѝ да се предпази наличната информация от изменение степента на нейната точност и да се накърни нейната завършеност.

Информацията може да се променя само от оторизираните за това субекти и по оторизираните начини (механизми). Както всяка една по отделно взета промяна, така и всички като цяло неоторизирани промени трябва да се предотвратяват, а ако това е невъзможно, в най-лошия случай еднозначно да се откриват, като се документира всяка стъпка на процеса. Информацията следва да е вярна и точна, да обобщава определен кръг от данни и да бъде относително завършена.

Наличност – основна характеристика на системата за сигурност, отразяваща способността ѝ да се гарантира:

- притежанието на информация от оторизирани лица;
- достъпът до използваема информация само на оторизирани лица;
- необходимите време, повторяемост, ресурси и начин на представяне в съответствие с направената заявка за достъп.

Информацията трябва да бъде налична за оторизираните субекти за оторизираните цели. Конфиденциалността и целостта не трябва да засягат наличността. Наличността не е по-малко важен аспект на информационната сигурност от останалите два.

Сигурността на информационната система може да бъде дефинирана само ако са защитени конфиденциалността, целостта и наличността на информацията и информационните ресурси.

Информационната сигурност е комбинация от превантивни, откриващи и възстановителни мерки. Превантивните мерки включват контрол на риска, отхвърляне или детерминиране на нежеланите събития. Примери за такива мерки са пароли, отличителни значки, планове за работа при непредвидени ситуации, политики за сигурност, файъруоли, засекретявания и др. Предприеманите мерки за откриване на събитията са част от контрола на риска с цел идентифициране на събитията и нежелателните явления. Като такива могат да се посочат инспекторските включвания, проследяващите проверки, сензорите за движение, телевизионните системи за наблюдение и прегледите на сигурността. Мерките за възстановяване на информацията са част от управлението на риска и включват дейности за възстановяването на целостта, наличността или/и конфиденциалността на информацията. Например наблюдение върху допустимия диапазон от грешки, резервни копия, планове за работа при аварии и др.

1.2. *Място и основни функции на системата за информационна сигурност*

Системата за информационна сигурност обхваща всички елементи, нива, звена (възли) и потребители на комуникационно-информационната система. Обекти на защита са:

- личният състав;

- работните помещения;
- комуникационно-информационните ресурси – работни станции и сървъри;
- приложното програмно и системно осигуряване, както и данните към тях;
- комуникационната среда;
- средствата за криптографска защита.

Системата за информационна сигурност изпълнява следните основни функции:

- идентификация и автентификация;
- контрол на достъпа до ресурсите на системата;
- изграждане на защитни стени;
- изграждане на виртуални частни мрежи;
- отдалечен достъп, включително до ресурси на интернет;
- предоставяне на криптографски услуги;
- защита на програмите и данните от копиране, разрушение и изменение;
- наблюдение и регистрация на извършваните дейности;
- антивирусна защита и профилактика;
- защита от излъчване;
- контрол на трафика;
- анализ и откриване пробивите в сигурността на интранет на организацията.

Към посочените основни функции следва да се добавят и т.нар. сервизни функции, като:

- контрол на състоянието на системата;
- откриване и обработка на събития, заплашващи сигурността;
- тестване и самотестване на отделни елементи;
- отчетност на действията, свързани с работата на системата.

Нива на конфиденциалност на информацията в НАТО.

COSMIC (CTS) – строго секретно.

Това е най-високото ниво за класифицирана информация. Достъпността до такава информация на неоторизирани лица може да доведе до сериозна вреда за националната сигурност, сериозно да застраши държавния ред и да води до изключително опасни последици за човешкия живот. За защитата на това ниво се полагат най-големи усилия.

Секретно (NS).

Достъпността до такава информация на неоторизирани лица може да доведе до сериозни вреди за организацията или националната сигурност, например планове за развитието на армиите на страните, членки на Алианса, планове за тяхното разположение и др. Това ниво е второ в йерархията за конфиденциалност.

Конфиденциално (NC)

Това е най-ниското ниво на конфиденциалност. Неоторизиран достъп до такава информация би довел до едни или други вреди за организацията. На това ниво за пръв път е въведено отхвърляне, отказ на достъп, като същевременно се запомнят характеристиките на заявката.

За ограничено ползване (NR).

Нива за класифициране на информацията в икономиката.

Конфиденциална – най-високото ниво на защита на информацията в икономиката. Неоторизиран достъп до това ниво може да предизвика настъпване на крайно неблагоприятни обстоятелства или банкрут. Потребителите се задължават да спазват специални указания за ограничено използване, разпространение или разкриване на такава информация (NDA's).

Чувствителна – достъпът до такава информация води до потенциални тежки финансови вреди.

Частна – достъпът до такава информация води до възможни финансови загуби поради лишаване от конкурентни предимства.

Публична – този вид информация не подлежи на защита.

Критерии за оценка на системите за сигурност.

Критериите са разделени в четири категории – D, C, B и A, подредени в йерархична структура, като D е запазена за системи, предоставящи основната, базисната сигурност. Всяка категория представя най-важните и главни подобрения по опазване на тайната, намиращи приложение в системите за защита на чувствителната информация. Категориите C и B включват подкатегории, наричани класове, които също имат йерархично подреждане по подобие на категориите. Класовете характеризират мрежата от механизми за компютърна сигурност, които те притежават. Осигуряването на коректно и цялостно разработване и внедряване за такива системи е постигнато чрез тестване на всички части, свързани със сигурността им.

Категория D – минимална защита.

Отнася се за системи, които ще се развиват в бъдеще, но които в това си състояние не могат да изпълнят изискванията на по-горните категории и класове.

Категория C – негарантирана защита.

Класовете в тази категория предоставят недостатъчно устойчива защита (необходимост – знание), както и частични способности за одит, за предявяване на отговорност към субектите и предприеманите от тях действия.

Клас C1 – недостатъчна защита на сигурността.

Системите от този клас задоволяват номиналните изисквания за сигурност чрез поддържане на отделни разделени групи от потребители и групи от данни. Тук са включени и някои форми на осигуряващ доверие контрол, способен да наложи спазване на ограниченията в достъпа до индивидуалните данни. Това означава, че на пръв поглед имаме подходящи условия, позволяващи на потребителите да защитят проектите си или частната информация и да запазят другите потребители от инцидентно четене или унищожаване на данни. Клас C1 предоставя среда, за която се очаква да подпомага поддържането на данни с подобни нива на чувствителност. Следващите изисквания са задължителни за системи от този клас:

- Политика за сигурност и негарантирано управление на достъпа. Политиката за сигурност трябва да дефинира и управлява достъпа между обозначени потребители и обозначени обекти на системата. Приложените механизми, като индивидуално, групово и общо управление, списък за контрол на достъпа и др., следва да позволяват на потребителите да управляват достъпа до предоставените от тях ресурси, като това се отнася за индивидуален потребител, за групата като цяло и/или за двете.

- Отговорност, идентификация и автентикация. Изискването тук е да има възможност всеки потребител да се самоидентифицира, преди да започне каквато и да е друга дейност. От

своя страна системата следва да разполага с механизми, например паролиране, за автентикация на потребителската идентификация. Системата трябва да защитава данните за автентикация, така че неоторизираните потребители да нямат достъп до тях.

- Сигурност. Различават се следните аспекти – при работа (на системната архитектура, на системната цялост), на цикъла на живот при тестване.

- Наличие на документи, като ръководство на потребителя за свойствата на сигурността, ръководство за способността да предостави дадена надеждност, тестова документация, документация за конструирането на системата.

Клас С2 – управлявана защита на достъпа.

Системите от този клас се отличават с по-строги мерки за управление на достъпа на потребителите, като различават индивидуалната им отговорност по предприетите действия през процедурите за присъединяване към системата, одит на събитията, свързани със сигурността, и изолиране на ресурси. Минималните изисквания за системи, определени за този клас, са:

- Политика за сигурност (управление на негарантирания достъп и допълнителни предимства). Както за клас С1, с допълнителна възможност за управление на ограниченията за разпространение на правата за достъп. Механизмите за управление на негарантирания достъп трябва едновременно с това да представят действията на всеки потребител и да защитават от неоторизиран достъп. Този контрол на достъпа следва да предоставя достъп или да отказва такъв. Наред с това достъп до обекти в системата, когато няма за това изрично дефинирани права, трябва да е разрешен само на оторизирани потребители. Допълнителни предимства са, че всички оторизации до информацията, съдържаща се в съхраняващите обекти, трябва да бъдат отменени до въвеждане на система за посочване, разпределение и преразпределение на имащите право на това. Не трябва да има информация, включително засекретена, получена от предишни действия на субекти в системата, и тази информация да е достъпна чрез извършване на back действия на който и да е потребител.

- Отговорност (идентификация, автентикация и одит). Системата следва да открива, да предприема действия и да защитава от модификация, неоторизиран достъп или разрушаване последователността за одит или достъпа до обектите, които подлежат на такава дейност. Защитата включва и ограниченията, осигуряващи четене само от оторизирани лица, имащи право на одит на данните. В този клас е задължително да се поддържат функции по регистриране на дейности, като използване на механизмите за идентификация и автентикация, въвеждане на данни в адресното пространство на потребителите, изтриване на обекти и действия, присъщи на системния администратор, на персонала по сигурността или други, свързани със сигурността събития. За всяко подобно регистрирано събитие, одитът следва да идентифицира датата, времето, потребителя, типа на събитието и степента на успех на реализацията. При такава регистрация предварително трябва да бъде направен запис на съществуващото състояние преди въвеждане на промените.

- Сигурност (при работа – на системната архитектура, на системната цялост). Системната архитектура за този клас е задължително да поддържа собствена домейн област, която да защитава ресурсите от външно влияние или намеса. Самите ресурси следва да са дефинирани в подмрежи от обекти и субекти, а системата да ги изолира с цел защита, още повече че част от тях са субекти на управлявания достъп и на изискванията за одит.

Изискванията към системната цялост определят възможността хардуерът и софтуерът да могат периодично да извършват оценка на коректността на действията на хардуерните и фърмуерните елементи.

- Регламентиран жизнен цикъл (тестване на сигурността). Механизмите за сигурност трябва да са тествани и предявяваните изисквания да са налични в системната документация. Необходимо е резултатите от тестването да предоставят достатъчно аргументи, че не съществуват очевидни начини за преодоляване защитните механизми за сигурност. Тестването трябва да съдържа изследване за начините, по които може да се наруши механизмът за изолиране на ресурсите, или за възможните пътища за получаване на разрешение за неоторизиран достъп.

- Документация – ръководство на потребителя за възможностите на сигурността, ръководство за надеждността на предоставените способности, тестова документация и конструкторска документация. Важна част от всички документи е конструкторската документация. Тя трябва да предоставя информация за това каква е философията за защита, и да обяснява как тази философия се реализира в системата.

Категория B – делегирана защита.

Основната идея на тази категория е да се защити целостта на чувствителните нива и да се използва система от задължителни правила за достъп. Системите от категория B следва да поддържат нивата на чувствителност съвместно с основните структури от данни. При тези системи за първи път се изисква наличието на модел на политиката за сигурност и перспективите за неговото развитие.

Клас B1 – защита на сигурността при класифициране.

В този клас се предявяват като минимум изискванията на клас C2, като се доразвиват по отношение на модела на политиката за сигурност, класифицирането на данните, задължителните правила за управление на достъпа за обозначените субекти и обекти. В този клас не съществуват откритите недостатъци за клас C2. Основните изисквания са:

- Политика за сигурност – с основни моменти контрол на достъпа, правила за използване на обектите и класифициране, делегиране управлението на достъпа. Изискванията към контрола на достъпа и правилата за използване са същите като при клас C2. Новото при този клас е свързано с класифицирането. То се отнася за обектите и субектите на системата и се използва при вземането на решение за управление на достъпа. По принцип за изпращане на данни системата изисква и очаква да получи отговор от оторизираните лица за разрешаване на подобни действия, като при това прави регистрация на процесите. Основна характеристика на класифицирането е неговата цялост, което означава, че нивата на класификация следва точно, без двусмислие да отразяват нивата на сигурност за специфични субекти и обекти на системата. Тази характеристика притежава два аспекта – ползване на класифицирана информация от дадено ниво и ползване на информация чрез достъп до множество нива. Първият аспект отразява изискванията към дефиниране на комуникационните канали за вход/изход за всяко отделно ниво, като каквато и да е промяна следва да бъде описана на ръка и приложена към конструкторската документация. Вторият аспект отразява начина, по който може да достигне информация по един комуникационен канал до различни нива на сигурност. В този случай следва недвусмислено да се опишат протоколите за достъп и да се гарантира, че не съществува друг път освен посочения за достъп до различните нива. Важна особеност е

дефинирането на съответствието за въвеждане на информацията съобразно с нейната класификация в необходимото ниво на сигурност. Системата поддържа също представянето на информацията към крайния потребител да съответства на зададен формат. Последният акцент е върху делегирането на управлението на достъпа. Той е в сила за всички ресурси и субекти на системата. На всички тях се задава ниво на класифицираност. Основната идея по отношение на класифицираността е, че са разрешени само ресурсите, които имат по-ниско или равно ниво на достъпа от това на субекта.

- Отговорност – с основни моменти идентификация, автентикация и одит. Системите от този клас задължително следва да притежават всички характеристики на тези от клас С2. Към тях се добавят изискванията за идентификация на нивото на достъп (нивото на класификация) на потребителя. Системата следва да игнорира всички опити за достъп от името на оторизиран потребител. По отношение на одита системата следва да предоставя данни само на точно и ясно определени лица, като при това прави пълна регистрация на лицето (по неговия ID), датата, времето, използваните процедури и предприетите действия, както и върху кои ресурси е въздействано.
- Сигурност – с основни моменти оперативна сигурност и сигурност относно жизнения цикъл. Освен изискванията за системи от клас С2 се предявяват и допълнителни изисквания за имплементиране на сигурността във всички етапи на жизнения цикъл. По-конкретно това са изисквания за наличието на тестови резултати от реализираните специфични приложения, разширяващи възможностите на системата. Тези приложения не трябва да нарушават сигурността в никакъв аспект.
- Документация на системата – с основни акценти върху ръководствата на потребителя и ръководството за надеждността на предоставяните възможности.

Клас В2 – структурирана защита.

Този клас усъвършенства системите за защита. Използваният модел на политика за сигурност изисква механизмите за достъп и делегирането на управлението на достъпа да са валидни не само за всички обекти и елементи на системата, но и за всички структурно обединени системи. Използваните комуникационни канали се адресират. Следва внимателно да се структурират защитените критични елементи, както и критичните елементи, които остават незащитени. Специално внимание се обръща на реализирането на интерфейса с външната среда и детайлното тестване и преглед на резултатите. Механизмите за автентикация са значително по-строги, надеждността на предоставяните възможности е подобрена, като тяхното управление е делегирано на системния администратор, а операторските функции и строгият контрол на управлението на конфигурацията са задължителни. Системата остава да е относително защитена от проникване. Характерните изисквания са съсредоточени към:

- Политика за сигурност, като акцентът се поставя върху контролиране сигурността на достъпа, използване на обектите, класифициране – цялостност, обмен на данни по нива, решения за достъп до няколко нива, решения за достъп до едно ниво, класифициране нивата на чувствителност на субектите, класифициране на устройствата.

Политиката за сигурност съдържа всички основни моменти на предходния клас, като допълнително са включени изисквания, с които се делегира отговорност към системата с оглед това, че самостоятелните входни/изходни устройства и телекомуникационни канали нямат собствени механизми за защита. На следващо място се въвежда контрол над

разпространението на наименования, имащи класификация и включени към чувствителни нива, предназначени за обмен. Налага се изискването всички заявки за отпечатване или изработване на друг веществен носител на чувствителна информация да бъдат строго контролирани или забранявани, когато надхвърлят нивото на достъп. Следващото изискване е нивата на чувствителност на субектите да бъдат незабавно присвоени и на терминалите, от които те работят. Това се прави с оглед даден субект да работи само от един терминал. По отношение на използваните устройства следва да се зададат минималното и максималното ниво на сигурност на прикачените физически устройства. Това е необходимо, тъй като различните устройства се намират в различни среди с вариращa сигурност. Управлението и контролът на делегирания достъп се разпростира върху всички ресурси (субекти, съхраняващи бази, обекти, входно/изходни устройства).

- Отговорности – с акцент върху идентификация, автентикация и одит. Освен изискванията, предявявани към клас B1, по отношение на отговорността се налага допълнително да се осигури защитен път, по който да се обменят данните от потребителя, искащ свързване до системата.
- Сигурност – има се предвид оперативна сигурност (системна архитектура, системна цялост, анализ на скритите канали, управление на надеждността на услугите) и сигурността през отделните цикли на живота на системите (тестване на сигурността, разработване на спецификации и гарантиращи условия, управление на конфигурацията). Допълнителните изисквания към системната архитектура налагат отделните устройства да бъдат сегментирани по предназначение. Системите следва да бъдат добре структурирани независимо от добрата конфигурация на самостоятелните модули. Налага се потребителският интерфейс да бъде цялостно определен и всички елементи идентифицирани. Важно изискване е да се прави обзор за скрити канали за съхранение на данни.
- Документация – с налични ръководства на потребителя и на надеждността на устройствата и услугите, тестова документация и цялата документация по конструирането на системата.

Клас B3 – сигурни домейни (области).

Системата отговаря на изискванията за мониторинг на средата за достъп на субектите към обектите, не позволява вмъкване на фалшива автентикация, различава достатъчно малки факти и може да ги подлага на анализ. Тези системи са така структурирани, че изключват всички елементи, нямащи отношение към сигурността. Разполагат с администратор по сигурността, механизмите за одит са разширени и обхващат събитията, свързани със сигурността на комуникациите, както и задължителното наличие на процедури за прикритие на системата. Тези системи притежават висока степен на устойчивост на проникване.

Особености на политиката за сигурност:

а) Контрол на външния достъп – позволява потребителите да специфицират и управляват предоставените обекти за общо ползване и да управляват ограниченията в разпространението на правата за достъп. Контролът на външния достъп и механизмите на реализацията му предотвратяват опитите за неправомерно включване към системата. Този контрол се разпростира над всеки обозначен обект, списък на индивидуални или групови потребители. Нещо повече, за всеки обозначен обект е възможно да се определи списък на обозначени субекти или групи субекти, чрез които се разрешава достъпът.

б) Използване на обекти – както за клас B2.

в) Класификация на обектите – както за клас B2.

г) Делегирано управление на достъпа.

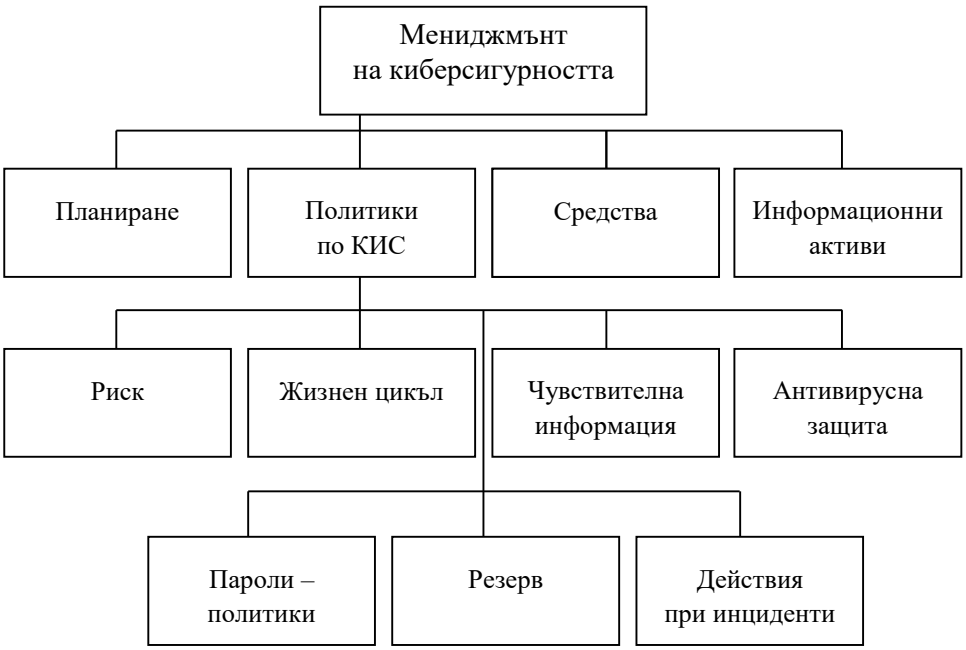
2. Мениджмънт на киберсигурността – политики, стандарти и процедури [2]

Мениджмънтът на киберсигурността представлява система от взаимнообвързани процеси по управление на информационни ресурси за постигане на широкообхватна цел по контрол на достъпа, осигуряване цялостност и наличност на тези ресурси.

Поради широкообхватната цел на мениджмънта (решаването на задача с голяма сложност) се прилагат методи на управление, обединяващи процесите по планиране на ресурси и прилагане на технологии.

Елементи на мениджмънта на киберсигурността:

- наличните информационни активи на организацията;
- политиката по киберсигурност на организацията;
- средствата, с които се реализира политиката по киберсигурност на организацията (организационни, технически и др.);
- планиране на ресурсите по киберсигурност на организацията (фиг. 1).



Фиг. 1. Елементи на мениджмънта на киберсигурността

Необходимо е изпълнението на две важни условия за реализирането на успешна политика за киберсигурност.

Първо, създаване пълен списък на информационните активи на организацията.

Второ, анализиране как тези активи се използват (от служители, партньори, клиенти и др.)

Политика по киберсигурност на организацията.

Политиката по киберсигурност е основният фактор, позволяващ на организацията успешно да преодолява заплахите от киберпространството. Тя включва регламентиране на поведението на организацията в следните основни области:

- определяне и управление на риска;
- определяне на жизнения цикъл на информационните активи;
- определяне на чувствителната информация за организацията;
- антивирусна защита;
- идентификация и автентификация (политика за пароли);
- резервиране и осигуряване на надеждност на активите (данните);
- действия при инциденти.

Определяне и управление на риска.

При определянето на риска от прояви на заплахи в киберпространството организациите се стремят да определят максимално точно възможните загуби – веднъж директно върху информационните активи и втори път индиректно върху основните дейности на организацията. Изборът на подходящ метод, съответстващ на възможностите за анализ в условия на неопределеност, е възлов елемент, влияещ непосредствено върху всички елементи на политиката на организацията.

Определяне на жизнения цикъл на информационните активи.

Жизненият цикъл в политиката по киберсигурност обхваща всички етапи по придобиване, използване и освобождаване на организацията от информационни активи.

Определяне на чувствителната информация за организацията.

Това е процес, който позволява да се обективизира основната причина за необходимостта от мениджмънт. Всяка организация има чувствителна информация, която не иска да бъде изложена за свободен достъп, като определени продукти, проекти, промоционални планове, стратегии, финансови прогнози, медицински досиета на персонала и др. Политиката за управление на сигурността в киберпространство трябва да подсили официалните класификации на информацията за компанията и да уточни правилата, насоките и процедурите за защита за всяка от тях. Това трябва да е ясно за служителите и какви са последиците от неадекватното им прилагане. Необходимо е да има собствена информация от редовно одитиране по отношение на начина на обработка, кой има достъп, до какво нивото, за каква цел и др.

Антивирусна защита.

Антивирусната защита има основно отношение към процесите и процедурите при свързване с външните за организацията системи, с които тя трябва да взаимодейства (интернет, съдружници, клиенти, държавни органи и др.). В тази насока политиката включва анализ на заплахите от зловреден софтуер по отношение на активите и определяне на решение (търговско или собствено) за разполагане на антивирусен софтуер. От значение е неговото класифициране (по видове – мрежов, сървърен и др.), инсталиране в съответствие с приетия жизнен цикъл, поддръжка и действия за доклад и отчитане на инциденти.

Идентификация и автентификация (политика за пароли).

Управление на паролите.

Паролите са първата линия на защита, когато става въпрос за контролиране на достъпа до защитени системи и информация. Управлението на паролите включва:

- процедури за защита на активи с пароли и администраторски профили;
- методи за произволно генериране на пароли, еднократни пароли и двуфакторен идентификационен код;
- продължителност на живота на паролата;
- изтичане и подновяване на паролата;
- процедури за почистване на достъпа на бивши служители;
- дължина и качества на приемливи пароли.

Резервиране и осигуряване на надеждност на активите (данните).

Архивиране и възстановяване.

Причината голяма част от използваната информация да е дигитализирана и съхранявана като информационен актив, е способността на технологията да автоматизира информационните процеси, което значително повишава ефективността в управлението. Затова всяка развита организация не може да си позволи загуба на информация, оттам и загуба на ефективност в управлението. Основно значение имат процесите на архивиране и възстановяване. Процесът на архивиране може да се класифицира по видове, методи и технологии за архивиране, както и да се създаде процедура за действия в извънредни ситуации.

Действия при инциденти.

Политиката трябва да обхваща достатъчно практични стъпки, които дадена организация трябва да предприеме, когато се случи киберинцидент. Документираните задачи за работа при инциденти са насочени към осигуряване на информационни активи с цел минимизиране на щети, и то възможно най-бързо. Освен предоставянето на незабавна защита на място, писмените задачи за работа при инциденти ще укрепят организационното обучение и ще подпомогнат отговорните органи.

3. Направления за неоторизиран достъп [3, 4, 5, 6]

Основни събития, белязали началото на умишлените опити за неоторизиран достъп.

Първите компютърни хакери се появяват в Масачузетския технологичен институт. Името им идва от термин, използван за група в Университета, която „хаква“ електрически влакове, релси и стрелки, за да работят по-бързо и по-добре. Някои от членовете на групата прехвърлят любопитството и уменията си към новите мейнфрейм компютърни системи, използвани в Института.

През 70-те години на XX в. хакерите влизат в регионалните и международните телефонни мрежи, за да провеждат безплатни телефонни разговори. Един от тях, Джон Дрейпър, установява, че свирка играчка, която се раздава с детски храни, генерира 2600-херцов сигнал – същият тон, който дава достъп до системата за превключване за далечни разговори на американската телекомуникационна компания AT&T.

Дрейпър създава синя кутия, която в съчетание със свирката позволява на хакерите да се обаждат безплатно. По-късно американско списание публикува „Тайните на малката синя кутия“ с подробни инструкции за създаване на устройството и скандалът с телефоните

ескалира. Сред поддръжниците на идеята са студентите Стийв Возняк и Стийв Джобс, бъдещите основатели на Apple Computers, които създават домашен бизнес за производство и продажба на сини кутии.

Телефонните хакери започват да се преориентират към компютърната сфера и първите електронни бюлетини (BBS) се появяват.

Таблата (с имена като „Параграф 22“), предшественици на Usenet нюзгрупите и електронната поща, стават много популярни сред хакерите за клюки, обмен на трикове и публикуване на откраднати компютърни пароли и номера на кредитни карти.

Започват да се оформят хакерски групи. Сред първите са „Легионът на съдбата“ в САЩ и Компютърен клуб „Хаос“ в Германия.

Филмът „Военни игри“ показва хакерството на широката общественост и легендата за кибергероите е родена. Главният герой, чиято роля се изпълнява от Матю Бродерик, се опитва да проникне в компютъра на производител на видеоигри, за да поиграе, но вместо това попада във военен компютър за симулация на ядрена война.

Компютърът с кодовото название WOPR (игра на думи с истинската военна система, наречена BURGR) погрешно интерпретира желанието на хакера да играе глобална термоядрена война като изстрелване на вражеска ракета. Проникването в системата хвърля военните в пълна бойна готовност. Същата година властите арестуват шест тийнейджъра, известни като „Банда 414“ (кодът, по който са открити). В продължение на девет дни те проникват в 60 компютъра, сред които са тези на Националната лаборатория в Лос Аламос, където се разработват ядрени оръжия.

Списанието 2600 (www.2600.org) започва да излиза редовно, а година по-късно се появява и онлайн изданието Phrack (www.phrack.com). И двете предлагат съвети за начинаещи хакери, както и коментари по актуални въпроси. Днес 2600 може да се намери във всички по-големи магазини в САЩ.

Смята се, че първият вирус за MS-DOS (1986) е (c) Brain, който заразява „boot“ сектора на дискетите и така се разпространява. Вирусът няма деструктивни функции, тъй като е замислен като инструмент за пресичане пиратско копиране на софтуер за IBM PC за следене на сърдечни заболявания. Съставен е от двама братя в Пакистан. Впоследствие кодът на този инструмент се използва за създаване на едноименния вирус.

Робърт Морис, студент в Университета „Корнел“ (1988 г.) и син на учен в Националната агенция по сигурността, пуска саморазмножаващ се червей в правителствената мрежа ARPAnet (предшественик на интернет), за да тества ефектите му върху UNIX системите. Червеят излиза извън контрол и заразява 6000 свързани в мрежа компютъра, като задръства правителствените и университетските системи. Морис е изгонен от „Корнел“ и глобен.

По време на радиосъстезание (1993 г.) с участие на слушатели Кевин Пулсен и двама негови приятели проникват в телефонната система на радиостанцията и блокират всички обаждания с изключение на техните. Така „спечелват“ две поршета, екскурзии и 20 000 щатски долара.

Пулсен, издирван за проникване в телефонните системи на фирми, излежава пет години затвор за компютърни и телефонни измами. (След както излиза от затвора, работи като журналист на свободна практика в областта на компютърните престъпления.)

През 1993 г. в Лас Вегас се провежда първата хакерска конференция Def Con. Идеята е еднократен купон за довиждане на BBS (вече заместени от Мрежата), но мероприятието е толкова популярно, че става годишно събитие.

Инструменти.

Интернет започва бързо развитие, след като новият браузър, Netscape Navigator, прави информацията по-достъпна. Хакерите бързо се вместват в новата тенденция, като прехвърлят цялата си информация и програмите си от старите BBS на новите хакерски сайтове.

Липса на компютърна хигиена.

Неопитни имейл потребители безропотно препращат електронно съобщение, което предупреждава потребителите да не отварят писмо с фразата Good times в темата на съобщението. Посланието, предупреждаващо за вирус, който унищожава информацията на твърдия диск, демонстрира саморазпространяващата се сила на лъжливите писма. Все още подобна техника се използва изключително успешно в различни форми.

Резултат.

Серийният кибернарушител Кевин Митник е заловен от федерални агенти и обвинен в кражбата на 20 000 номера на кредитни карти. Той лежи в затвора четири години преди процеса и става много популярен сред хакерския ъндърграунд.

Руски кракери източват 10 млн. щ.д. от Citibank и прехвърлят парите по сметки в целия свят. Владимир Левин, 30-годишният водач на групата, използва служебния си лаптоп в извънработно време, за да прехвърли парите в сметки във Финландия и Израел.

Безплатни приложения.

През 1997 г. Излиза AOHell, безплатно приложение, което позволява на нарастващо общество от неопитни хакери да всее смут в America Online. В продължение на няколко дни стотици хиляди потребители на AOL намират пощенските си кутии задръстени от писма с големина по няколко мегабайта, а стаите за разговори са пълни със спам.

Компютърни вируси.

Вирусът Melissa (1999 г.) успява да се разпространи с алармираща скорост, като заразява хиляди компютри и причинява загуби за 80 млн. долара. Поради това продажбите на антивирусен софтуер поставят рекорд. Вирусът стартира програма, която праща свои копия до първите 50 потребители от адресната книга на Outlook. Той заразява също документи на Microsoft Word на твърдия диск и ги изпраща на същите 50 потребители. Първоначално вирусът не е с деструктивни функции, но последствията от него са претоварване на пощенските сървъри и намаляване производителността на мрежата.

През следващата година се разпространява подобен вирус, който препраща на автора си потребителски имена и пароли, съхранявани на твърдия диск на заразения компютър.

Отказ за обслужване (Denial of Service – DoS attacks).

В една от най-големите DoS атаки хакери вземат на прицел eBay, Yahoo, Amazon и други водещи интернет сайтове. Те провеждат серия DoS атаки, като резултатът е спирането на тези сайтове за няколко часа.

Кибератаки срещу Естония.

Атаките продължават около три седмици. Съгласно официалните доклади на Естония в първоначалните атаки са открити IP адреси на правителствени служби в Русия. Естонският външен министър обвинява Москва за атаките. Според съобщенията най-малко един милион

компютъра са използвани в киберофанзивата срещу уебсайтовете на естонското правителство, банки и медии, което довежда до временното им блокиране.

Особености на заплахите за мрежите.

Под уязвимо място се разбира всяка точка на компютърните и комуникационните системи и на системата за тяхната защита, където те са слабо защитени от заплахи и атаки, свързани със сигурността им. Уязвимите места в една система зависят от конкретната ѝ реализация.

В зависимост от това как се извършва атаката срещу мрежата, заплахите се разделят на външни и вътрешни.

Външни заплахи.

В локална мрежа, която не е свързана към интернет, този вид заплахи не са сериозен проблем. Единственият вариант за включване на външен потребител към мрежата е да се прикачи към нея или да се включи с помощта на периферен терминал. Днес обаче, когато почти всяка локална мрежа има достъп до интернет, външните заплахи са основен проблем за мрежовата сигурност. Вариантите за проникване в една система са различни – неоторизиран достъп, DOS атаки, компютърни вируси, троянски коне и др.

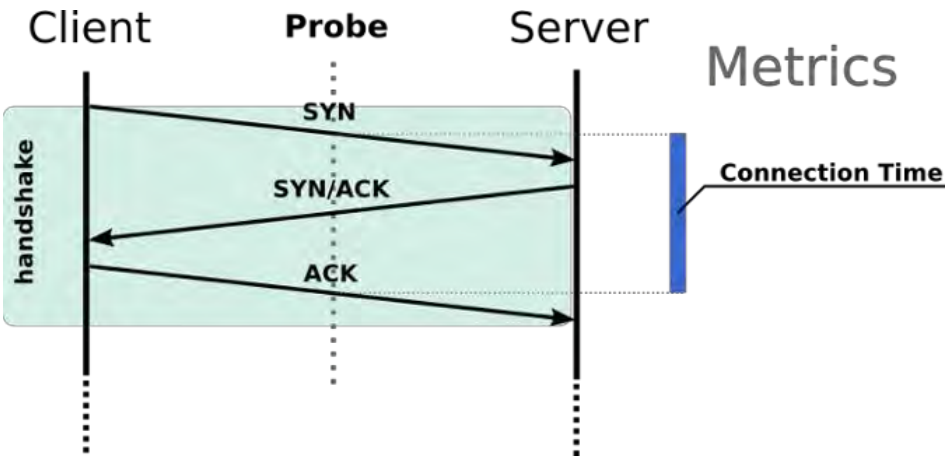
Под неоторизиран достъп се разбира неразрешен достъп до данните в една компютърна система.

Отказ за обслужване (Denial of Service – DoS).

Този тип атака се постига чрез съгласувано насищане на компютъра цел с множество външни заявки, които той не може да изпълни или изпълнява толкова бавно, че се оказва недостъпен и впоследствие не е в състояние да осигурява услугите си по предназначение. Такава атака предизвиква натоварване на мрежовите устройства или сървъри и те не могат да обработват подадените им заявки, поради което ги отказват (drop). Устройството, към което е насочена атаката, се опитва да обработи всички заявки за връзки и по този начин се утилизират всички възможни ресурси. Намерението е да се наруши мрежовата свързаност, за да се отворят множество фалшиви TCP или UDP (User Datagram Protocol) връзки. Този вид атаки често се използват наред с други атаки, като целта им е да дестабилизират системите за сигурност преди реалната атака.

Най-често мишените на тези атаки са сървърите на най-популярните интернет сайтове, като стремежът е да се наруши нормалната операция на дадена система или мрежа. Целта е да се претовари или спре достъпът до системата или дадения ресурс на мрежата, т.е. да се откаже (спре) достъпът на легитимни потребители до различните услуги.

Съществуват три типа DoS атаки, които целят нарушаване на мрежовата свързаност. Те са проектирани така, че да се възползват от слабостта на TCP протокола и по-специално от процеса на установяване на връзката (TCP tree-way handshake). Установяването на връзката при TCP се извършва от тройна размяна на пакети, както е показано на фигура 2.



Източник. https://www.performancevision.com/blog/diagnose-tcp-connection-setup-issues/

Фиг. 2. Установяване на връзката с TCP протокол

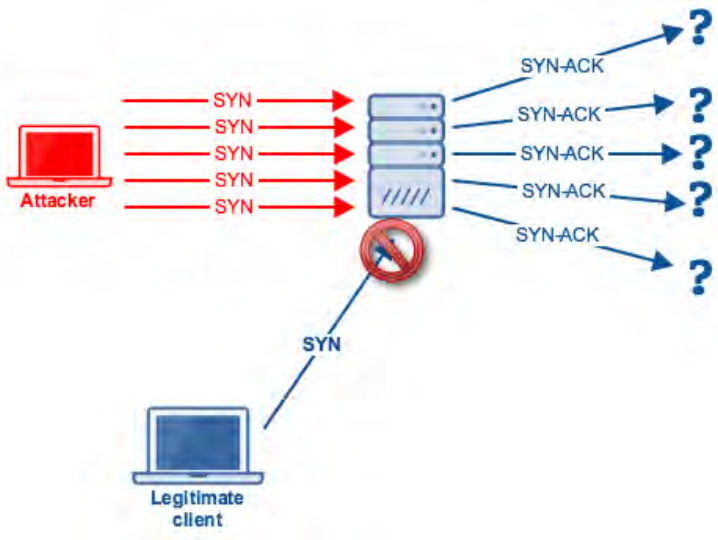
Клиентът се опитва да установи връзка с уеб сървъра.

Първо той изпраща SYN (синхронизиращ) пакет до сървъра, за да се синхронизират поредните номера на клиента и сървъра. SYN пакетът съдържа ISN (Initial Sequence Numbers) на клиента. SYN, ACK, RST и други са битове (флагове) от хедъра на пакета. В този първи т.нар. SYN пакет SYN = 1, ACK = 0.

При втория пакет подателят вече е сървърът и той едновременно потвърждава, че е получил ISN номерата на клиента, и изпраща своите ISN номера (SYN = 1, ACK = 1). Сървърът увеличава с единица поредния номер на клиента и му го изпраща обратно като свой номер на потвърждение (acknowledgment number).

Последната стъпка в този процес на обмяна е пак от страна на инициализатора, който изпраща ACK пакет на сървъра. Връзката вече е установена.

При TCP SYN претоварването има претоварване на мишената на атаката чрез използването на множество подправени SYN пакети, които симулират валидни заявки за връзки. Тези пакети се изпращат на сървъра все едно са начало на уговарянето на връзка, той отговаря с SYN-ACK, но последната стъпка от процеса никога не настъпва, никога не се получава третият пакет ACK. Всеки SYN пакет заема определен ресурс на мишената, следователно при множество SYN пакети, изпратени от атакуващия, машината, която е цел на атаката, се претоварва и спира да отговаря на всички заявки за връзки, включително на реалните. Налице е отказ от обслужване, показан на фигура 3.



Източник. https://defintel.com/blog/index.php/2017/05/these-6-dns-attacks-threaten-your-business.html

Фиг. 3. Схема на TCP SYN претоварваща атака

Подправянето на SYN пакети най-често се състои в това, че се подменя адресът на подателя с цел да се прикрие самоличността на атакуващия или да се заобиколи дадена защитна стена, като се използва адрес от нейните списъци за разрешение на достъпа.

Допълнително тази техника позволява да се причини двойна вреда, защото освен мишената и реалните машини, които са с преправения адрес на подателя, получават множество пакети от самата мишена. Всяка полуотворена връзка заема ресурс, а броят на тези връзки е краен. След достигането му устройството спира комуникацията с потребителите, докато тези отворени връзки не се затворят и изчистят от стека.

SYN атаките са прости атаки, но те все още се използват масово и имат голям успех поради следните особености на протокола:

- SYN пакетите са част от нормалния мрежов трафик и следователно е трудно (по-скоро нелогично) да се филтрират.
- За изпращането на SYN пакети не е необходим канал с огромна пропускливост, т.е. всеки нормален потребител има ресурса да извърши такава атака.
- Лесно се променя адресът на подателя поради факта, че не се изисква отговор от мишената.

Смърф атаки (Smurf attacks).

Атакуващият може да „изяде“ канала на жертвата, като препраща безполезен трафик към мрежата й. Това е класически пример за смърф атаки.

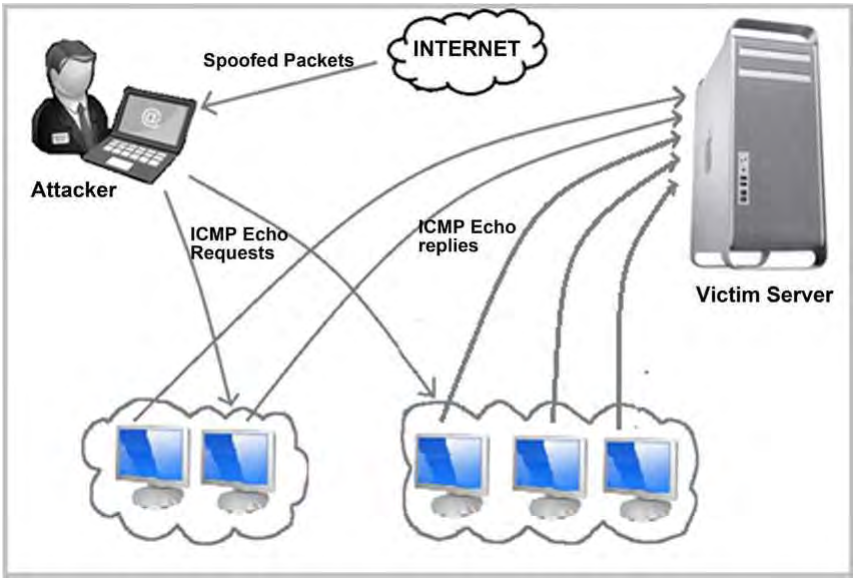
Два са компонентите, изграждащи такава атака:

- Използване на фалшиви ICMP (Internet Control Message Protocol) Echo-Request пакети (ping) работи с два определени ICMP пакета – Echo-Request и Echo-Reply).
- Маршрутизиране на пакети посредством т.нар. broadcast адреси (до всички абонати). Това са адреси на 2-ри и 3-ти слой, които карат мрежовото устройство да ги разпраща на всичките си портове. Това ли са двата компонента?

ICMP протоколът по принцип се използва за обработване на грешки (по-скоро да ги съобщава) и да контролира връзката на 3-ти слой.

Друга широка употреба е ping услугата (Windows ползва ICMP за ping, а Unix, Cisco IOS използват UDP пакети на произволен висок порт).

При Smurf атаките ICMP echo-request пакети се изпращат към броудкаст адреса (broadcast address) на отдалечени мрежи с цел да се наруши нормалната работа на мрежата. На фигура 4 е показано как се провежда такава атака.



Източник. https://www.researchgate.net/figure/SMURF-Attack_fig2_319532864

Фиг. 4. Провеждане на smurf атака

В смърф атаките обикновено има атакуващ, посредници и жертва (в този случай това е сървърът).

Разновидност на смърф атака е Fraggle атаката, но тя работи с UDP вместо ICMP. Fraggle атаките използват Chargen и Echo UDP програми, които заемат UDP портове 19 и 7. Тези две приложения действат на принципа на ICMP ping и са проектирани да проверяват дали дадени компютри са включени в дадена мрежа. Chargen и Echo изпращат отговор на всеки, който прати трафик на обособените портове. Атакуващият може да се възползва от това, като създаде безкраен цикъл, който да препраща трафик между тези портове.

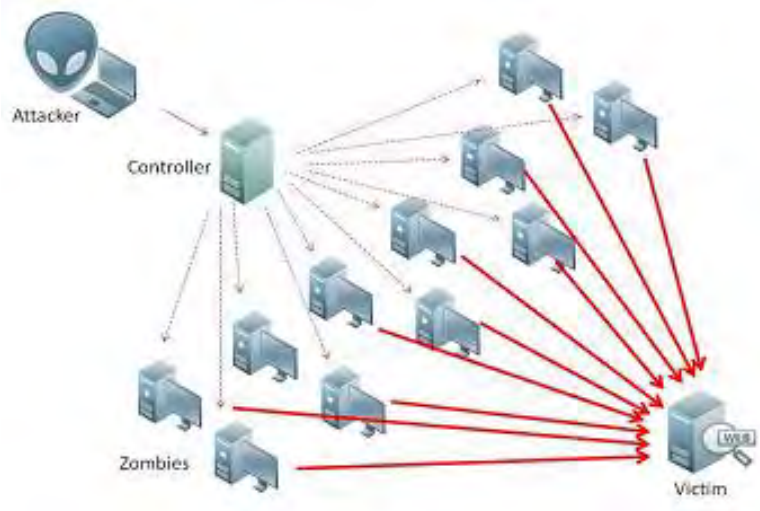
Land.c атаки.

Изключително прост и ефективен пример за DoS атака. Атакуващият изпраща множество SYN пакети с еднакви адреси и портове на подателя и получателя. Целта е да се накара жертвата да изпраща отговор на този пакет сама на себе си. Процесът е цикличен, скоро машината жертва остава без ресурси и спира да предоставя услуги. Хитрото при тази атака е, че атакуващият използва ресурсите на жертвата срещу самата нея.

Разпределени DoS атаки (Distributed DoS).

Този тип атаки изисква предварително планиране и подготовка на атакуващия. Той използва различни системи, свързани към интернет, за да атакува определена жертва, и това ги прави много трудни за проследяване и противодействие.

Подготовката на атаката се състои в това, че атакуващият предварително разбива защитата на няколко машини в интернет и ги поставя под свой контрол, като инсталира вреден код. Тези вече компрометирани компютри се наричат агенти (зомбита), защото следват сляпо командите на атакуващия. Атакуващият ги използва за координирана едновременна атака от всички зомбита към жертвата. Тази атака изяжда канала и мрежовите ресурси на атакувания. Тя е високоефективна, тъй като е координирана (общият ресурс на всички зомбита е много по-голям от този на атакуващия) и изключително трудна за проследяване. По правило атакуващият контролира зомбита от обществено достъпна машина през прокси или като използва техниката на подправяне на адреса си. Начинът на действие е показан на фигура 5.



Източник. https://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/532197/

Фиг. 5. Действие на DDoS атака

Спам (Spam).

Спам е използване на среда за електронни комуникации за масово изпращане на нежелани съобщения. Най-известната форма на спам е съобщения с рекламно съдържание по електронната поща.

Спамът се използва от рекламни търговци, за които това е безплатен начин да рекламират своите продукти. Той се появява като проблем, след като интернет става достояние на обществото. Изпращането на спам се увеличава с геометрична прогресия през годините и сега по данни на статистическите изследвания възлиза на около 80 – 85% от съобщенията в световната мрежа.

За да може да бъде изпращан спам до потребителите, са необходими техните имейл адреси. Разпространителите на спам разработват специални инструменти, като Webcrawler, с които сканират цели интернет сайтове за всичко, което прилича на имейл адрес. Впоследствие събраните адреси започват редовно да получават нежелани електронни съобщения с рекламно или друго съдържание.

Социално инженерство (Social Engineering).

Това е атака, основана на заблуда и измама на потребителите. Нейната цел е хакерът да добие информация, която нормално не се дава на непознати. В интернет заблудата често включва създаване на фалшив сайт или изпращане на фалшиво електронно писмо (с неверен

подател), така че хората си мислят, че предоставят информация (лични данни, имена, пароли, номера на кредитни карти и др.) на реално съществуваща организация. Впоследствие хакерът се възползва от придобитата информация най-вече за материални облаги.

Типична такава атака е фишинг (phishing). Думата phishing фонетично съвпада с английската дума fishing, която означава ловя риба.

Phishing атаката представлява опит за добиване на информация (понякога недиректно пари) като потребителски имена, пароли и данни за кредитни (дебитни) карти чрез представяне за доверен субект в електронна комуникация. Комуникирането, претендиращо да произтича от популярни социални интернет сайтове, сайтове за провеждане на търгове, сайтове за интернет разплащания или IT администратори, често примамва нищо неподозиращите потребители. Този тип атака обикновено се извършва посредством услугите за мигновени съобщения или електронна поща и често насочва потребителите да въведат данни в лъжливи сайтове, които са почти идентични с истинските.

IP спуфинг (IP spoofing).

IP спуфинг е метод за маскиране на едно устройство като друго. Реализира се чрез промяна в хедъра на IP пакетите на изпращащия компютър. IP адресът на изпращащия компютър се подменя с друг IP адрес. По този начин съобщенията от страна на компютъра получател изглеждат сякаш са изпратени от компютър с друг IP адрес. IP спуфингът може да бъде използван за неотозизиран достъп, кражба на данни и др.

DNS спуфинг (DNS spoofing).

В резултат от IP спуфинг атака атакуващият компютър се представя за DNS сървър на компютъра жертва. Когато жертвата подаде заявка за намиране на IP адрес по име, например при отваряне на уебсайт, атакуващият компютър прихваща заявката и връща собствения си IP адрес. Потребителят на компютъра жертва се доверява на сайта източник, без да подозира, че е подменен, и използва неговото съдържание.

Подслушване на мрежата (Sniffing).

Подслушване се използва от хакерите, за да се прихване всеки пакет, предаван по мрежата. Прихванатите пакети се натрупват и анализират и могат да се използват за извличане на чувствителна информация.

Подслушване на мрежата се използва и с полезни цели – за наблюдаване, анализиране и откриване на проблеми в мрежите.

Троянски кон.

Троянски кон е програма, отваряща вратичка в сигурността на системата. Тя дава неоторизиран достъп на атакуващия компютър, намиращ се в интернет. Това обикновено е програма от две части – клиент и сървър. При стартиране на програмата сървър се отварят един или повече порта на заразения компютър. Троянският кон е изпълним файл от операционната система и заразяването винаги става чрез стартирането му от потребителя. Чрез клиентската програма злонамерен потребител може да получи отдалечен достъп до този компютър. Атакуващият може да вижда съдържанието на екрана, да стартира и спира приложения, да изтегля, изпраща и изтрива файлове, да форматира дискове, да спира или рестартира компютъра и т.н.

Съществуват програми троянски коне, които се представят като други програми. Това може да бъде например прозорец за логване в системата. При въвеждането от потребителя на

името и паролата данните се предават по мрежата и съответно този, който е стартирал програмата клиент от троянския кон може да получи достъп до системата.

Компютърни вируси и червеи.

Компютърният вирус е паразитна програма, която има способността да се самовъзпроизвежда и е създадена с цел да унищожи друга програма или файлове с данни. Компютърният вирус не е самостоятелна програма. Той се свързва с програма гостоприемник, като при нейното стартиране се стартира и вирусът. При това големината на заразения файл се увеличава.

Действието на вирусите може да бъде различно. Някои са по-безобидни – действието им се свежда до извеждане на съобщения на екрана на компютъра. Други са доста по-злонамерени – те могат да повреждат, променят и изтриват файлове от компютърната система, така че компютърът да не може да бъде стартиран.

Вирусите се класифицират по видове и към настоящия момент съществуват около 30 вида. Най-често срещаните от тях са:

- BOOT секторни – заразяват сектора за първоначално зареждане (boot record).
- BIOS – заразяват входно-изходната система на компютъра.
- Файлови – заразяват всички активни програмни файлове (*.COM, *.EXE, *.OVR, *.BIN, *.SYS).
- Стелт – те не променят размера на заразения файл. Секторите, които заразяват, се маркират като лоши, въпреки че не са повредени.
- Макровируси – заразяват файлове с документи, притежаващи макроси (*.DOC, *.DOT, *.RTF, *.XLS, *.XLT.
- Имейл вируси – особено актуална категория вируси. Разпространяват се чрез електронна поща и използват адресната книга, за да нападат нови компютри.
- Java вируси – могат да заразяват само java програми. Стартират се от java applet в браузъра или като самостоятелно java приложение.

Компютърният червей (computer worm) е самовъзпроизвеждаща се компютърна програма. Той използва компютърната мрежа, за да изпраща свои копия до компютрите. За разлика от компютърния вирус за него не е необходима програма гостоприемник.

Компютърният червей е самостоятелна програма. Червеите почти винаги причиняват вреда на мрежата, тъй като консумират от нейната пропускателна способност. Те се разпространяват, като използват пролуки в операционните системи. Някои от компютърните червеи се разпространяват на отделни части по мрежата. Първо пристига стартиращ модул (starter) – малка програма, изтегляща и реконструираща червея. При пристигането на всички части на червея се „сглобява“ компютърната програма, след което тя може да бъде стартирана. Преминаването само на малки фрагменти от информация през входно-изходната система не позволява на антивирусните програми да разпознаят червея.

Много червеи са полиморфни. При сглобяването програмните сегменти се разбъркват случайно. Това ги прави много трудни за откриване.

Вътрешни заплахи.

Въпреки немалкия брой външни заплахи за мрежовата сигурност не са за пренебрегване и заплахите вътре в локалната мрежа на организацията или фирмата. Вътрешните заплахи могат да класифицират в няколко групи.

Корпоративен шпионаж.

Това е най-интелигентният тип вътрешна заплаха за сигурността. Важна задача за всяка фирма е опазването на търговските тайни, свързани с бизнеса. Конкуренцията винаги се стреми да се сдобие с повече информация за другите фирми от този бизнес. Възможни са ситуации, когато се назначават на работа чужди служители в дадена фирма с цел получаване на достъп отвътре до фирмените тайни. Обикновено хората, които могат да осъществяват корпоративен шпионаж, са едни от най-интелигентните служители с големи професионални умения. Затова и разкриването на този вид шпионаж е доста трудна задача.

Вътрешни политики.

Заплаха за сигурността на данните в локална мрежа могат да бъдат и действията на някои от служителите във фирмата, които искат да саботират работата на отделни свои колеги. Техните мотиви могат да бъдат различни – откриване на възможности за повишаване в длъжност, увреждане репутацията на хора от екипа и др. Действията им не са насочени към сигурността на данните на компанията, но въпреки това могат да ѝ създадат множество проблеми. Извършителите на този вид престъпления обикновено не са висококвалифицирани специалисти, затова и по-лесно могат да бъдат предприети действия за тяхното предотвратяване или разкриване.

Недоволни служители.

Друг много сериозен вид заплаха за мрежовата сигурност могат да бъдат уволнени служители или такива, които не са доволни например от своето възнаграждение. Те обикновено предприемат действия, с които целят да навредят на компанията. Тъй като имат достъп до системата, могат да изтрият важни данни за фирмата, да прекъснат мрежовите комуникации и др. Съществуват редица случаи на уволнени служители, които преди да си тръгнат от фирмата, сменят паролите за достъп до системата или стартират програми, които отварят вратичка в нейната сигурност.

Политиката на мрежова сигурност трябва да има предвид и този вид заплаха, като действията могат да бъдат насочени към своевременно изтриване на потребителските акаунти на уволнените служители.

Случайни пробиви.

Случайни пробиви в системата могат да се получат от неопитни служители, които в стремежа си да извършат едно или друго действие на компютъра изтрият неволно важна фирмена информация. Операционните системи с файлова система NTFS позволяват да се задават нива на сигурност. По този начин мрежовият администратор може да ограничи действията на отделните групи потребители.

Дейности за осигуряване на защита.

Прегледът на видовете заплахи и направления за неоторизиран достъп показва, че за да се осигури необходимото ниво на киберзащита, са необходими задълбочен анализ на уязвимостите в системата и прилагане на адекватни мерки за минимизиране на възможностите за провеждане на атаки.

Мерки и действия за киберзащита.

Те съдържат набор от дейности и мерки, целящи защита от атака, разрушаване или други заплахи за компютрите, компютърните мрежи, свързаните с тях хардуерни и софтуерни устройства, както и информацията, която съдържат и предават, включително софтуер и данни, а също и други елементи на киберпространството. Дейностите могат да включват одит на сигурността, управление на версиите, автентификационни процедури, управление на достъпа, оценяване силните места и уязвимостите на хардуера и софтуера, използван в държавната и икономическата електронна инфраструктура на страната. Те обхващат също откриване и реагиране на заплахи за сигурността, намаляване на въздействието и възстановяване на засегнатите компоненти. Други мерки могат да включват хардуерни и софтуерни защитни стени, физическа сигурност, както и обучение на персонала.

Факторите, определящи осъществяването на киберзащитата, са три: човешки, технологични и законодателни.

Човешкият фактор има съществена роля за осигуряване киберсигурността на информационно-комуникационните системи. Той е зависим както от морално-етичните характеристики на отделния човек, така и от нивото на неговата подготовка. Човешкият фактор е пряко свързан с процеса на създаване на организация за опазване на чувствителна и конфиденциална информация. Достъпът до обработваните и съхраняваните данни и информация трябва да е съобразен с изискванията на Закона за защита на класифицираната информация, а именно да се спазва принципът „необходимост да се знае”.

Необходимо е да се предвидят и изпълняват мерки за архивиране и съхраняване на данните с цел тяхното бързо и надеждно възстановяване в случаи на кибератаки или след възникнали сривове, а също така следва да се алгоритмизират и документират процедурите за възстановяване.

Техническите и технологичните средства са свързани основно с хардуерната и софтуерната защита на информационните и комуникационните системи и могат да се обобщят по следния начин: средства за физическо осигуряване на компютърните системи срещу кражба, несанкциониран достъп и некоректно използване.

Средства за контрол на достъпа – защитни стени, пароли, използване на биометрични данни.

Средства за превенция/откриване на непозволени проникванията – системи за предотвратяване на проникване в мрежа (Network Intrusion Prevention Systems – NIPS) и системи за откриване на проникване в мрежа (Network Intrusion Detection Systems – NIDS).

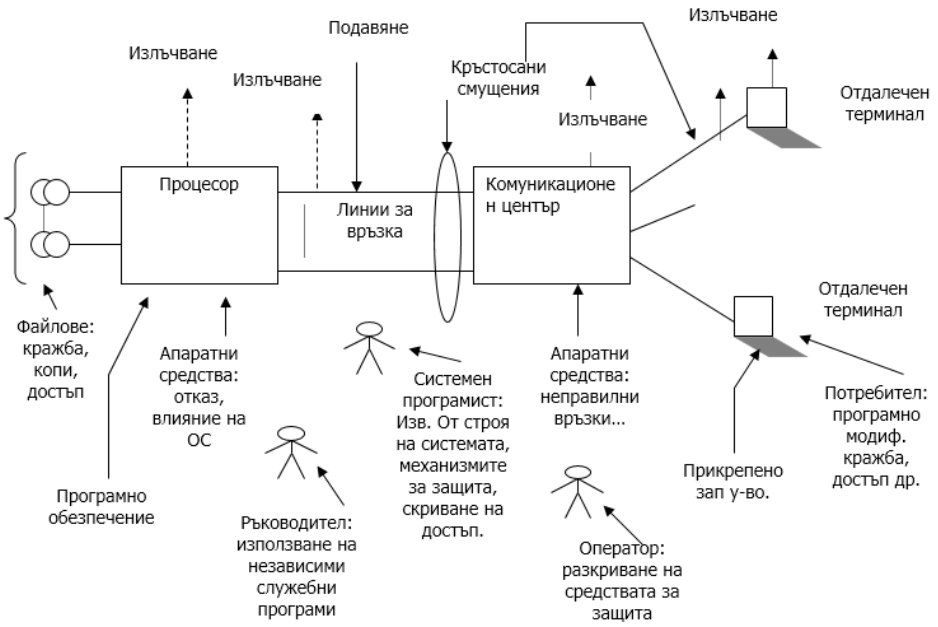
Средства за кодиране – системи за PKI и частни ключове.

Средства за автентификация – цифрови сертификати, маркери, електронни подписи.

Средства за защита от въздействие на електромагнитни смущения и импулси (EMI/RFI екраниране).

Средства за контрол на мрежата – използване на подходящ софтуер и хардуер (скенери, снифери, Profilers, Honeypots, Shunts).

Необходимо е да се съгласува съществуващото национално законодателство с това на водещи страни в света в частта си за наказателните мерки спрямо специалистите, които създават и разпространяват злонамерен софтуер с цел нанасяне на щети и опит за неправомерен достъп до данни и информация, а също така да се актуализира в съответствие с динамичната промяна на условията за сигурност (фиг. 6).



Фиг. 6. Обобщена схема на направленията за несанкциониран достъп

4. Подсистема за идентификация и автентификация [7]

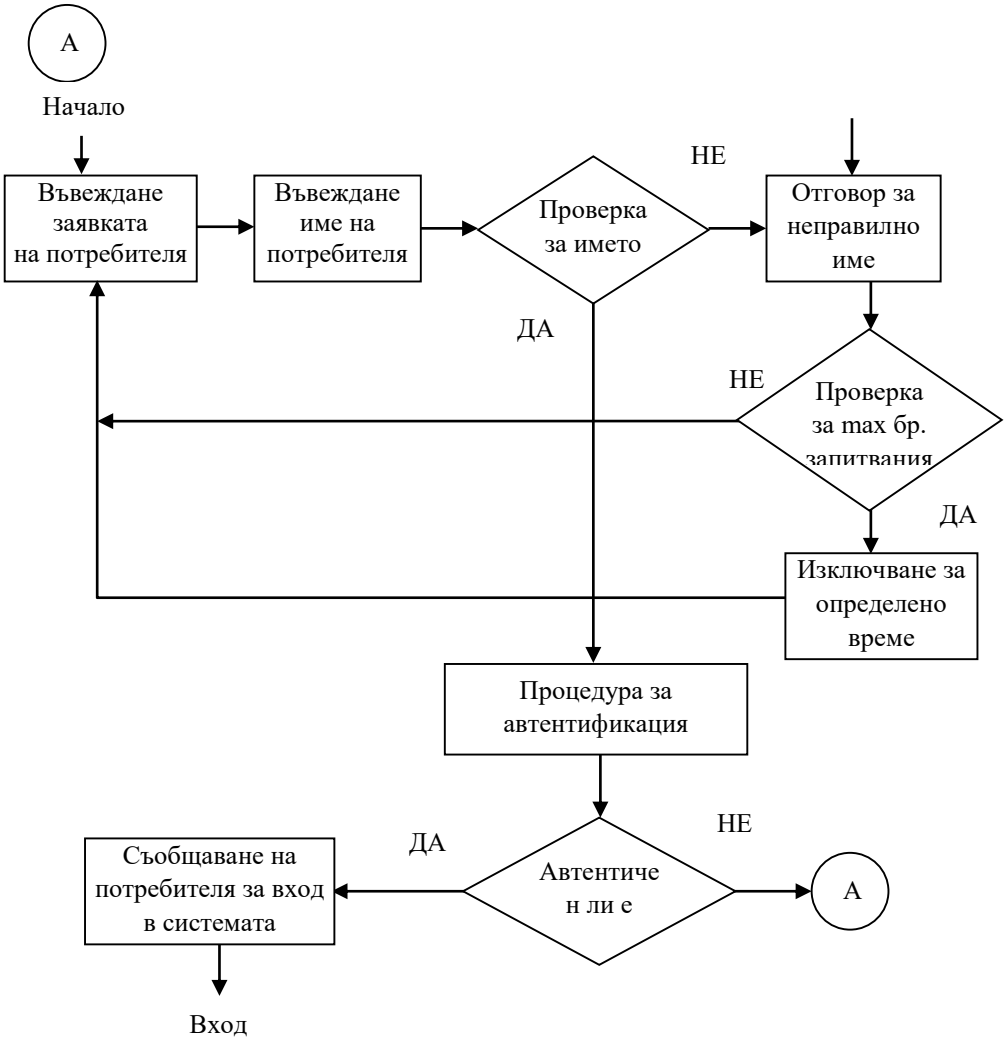
Методите за автентификация преди всичко трябва да се разглеждат като част от общото взаимодействие на идентификация, автентификация и предоставени права, които в съвкупност определят какъв достъп се предоставя до защитените ресурси. Идентификацията е присвояване уникално име или число на обекта, автентификацията се състои в проверка действителността на обекта, който се представя под определеното име, а предоставянето на права определят степента, до която даденият обект може да ползва защитените ресурси.

Идентификация и установяване на автентичност.

Идентификацията на потребител, устройство, файл, програма или друг обект представлява присвояване уникално име или число на обекта. Това е заявка за установяване на идентичност. В идентификаторите би следвало да се въведат контролни цифри с цел да се сведе до минимум грешката при идентифициране. Идентификацията е необходима не само за опознаване, но и за отчет на обръщенията. Нейното използване обаче е безсмислено без съчетаване с автентификация особено ако в системата трябва да се осигури определена безопасност.

Процедура за автентификация.

Автентификацията е процес на установяване идентичността между името на даден обект и самия обект. Тъй като е възможно да се извършат определени действия, преди да завърши автентификацията, е прието тя да се разглежда като процес. По принцип автентификация се прави само веднъж. Възможно е обаче в системи с висока степен на защита този процес да се повтаря периодично или при определени ситуации – срив, специални права и др. (фиг. 7).

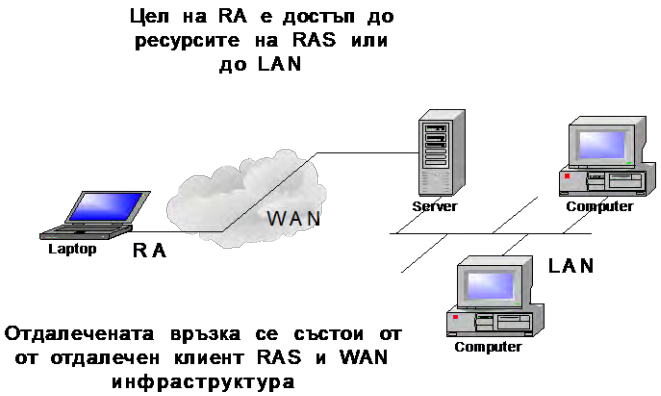


Фиг. 7. Типична процедура на автентификация

За установяване на автентификация потребителите в информационните мрежи използват пароли и други методи на диалог със системата. Ако потребителят е в състояние правилно да представи изискваната информация, системата го признава за автентичен. Използването на значително сложни методи и пароли не затруднява критично производителността в информационните системи. От потребителска гледна точка обаче сложните методи са неприложими в системи с много абонати. В този случай проектантът на системата за информационна сигурност трябва да намери компромисното решение между простото реализиране и изискването за безопасност.

Логика на стратегия за отдалечен достъп и настройка на потребителски акаунт.

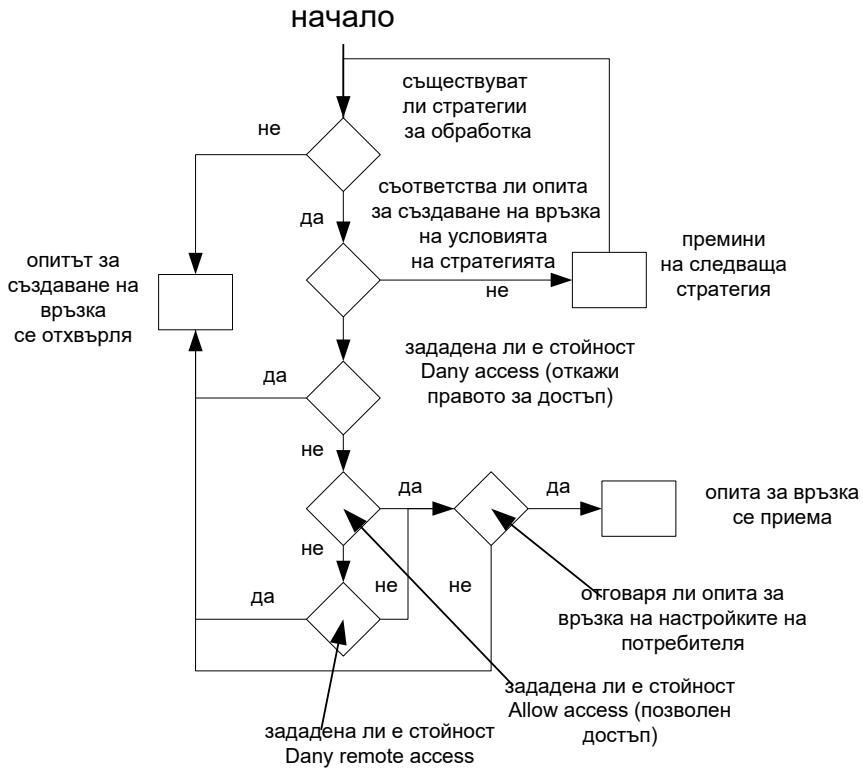
Направлението, съсредоточаващо в себе си най-висока степен на уязвимост спрямо несанкциониран достъп в информационните системи, е отдалеченият достъп (фиг. 8). То мултиплицира широка гама от заплахи, чиято неутрализация е изключително трудна поради териториални, времеви, административни и други фактори, съпътстващи тази услуга. Изискванията към защитата при такива обстоятелства включват еднозначно определяне на потребителя, неговите разрешения, информацията, която ще се обменя, и други свойства на политиката за сигурност. Поради тези условия типичната процедура по идентификация и автентификация не е в състояния да изпълни предявените изисквания. На практика се прилага цялостна стратегия, съпътстваща процеса от край до край, която включва шест последователни проверки, чиято основна функция е:



Фиг. 8. Инфраструктура на RAS

- Проверка за съществуване на политика, описваща отдалечена връзка – по подразбиране във всички информационни системи RAS услугата е забранена. Нейното разрешение е възможно само след изрично действие на администратора на системата. Много често забраната е част от идеологията на системата за защита.
- Проверка за съответствие на опита за създаване на връзка с условията на стратегията – търси се съответствие между заложения профил на потребителя в паметта на сървъра и профила, изпратен от самия потребител. При тази проверка се задейства и процедура по идентификация и автентификация.
- Проверка за отказ на достъп – обикновено това е брояч, който следи за крайния брой опити за свързване, след което процедурата се стартира от начало (при някакви условия, например време).
- Проверка за предоставяне на достъп – като при горния случай брояч следи за крайния брой опити за свързване, след което процедурата се стартира от начало (при някакви условия, различни от предната проверка).;
- Проверка за разрешение за отдалечен достъп – извършва се определяне на принадлежност към рестриктивен списък, който е част от общия списък на потребителите.
- Сравняване на всички резултати от предходните проверки с предварително заложените стойности – в част от системите такава проверка се съпровожда от аналитична обработка на данните с цел намаляване обема на съхранявана информация в log файловете.

Представената последователност (фиг. 9) в пълна степен гарантира удовлетворяване на изискванията, като дава възможност за гъвкаво администриране на услугата чрез вложената идентификация и автентификация на потребителите.



Източник. “Windows 2000 server” Microsoft Corporation.

Фиг. 9. Настройка на потребителски акаунт

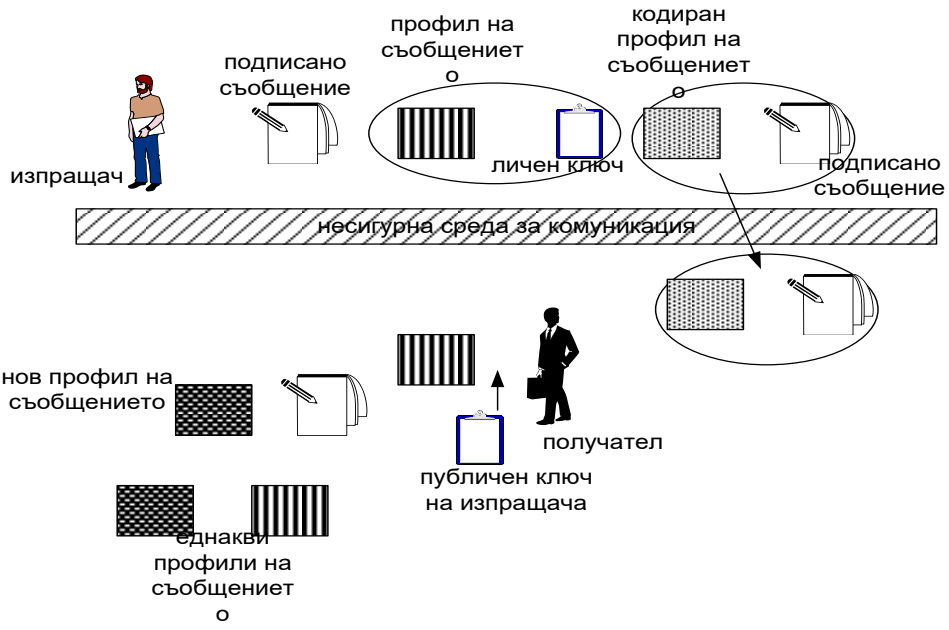
Система за идентификация и автентификация с публичен ключ.

Тази процедура за разлика от криптирането с публичен ключ няма за цел да скрие съобщението в хода на неговия пренос до получателя. Целта тук е чрез разгърната PKI инфраструктура еднозначно в публична среда да се установи източникът на съобщението и дали то е модифицирано в процеса на комуникация. Това се извършва по следната процедура:

1. Изпращащият подготвя електронния документ, като го подписва. Подписът може да бъде определен атрибут, който се присъединява към електронния документ. Това може да бъде например потребителското име на изпращащия в системата.
2. Задейства се алгоритъм за сваляне на т.нар. профил на съобщението. Това могат да бъдат уникалните свойства на електронния документ, генерирани от операционната система.
3. Изпращащият криптира с частния си ключ само профила на съобщението (профилът на съобщението включва атрибутите на документа с електронния подпис на автора на документа).
4. Криптираният профил се прикрепя към електронния документ и се изпраща на получателя.
5. Получателят прави едновременно две процедури: 1) сваля профила на получения документ и 2) декриптира получения профил с публичния ключ на изпращащия.

6. Сравнява генерирания профил на получения документ и декриптирания изпратен профил.

Ако двата профила съвпадат, получателят е сигурен, че документът е автентичен източник и в процеса на комуникация същият не е модифициран (фиг. 10).



Източник. “Windows 2000 server” Microsoft Corporation.

Фиг. 10. Система за идентификация и автентификация с публичен ключ и електронен подпис

Паролиране.

Методът на паролиране изисква от потребителя да въведе (от клавиатура или друго устройство) последователност от символи (парола) за проверка от системата. Ако паролата съответства на тази, съхранявана в паметта на ЕИМ за конкретния потребител, той може да ползва целия инфоресурс, до който има достъп.

Обикновена (проста) парола.

Методът е пределно опростен и дава възможност на потребителя сам да избере подходяща за него парола. Реализацията също не изисква специални ресурси. Този метод има редица недостатъци. От една страна, паролата не е необходимо да бъде записана и оттам възможността да попадне в странични лица, от друга страна обаче, по принцип това е лесна за запомняне последователност от символи – обикновено дума. Едно от компромисните решения е използването на генератор на случайни пароли, които лесно се запомнят. Друг вариант е вмъкването на интервали на определени места в паролата. В този случай дори при неволно попадане на листа, където е записана паролата, в странични лица това няма да им позволи автоматично да разкрият тайната.

Дължина на паролата.

Колкото е по-голяма дължината на паролата, толкова по-голяма е защитата, която тя осигурява, тъй като ще е необходимо по-голямо усилие да бъде разгадана. Това обстоятелство може да се представи с термина „очаквано време за разкриване на паролата“, което аналитично се определя от полупроизведението на общия брой възможни пароли и необходимото време за проба на всяка парола от общата последователност:

$$\frac{\left(A^S * \frac{R}{E}\right)}{2} = \text{време за разкриване [s]}, \quad (1)$$

където R е скоростта за предаване по линията за връзка;

E – броят символи във всяко предавано съобщение;

S – дължината на паролата;

A – броят символи, които участват в съставянето на паролите.

Пример: R = 600 симв./мин.; E = 20; S = 6; A = 26. Получаваме:

½*(26^6*2) = 30 891 578 с = 357 дни.

Ако след всеки неудачен опит системата включва 10 със задръжка, времето се увеличава 6 пъти.

В практиката се използва и аналитична формула на Андерсън, която с помощта на въведени изисквания за вероятност за разкриване на паролата (P) и периода от време, в който могат да се предприемат административни мерки за смяна на паролата (M), се определя нейната дължина:

$$4.32 * 10^4 \frac{RM}{EP} \le A^S . \quad (2)$$

При положение че за съставяне на паролите се използват стандартните азбуки, то основно влияние върху вероятността за разкриване оказва дължината ѝ. Например за горните данни при трисимволна парола са необходими 3 месеца, а при четирисимволна – 78 месеца.

Основен недостатък на системите с обикновени пароли е възможността да се ползва неправомерно придобита парола, без това да се санкционира от системата. Решенията на този проблем са много – честа смяна на пароли, определяне срока за ползване на парола и др.

Модификация на системата с обикновена парола.

Подбор на символи от паролата – моделът дава възможност на системата да предложи на потребителя да въведе само определени символи от паролата.

Пароли с еднократно действие – системата съдържа списък с пароли, които потребителят ползва последователно при всяко влизане в нея. Недостатъците на този метод са, че абонатът трябва да помни или да притежава целия списък от пароли, при грешки потребителят се оказва в затруднено положение и не на последно място, ако паролите се генерират от сървър, достъпът до него е критичен за системата.

Метод „въпрос – отговор“.

Основава се на замяна на паролирането с въвеждане на анкетен лист, на който потребителят трябва да отговори. Методът може да се модифицира чрез промяна на анкетата или пълнотата на отговорите.

Установяване на автентификация на системата.

Това по същество е подобна система, но с различно предназначение. Идеята е за автентификация на устройството, с което се извършва управление и настройка. Основният способ, използван за такива потребности, е апаратното автентифициране, т.е. заложените на микро програмно ниво средства за автентификация, чрез които системата автоматично разпознава устройството.

Основни мероприятия за защита при работа с пароли.

Паролите никога не трябва да се съхраняват в ЕИМ в явен вид.

Паролите не бива да се отпечатват при въвеждане.

Колкото е по-голям периодът на действие на дадена парола, толкова вероятността за нейното разкриване е по-голяма.

Системата никога не трябва да генерира нова парола в края на сеанса.

Физически методи за установяване на автентичност и действия при отказ на достъп.

Освен разгледаните чисто програмни средства съществуват и т.нар. физически методи за автентичност. Те проверяват някои от физическите характеристики на потребителя. В последно време масово приложение намират електронните карти за автентификация, изискващи и потребителски ключ за ползване.

Основният способ за действие при отказ от достъп до системата е методът на регистриране и задръжка. При този процес се цели:

- да се ограничи вероятността за пробив;
- да се регистрират нарушителят и видът на опита за достъп – получените данни са основни за анализ и адаптиране на системите за сигурност.

Идентификацията и автентификацията винаги се разглеждат като два неразривно свързани процеса. Във всяка система за сигурност те са основа на действащата политика. Значителна част от задачите в тази политика се решават чрез процедурите за идентификация и автентификация.

Съвременните технологии реализират огромно разнообразие от процедури, но нито една сама по себе си не е в състояние да изпълни високите изисквания към защитата на информацията.

5. Оценка на риска в системите за киберсигурност [8, 9, 10, 11]

Определение.

Количествената оценка на риска $\rho_{il} = \rho(V_i, \theta_l)$ се определя по формулата:

$$\rho_{il} = \rho(V_i, \theta_l) = \mu(V_s, \theta_l) - \mu(V_i, \theta_l) = \mu(\theta_l) - \mu(V_i, \theta_l), \quad (3)$$

където $\mu(V_S,\theta_l)$ е полезността, която би се получила, ако лицето, вземащо решение (ЛВР), знае реалното състояние на околната среда и на тази основа прави своя избор,

$\mu(V_i,\theta_l)$ – полезността, която се получава при реално избрана алтернатива за появилата се ситуация на околната среда.

Чрез понятието „риск“ ЛВР изразява своето субективно отношение към специфичната ситуация на задачата за вземане на решение (ЗВР). Методите за решаване на такъв тип задачи се различават основно по подходите за добиване на априорна информация за околната среда. В зависимост от специфичните особености на конкретната предметна област тази информация се добива чрез:

- провеждане на експеримент;
- многократен избор;
- статистика;
- използване на знания за предметната област.

Първите три подхода са крайно неподходящи за добиване на информация, тъй като те ще доведат до нецелесъобразен разход на човешки, времеви и материални ресурси. Това определя избора на метод за решение, който се ориентира само към вземане на решение без експеримент при еднократен избор, с използване на знания в конкретната предметна област.

Анализът на риска по същество представлява систематичен подход при определянето на заплахите и мерките за защита от тях. Основната цел е вземането на обосновано решение, в съответствие с което да се изгради системата за киберсигурност.

Процесът на анализ на риска е продължителен и включва преди всичко непосредствен диалог със заявителя на изискванията за сигурност. Този процес може да се реализира по различни методи, като допитване, конференции, анкети и др. (табл.1).

Форма, използвана при оценка на риска, е показана в таблица 1.

Таблица 1

Описание на риска	*Възможен ефект*	*Възможна стойност на риска (лв.)*	*Вероятност (0 – 1) P*	*Произведение P*ст.*	*Превантивни и възстановителни мерки*	*Стойност на защитата (лв.)*
1. Разрушено помещение на сървъра	1. Загуба на достъп до данните. 2. Преместване на помещението	500 000 200 000	0,25	120 000 50 000	1. Резерв. 2. Застраховка на помещението	3000 за година

Многобройните кибератаки, случващи се ежедневно в глобалната мрежа, както и нарастващият интерес към проблемите на безопасността принуждават голяма част от организациите да променят подхода си към сигурността. На първо място, отчита се фактът, че не е възможна пълна защита в условие на откритост на информационните процеси, съпровождащи отношенията с партньори, съдружници и клиенти. На второ място, все повече организации прилагат общоприети или стандартизирани препоръки за компенсиране на непредвидените загуби чрез определяне на риска, пред който те са изправени.

Заедно с това според проучване на PwC (PricewaterhouseCoopers) за 2017 г., в което са анкетирани повече от 9000 бизнес ръководители от цял свят, повече от една четвърт от тях не знаят на колко кибератаки са били подложени ръководените от тях организации, а една трета от тези, които имат представа за проявените кибератаки, не знаят как това се е случило. Друг

интересен факт е, че повече от половината кибератаки са причинени от общи пропуски на сигурността, които могат лесно да бъдат преодолени с добро управление. Във връзка с това една от важните стъпки, които всяка организация може да предприеме за подобряване на киберсигурността си, е да направи задълбочена оценка на риска от киберзаплахи. Този подход със сигурност ще ѝ позволи да преодолее високата степен на неопределеност от проява на такива заплахи и значително да редуцира възможните загуби от грешки в управлението.

В областите, в които се използва понятието „риск“, съществуват редица определения, някои от които не изискват точна връзка между вероятност и последствия. Други еднозначно определят риска чрез наличието на такава връзка. Всички определения обаче съдържат условие за пропорционалност между вероятност и последствията.

Определението, формулирано от Блез Паскал, е: Рискът трябва да бъде пропорционален на вероятността за неговото възникване, както и на степента на увреждане в резултат на проявата му. (Risk should be proportional to the probability of occurrence as well as to the extent of damage.).

В областта на киберсигурността се използва следното определение за понятието риск: Рискът (K) е „произведението от вероятността за проява на нежелано събитие (P) и количеството загуби (C) при неговата проява“.

$$K = PC. \tag{4}$$

В областта на теорията за вземане на решение рискът (K) се определя като „разлика между очаквания резултат (B_i) в момента на вземане на решение и получения резултат (B_{i+t}) след реализация на решението“.

$$K = B_i - B_{i+t}. \tag{5}$$

Определенията могат да се приемат за съпоставими, при условие че се определя резултатът от взетото решение като ефективност с размерност от 0 до 1.

Рискът е понятие, което често се използва за определяне субективно отношение на обект, организация или система към нежелани ефекти или загуби от събития с вероятностен характер. На практика това означава, че за една и съща ситуация различни субекти, организации или системи ще отчитат различни стойности на риска. Но за самата организация оценката трябва да се обосновава на научни и обективни методи. Това включва отчитането на множество вътрешни и външни за компанията фактори, включително отношенията с подизпълнители, доставчици, работната сила, както и динамиката на средата, в която системата функционира.

Краткият преглед на същността на риска от киберзаплаха за дадена организация показва, че за определянето му е необходимо да бъдат отчетени множество параметри – като случайни вероятностни величини и закона за разпределение на тези случайни величини. Такъв тип задача винаги се класифицира като задача с голяма сложност поради високата степен на неопределеност в процеса на верификация на резултата. Често пъти тя може да се решава само на основата на специфична интерпретация на данни или готови знания за конкретната предметна област.

В резултат на представената сложност повечето организации използват някоя от съществуващите методологии за оценка на киберриска под формата на рамки за оценка на риска, разработени през последните години. Едни от най-разпространените са рамките за оценка на риска NIST SP 800-53 Rev. 4 и ISO/IEC 27001:2013.

Създадената от Националния институт за стандарти и технологии на САЩ (National Institute of Standards and Technology – NIST) описателна рамка CSF (Cybersecurity Framework) се използва както от правителствени агенции, така и от бизнеса и образователни институции. Нейното приложение е индикатор за правилно управление на процесите, свързани с киберсигурността, от организацията.

Стандартизираната рамка се състои от три елемента – основа или ядро (Framework Core), нива на приложение (Framework Implementation Tiers), рамков профил (Framework Profile – Profile).

Основа или ядро.

Това е сбор от дейности в областта на киберсигурността. Тук съвкупно се разглеждат желаните резултати и приложените препоръки, които са общи за елементите на критичната инфраструктура, взаимодействието между дейности и резултати, свързани с киберсигурността в цялата организация – от ръководното ниво до нивото на изпълнение. Framework Core се състои от пет едновременни и непрекъснати функции – идентифициране, защита, Откриване, отговор, възстановяване. Всичките са обвързани с категории и подкатегории. Във функцията „идентифициране“ (identify) съществува подкатегория „определяне на риска“ (risk assessment) (фиг. 11).

Фиг. 11. Framework Core

Нива на приложение.

Тази част предоставя информация как организацията вижда риска за киберсигурността и процесите, които съществуват за управление на този риск. Нивата на приложение на процесите варират от:

- организации, частично информирани за риска (Partial – Tier 1);
- организации, информирани за риска (Risk Informed – Tier 2);
- организации, постоянно отчитащи риска (Repeatable – Tier 3);

- до организации, адаптиращи се към промените при отчитането на риска (Adaptive – Tier 4).

Рамков профил.

Представлява конкретното описание на функциите, категориите и подкатегориите за организацията. Профилът позволява на организацията да създаде моментна снимка на системата за киберсигурност. Чрез своя профил тя може да определи моментното си състояние и бъдещото си желано състояние и да свърже двата профила с пътна карта за постигането на своята цел. Профилът се препоръчва и при необходимост от взаимодействие между различни организации, които се стремят да изравнят своите профили за по-добра свързаност.

Методологията за определяне на риска от киберзаплахи се реализира от функцията „идентифициране“ (identify) и подкатегорията „определяне на риска“ (risk assessment - NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16). В тази подкатегория (Risk assessment - RA-3) единствено в три абзаца се определя какво се включва в оценяването на риска и как се измерва. Това са:

- Оценката на риска отчита вредата чрез определяне на вероятността от неоторизиран достъп или използване, разкриване, прекъсване, промяна и унищожаване на информационната система и информацията, която се обработва, съхранява или обменя.
- Оценката на риска отчита чрез определяне на вероятността заплахите, степента на уязвимост и външния, привнесен за организацията риск.
- Оценката на риска (формална или неформална) може да се извършва на трите нива в управлението на риска (т.е. на ниво организация, на ниво на мисия/бизнес процес или на ниво информационна система).

Друга широко използвана рамка за определяне на системата за киберсигурност е ISO/IEC 27001:2013. Серията ISO/IEC 27000 е съвместно публикувана от ISO и Международната електротехническа комисия (IEC). Подобно на NIST рамките на ISO са достатъчно гъвкави, за да отговарят на повечето организационни изисквания и структури. Те насърчават организациите да оценяват собствените си рискове за информационната сигурност и да прилагат контрол според потребностите си. Серията ISO също така подкрепя непрекъснат подход за обратна връзка и справяне с промените в средата от външни заплахи или заплахи в рамките на компанията и осъществява итеративни подобрения.

ISO/IEC 27001 официално определя задължителните изисквания за система за управление на информационната сигурност – СУИС (ISMS). Той използва стандарт ISO/IEC 27002, за да посочи подходящ контрол за сигурност на информацията в системата за управление на безопасността, но тъй като ISO/IEC 27002 на практика е кодекс (насока), а не стандарт за сертифициране, организациите са свободни да избират и прилагат други контроли, както и допълнителни контроли за сигурност на информацията, които смятат за подходящи. ISO/IEC 27001 включва обобщение на контролите от стандарт ISO/IEC 27002 в приложение А. Реално повечето организации, които приемат ISO/IEC 27001, също приемат и ISO/IEC 27002.

Оценката на риска за киберсигурността в този стандарт се разглежда в раздела ISO/IEC 27001:2013 A.12.6.1.

Само в два параграфа – 6.1.2, буква c и 6.1.2, буква d, се определя какво се включва в оценката на риска и с какво се измерва. Това е: Оценките на риска да се извършват с реалистична вероятност от възникване на загуба на поверителност, цялостност и наличие на информация в обхвата на информационната система.

Очевидно е, че и в най-широко използваните рамки за описание на системите за киберсигурност не се детайлизира методологията за определяне на случайните вероятностни величини, участващи при формулирането на риска. И двете рамки обаче използват за основа за определяне на средата общи фактори, като загуби, възникнали от заплахи, уязвимост, външен, привнесен за организацията риск, поверителност, цялостност и наличие на информация.

И в двете рамки оценката на риска се съпровожда с достатъчно широк анализ на средата, където еднозначно трябва да бъдат определени съществуващите заплахи (външни и вътрешни) и тяхната обвързаност с уязвимостите (отнесени към поверителност, цялостност и наличие на информация) на информационната система, след което се определя възможната загуба от проява на определена заплаха (и). Очевидно е взаимодействието на две вероятностни величини – заплахи и уязвимости, а резултатът от това взаимодействие може да се определи като стойност на риска.

6. Моделиране на системи за киберсигурност [7, 12]

Моделирането е една от главните съставни части в апарата на системотехниката.

Моделът е система, притежаваща идентични свойства с оригинала. Всяка човешка дейност започва с моделиране – представа за ситуацията, представа за целите и способите за действие. Берталанфи („Обща теория на системите“) изказва мисълта, че „всяка наука в широк смисъл е модел на понятийна структура, чиято цел е да отрази определени аспекти от реалността“.

Моделът е предназначен за интелектуално или апаратно експериментиране с цел разпознаване свойствата на реална система, възможните способи за нейното прилагане или преобразуване за получаване на нови възможности.

Моделиране – общи положения.

Математическото моделиране се използва като основен метод в управленския процес, когато трябва да се съобразяват материалните и времевите разходи.

Пълното описание на модел може да се представи с израза:

$$m = \mu * M_0, \tag{6}$$

където m е матрицата на параметрите на модела;

μ – матрицата на мащабни коефициенти;

M_0 – матрицата на параметрите на оригинала.

Тази форма на описание на модела много рядко би се използвала. Тя противоречи на компромисното съчетание между практическо изпълнение и моделиране, тъй като описва цялостен модел на системата. На практика би следвало да се използва непълното моделиране, където моделът е функция от оригинала – т.е.:

$$m = \mu * M: \tag{7}$$

$$M = \rho\left(M_0, x, t\right), \tag{8}$$

където ρ е функцията от параметрите на оригинала;

x – пространствените координати;

t – времето.

При решаването на конкретни задачи обаче с цел избягване на прекалено голяма сложност, без това да влияе върху качеството, могат да се елиминират част от параметрите, които се смятат за маловажни. Тогава описанието става с т.нар. приближен модел:

$$m = \mu^* M: \tag{9}$$

$$M = \text{sub}M_0, \tag{10}$$

където subM_0 е субматрицата от параметрите на оригинала, включени в модела.

При такъв вид моделиране е възможно значително увеличаване на грешката при отклонение на параметрите на модела от параметрите на системата, особено в случаите на условности и субективизъм при определянето на функционалните зависимости и важността на параметрите. Този проблем може да се избегне посредством определянето на норма, представляваща допустимата грешка при моделирането, т.е.:

$$\Phi(M) - \Phi(M_0) \le \varepsilon, \tag{11}$$

където Φ е оценъчната функция;

ε – нормираната (допустимата) грешка.

Представените най-общи теоретични постановки в областта на моделирането са изцяло приложими при проектирането и вземането на решение за сложни системи, каквато е системата за киберсигурност, само в случаите, когато:

1. Съществува пълен модел за системата.

2. Налице са знания, въз основа на които могат да се определят функционалните зависимости.

3. Съставянето на субматрицата и определянето на допустимата грешка при моделирането става въз основа на определен регламент или в непосредствено взаимодействие с поръчителя на системата.

Моделирането в системотехниката винаги се ръководи от поставената цел за постигане при детайлизация. В зависимост от тази цел последователно се преминава през изграждането на функционален, информационен и морфологичен модел.

Моделиране на системи за киберсигурност.

В редица литературни източници представянето на отделна компютърна система със специализирано програмно осигуряване като средство за наблюдение и управление на безопасността на цялата информационна система се разглежда като сървърна система по безопасността (фиг. 12).

Фиг. 12. Области на модела на система за киберсигурност

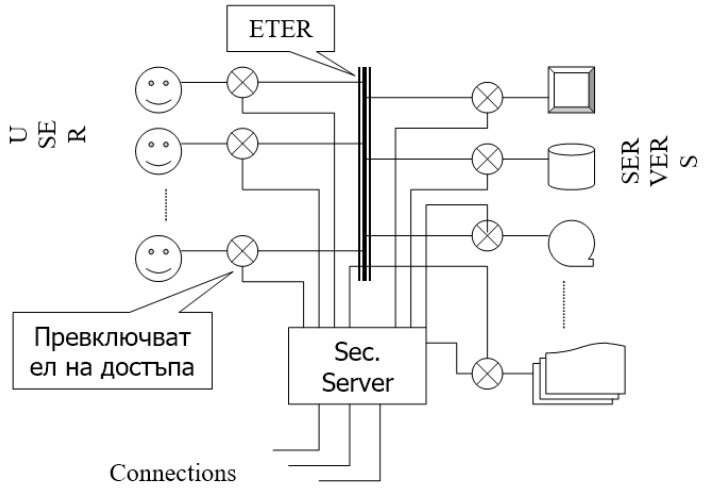
Основен проблем при проектирането на системи за киберсигурност се явява разкриването на направления за несанкциониран достъп в конкретната бъдеща среда, в която те ще функционират. Масово използваният способ в инженерната практика е аналитичното моделиране на системата и обкръжаващата я среда, чрез който лесно може да се подложи на анализ и оценка проектираната система. Съществуват редица модели за описание на системи за киберсигурност. Един от често използваните и сравнително лесно приложим е последователното моделиране на системата чрез изграждане на цялостна архитектура. Спазвайки логиката на архитектурния подход, последователно се разработват три модела – графичен, логически, аналитичен.

Графичен модел.

Предназначението на модела е чрез графика да представи основните елементи в системата за киберсигурност и тяхната свързаност (преди всичко физическа). Негови задължителни атрибути са:

- потребители;
- услуги;
- инфраструктура;
- преносна среда;
- външна свързаност;
- превключватели на достъпа;
- контролер на сигурността.

Примерен вид на такъв модел е показан на фигура 13.



Фиг. 13. Графичен модел на системата за киберсигурност

Чрез графичното представяне се цели бърз, лесен и точен структурен анализ, което позволява оценяването и определянето на т.нар. елементи от критичната инфраструктура. Такива модели служат за основа на следващата стъпка в моделирането, а именно изграждането на логически модел на системата за киберсигурност.

Логически модел.

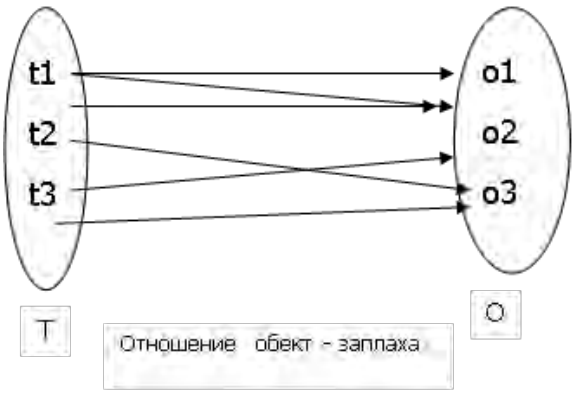
Моделът позволява изследване на функционалността на системата. Посредством него могат да се определят взаимовръзките и логиката на взаимодействие между различните елементи (обекти), представени с графичния модел.

Един от най-използваните подходи е изграждането на логически модел на система за киберсигурност с пълно прикритие.

Моделът се създава на два етапа и се състои от формирането на множества и определянето на тяхното логическо взаимодействие.

В първия етап се построяват множеството от заплахи и множеството от обект, подложени на тези заплахи. Отделните елементи на множествата се описват възможно най-подробно с цел използване свойствата на описаните елементи за постигане необходимата точност на модела.

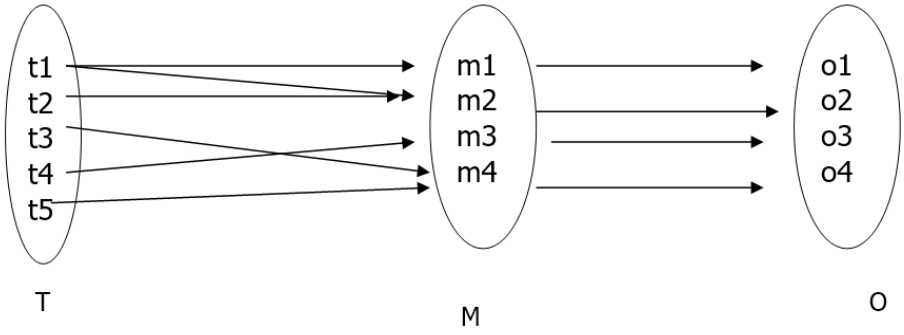
След формирането на двете множества елементите им се свързват чрез графи (или вектор) с прилежащите им атрибути (вероятност, време, честота, сила и др.). Формата на модела на този етап е показана на фигура 14.



Фиг. 14. Първи етап от създаването на модел с пълно прикритие

Множеството на отношенията обект – заплаха образува двуточков граф, в който реброто <ti, oj> съществува тогава и само тогава, когато ti се явява средство за получаване на достъп до обект oj. Трябва да се посочи, че връзката между заплаха и обект невинаги е от типа „едно към едно“. При представения модел целта на защитата е пред всяко ребро на графа да се постави бариера за достъп по този път.

Следващата стъпка в изграждането на модела е създаване на множество от средства за защита (M), предназначени да предпазват конкретните обекти от конкретните заплахи. Това множество се вгражда между съществуващите вече две множества – на заплахите и на защитаваните обекти. Важно е да се подчертае, че системата от въздействия на заплахите под формата на насочени графи се приобщава към заплахите и средствата за защита, при което се запазват формата, свързаността и характеристиките им. Формата на крайния вариант на модела с пълно прикритие е показан на фигура 15.



Отношение заплаха - защита - обект

Модел с пълно прикритие на СЗИ.

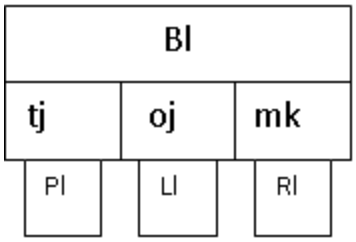
Фиг. 15. Модел на система за киберсигурност с пълно прикритие

Характерно за моделите с пълно прикритие е, че се разглеждат като идеални системи и затова са често използван инструмент при поставяне на изходни условия за оценка на риска.

Аналитичен модел.

В основата на аналитичното моделиране на системи за киберсигурност стои представянето на взаимовръзката между:

- Pl – вероятността за поява на определена заплаха,
- Ll – големината за загубата при проникване в системата,
- Rl – степента на съпротивление на елемента за защита чрез променливата Bl (фиг. 16).



Фиг. 16. Описание на променливата Bl

Друг вид аналитични модели са възможностите някои от процесите да се представят изразно. Такива са например аналитичните изрази за описване функционирането на СМО или времето за разбиване на парола (криптоключ).

Колкото по-голяма е дължината на паролата, толкова по-голяма е защитата, която тя осигурява, тъй като ще е необходимо по-голямо усилие да бъде разгадана. Това обстоятелство може да се представи с термина „очаквано време за разкриване на паролата“, което аналитично се определя от полупроизведението на общия брой възможни пароли и времето, необходимо за проба на всяка парола от общата последователност.

7. Supervisory Control and Data Acquisition – SCADA [13, 14]

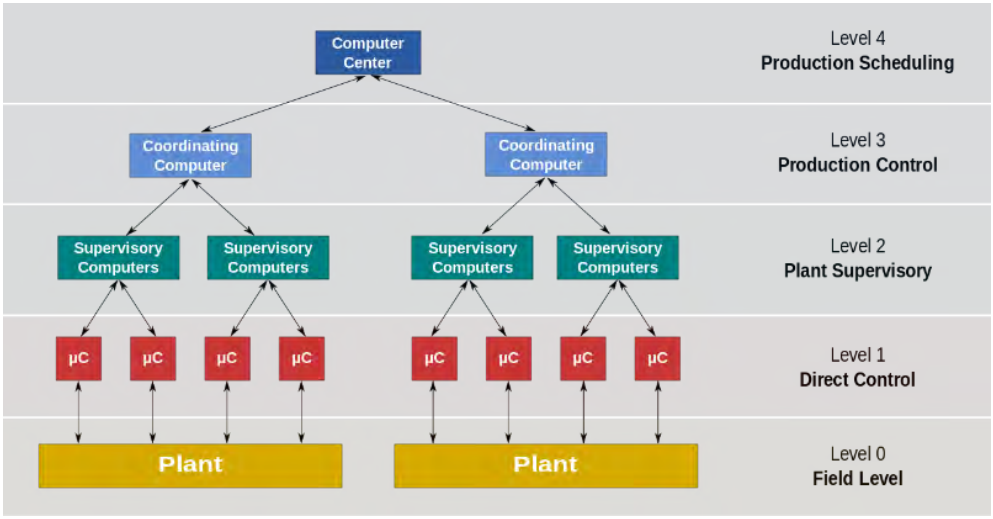
SCADA системите представляват съвкупност от програмни и апаратни средства, които позволяват локално или отдалечено управление на параметрите на автоматизирани технологични процеси в редица промишлени отрасли.

Основна функция на тези решения е програмното осигуряване на системите за автоматизация в процесните индустрии. Съвременните SCADA платформи предоставят също комплексен мониторинг, събиране и обработка на данни в реално време, както и запис на събития под формата на логове.

Структура, функции и приложения.

Базовата йерархична структура на SCADA системите включва четири отделни нива с ясно разпределени функции (фиг. 17):

- полево оборудване;
- програмируеми логически контролери (PLC) и/ли отдалечени терминални възли (Remote Terminal Units – RTUs);
- комуникационна мрежа;
- SCADA софтуер.



Източник.
https://en.wikipedia.org/wiki/SCADA#/media/File:Functional_levels_of_a_Distributed_Control_System.svg

Фиг. 17. Архитектура на SCADA система

На SCADA платформи е базирано управлението на технологични процеси в голяма част от предприятията в сферата на електроснабдяването и енергетиката, газо- и нефтодобива, ВиК сектора, хранително-вкусовата и химическата промишленост, транспорта, телекомуникациите, рециклиращата индустрия и др.

Особености на съвременните SCADA платформи.

Съвременните SCADA системи правят възможен достъпа до данни за работата на процесните съоръжения в реално време от всяка точка на света. Тези модерни платформи разполагат с възможности за бърз развой на приложения, което позволява на потребителите лесно да проектират и разработват различни приложни програми дори без задълбочени познания в областта на софтуерния дизайн.

SCADA системите, които обединяват децентрализирани съоръжения, като мощност, нефт, газопроводи, системи за водоснабдяване и събиране на отпадъчни води, са проектирани да бъдат отворени, здрави и лесни за експлоатация и ремонт, но не задължително сигурни. Преминаването от собствени технологии към стандартизирани и отворени решения заедно с увеличения брой връзки между SCADA системи, офис мрежи и интернет ги направи по-уязвими към типовете мрежови атаки, които са относително чести в компютърната сигурност. По-специално изследователите по въпросите на сигурността са обезпокоени от:

- липсата на загриженост относно сигурността и автентичността при проектирането, внедряването и работата на някои съществуващи SCADA мрежи;
- убеждението, че SCADA системите специализирани протоколи и собствени интерфейси;
- убеждението, че SCADA мрежите са защитени, защото са физически обезопасени;
- убеждението, че SCADA мрежите са защитени, защото са прекъснати от интернет.

Сигурността на тези SCADA системи е важна, защото компромисът или разрушаването им биха засегнали редица области на обществото далеч от първоначалния компромис.

Съществуват много вектори на заплаха за модерна SCADA система. Един от тях е заплахата от неоторизиран достъп до софтуера за управление независимо дали става въпрос за достъп на хора, или за промени, предизвикани умишлено или случайно от вируси и други софтуерни заплахи, които се намират на контролната машина. Друг е заплахата от достъп до пакети към мрежовите сегменти, хостващи SCADA устройства. В много случаи протоколът за контрол няма никаква форма на криптографска сигурност, което позволява на атакуващия да контролира SCADA устройство, като изпраща команди през мрежа. Не са малко случаите, когато потребителите на SCADA предполагат, че разполагането на VPN предлага достатъчна защита, без да е известно, че сигурността може да бъде тривиално заобиколена с физически достъп до мрежови жакове и комутатори, свързани със SCADA. Индустриалните контролери предлагат подход към сигурността на SCADA като информационна сигурност със стратегия за защита в дълбочина, която използва обичайните ИТ практики.

През април 2008 г. специална комисия прави оценка на заплахата за Съединените американски щати от електромагнитна импулсна атака (EMP). Комисията публикува доклад за критичните инфраструктури, в който се обсъжда изключителната уязвимост на SCADA системите от събитие с електромагнитни импулси (ЕМП). След тестването и анализа комисията заключава: „Системите SCADA са уязвими от електромагнитни импулси.

8. Изисквания за електромагнитна защита от излъчвания – (Transient Electromagnetic Pulse Emanation Standard – TEMPEST) [15, 16]

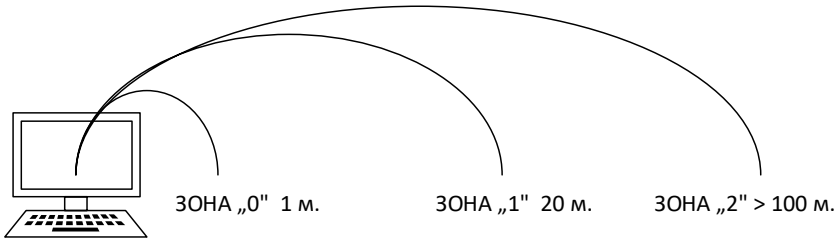
ТЕМПЕСТ е наименование на закрит военен проект на правителството на САЩ от края на 60-те години на XX век, чиято цел е проучване на възможността (както за умишлено използване, така и за формиране на защитни механизми срещу такова използване) в резултат на нежелани електромагнитни излъчвания (ЕМИ) от компютърни и телекомуникационни устройства да се възстанови информацията, съхранявана или обменяна в тези устройства. На по-късен етап ТЕМПЕСТ се превръща в абревиатура за телекомуникационна електроника, защитена от „паразитни“ електромагнитни излъчвания.

Днес във военната област се използва терминът EMSEC (за защита от емисии), а в гражданската област се е съхранило понятието ТЕМПЕСТ.

НАТО използва ТЕМПЕСТ като стандарт, който включва описание на изисквания, обединяващи двойна цел:

- изисквания, защитаващи електронните устройства от вторични ЕМИ, които могат да доведат до компрометиране на информацията в тях;
- изисквания, които могат да позволят чрез прихващане на вторични ЕМИ от електронните устройства да се възстанови защитавана информация в тези устройства.

Стандартът се препоръчва да се прилага за устройства, които функционират в уязвима или враждебна среда, като по този начин се гарантира (в съответствие с нормите на стандарта) високо ниво на защита срещу компрометиране на информацията от вторично електромагнитно излъчване.



Фиг. 18. Зони на приложение на стандарта TEMPEST

Към стандарта ТЕМПЕСТ НАТО дефинира три нива (степени) на прилагане – A, B и C.

Ниво A (Level A – NATO SDIP-27).

ТЕМПЕСТ стандартът на НАТО ниво А е най-стриктният като изисквания. Много често той се нарича и Full. Изискванията на ниво А се прилагат към области или устройства, където е възможно непосредствено да се прихванат ЕМИ (например през съседно помещение) или в среда, която не може да се контролира. Стандартът се прилага за устройства, функциониращи в зона 0 до 1 м.

Ниво B (Level B – NATO SDIP-27).

ТЕМПЕСТ стандартът на НАТО ниво В е следващият по стриктност като изисквания. Много често той се нарича и Immediate. Изискванията на ниво В обикновено се прилагат към области или устройства, където е невъзможно непосредствено да се прихванат ЕМИ (например до 20 м от устройството) или в среда, която може да се контролира в периметъра на зона 1 до 20 м. Като правило това са свободните пространства между сгради и препятствия, които не могат да се преодолеят.

Ниво C (Level C – NATO SDIP-27).

ТЕМПЕСТ стандартът на НАТО ниво С е с най-ниски по стриктност изисквания. Много често той се нарича и Tactical. Изискванията на ниво С обикновено се прилагат към области или устройства, където е невъзможно непосредствено да се прихванат ЕМИ и между елементите съществува т.нар. свободна зона (например над 100 м от устройството) или в среда, която може да се контролира в периметъра на зона 2 до 100 м. Като правило (над 100 м) това са свободните пространства между области (ПУ, КИВ, центрове и други инфраструктурни елементи) (фиг. 18).

За въоръжените сили придобиването на системи и оборудване в съответствие със стандарта ТЕМПЕСТ е една от критичните стъпки в реализацията на решения, позволяващи воденето на мрежово-центрични операции. По отношение на бизнес средите стандартът дава възможност за по-сигурно реализиране на бизнес процесите в условията на модерно информационно общество.

Предпазване на информационните системи от компрометиране в резултат на електромагнитни излъчвания.

Всички електрически устройства излъчват в някаква степен нежелани (вторични) електромагнитни сигнали (фиг. 19). EMSEC включва дейности и оборудване, необходими за анализ и определяне на риска от компрометиране на информацията, ако такива сигнали се прихванат умишлено от специални устройства или непреднамерено от прослушване

(кръстосване) или прехвърляне на сигнали между некомутирани устройства. Ако тези сигнали съдържат чувствителна информация, която може да бъде интерпретирана от неоторизирани потребители, това би било пагубно за всяка организация и нейната система за сигурност. Източниците на такива сигнали се дефинират като уязвими места в комуникационно-информационната система.

Фиг. 19. Електромагнитни излъчвания от различни устройства

В началото на 70-те години на XX век технологиите и методите за защита на КИС от ЕМИ мигрират от военната област към гражданските системи. Повече от 30 години обаче посоката е обърната и днес е налице взаимна интеграция и взаимно влияние на двете области по отношение на защитата от електромагнитни излъчвания.

Различават се два вида уязвими източници, породени от ЕМИ:

- информационни – информацията, която носят електромагнитните излъчвания;
- физически – електрическите компоненти, които генерират електромагнитни излъчвания.

Форми на електромагнитни излъчвания.

Радиовълни.

Радиовълните са електромагнитни вълни (ЕМВ) с дължина на вълната (λ) от 100 км до 0,1 мм. Използват се за предаване на информация (говор, данни, видео). Създават се около проводник, в който протича променлив ток с висока честота, и се излъчват чрез предавателна антена. Характерът на разпространението им в земната атмосфера зависи от дължината им. Попаднали върху приемна антена, индуцират в нея сигнали подобни на тези, които са генерирани от източника им.

Основна характеристика на радиовълните е способността им да се разпространяват във всички посоки през електрически непроводима среда, както и силната зависимост на енергийните им характеристики от разстоянието.

Трябва да се има в предвид, че радиовълните основно се излъчват преднамерено.

Кръстосани смущения.

Това са сигнали, прехвърляни обикновено чрез индукция от източник на ЕМИ към друга среда, изпълняваща функцията на приемна антена. Това винаги е непреднамерено и влияе на КИС в два аспекта.

Възможност за неоторизиран достъп до критична информация.

Взаимни вътрешносистемни смущения, водещи до влошаване качеството на услугите.

Електромагнитни излъчвания ЕМИ, генерирани от клавиатура. Създават се при предаването на информация, въвеждана от клавиатура и пренасяна към персонален компютър (PC).

Електромагнитни излъчвания, генерирани от видео. Създават се при предаването на информацията от PC и изобразяването ѝ на специализиран терминал (монитор, екран и др.). Като източници на ЕМИ могат да се определят два елемента:

- комуникационната връзка между PC и терминала;
- самият терминал.

Електромагнитни излъчвания, генерирани от инфраструктура:

- телефонни и силови линии;
- тръбна инфраструктура;
- метални структурни елементи.

Свързването на метални линии за пренос на информация обикновено е за честота под 30 MXц. Това е КВ диапазон, характеризиращ се със значителна дифракционна способност и голяма далечина на разпространение.

Електромагнитни излъчвания, генерирани от контактни повърхности. При механично-конструктивните контакти (познатите свързващи елементи, както силови, така и сигнални) се получава частичен преход на ЕМЕ да се изпише съкращението между двата свързващи елемента под форма на искри (включително миниатюрни). Това всъщност са ЕМВ, които генерират нежелани електромагнитни импулси. За разлика от инфраструктурните елементи тези ЕМИ са в диапазона, по-голям от 30 MXц, което позволява директно приемане от всеки радиоелемент, както специализиран за прихващане, така и системен, който внася смущения.

Основни методи, прилагани за EMSEC.

Повечето от нежеланите ЕМИ в системите са резултат от несъвършенствата на използваната технология за производство. Поради тази причина значителна част от направленията за намаляване на ЕМИ е повишаване качеството на техническото оборудване. В настоящия момент се прилагат три основни начина за контрол и намаляване на електромагнитните излъчвания.

1. Използване на специално оборудване, предотвратяващо ЕМИ. Специалното оборудване в стандарта ТЕМПЕСТ се класифицира в три групи:

- Клас 1 (U1) – оборудване без налично ЕМИ.
- Клас 2 (U2) – оборудване с ограничено ЕМИ.
- Клас 3 (U3) – оборудване с налично ЕМИ и реален риск от това (фиг. 20).

Източник. http://sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf

Фиг. 20. Оборудване, съответстващо на стандарта ТЕМПЕСТ

2. Изграждане на специална среда с ниско ниво на електромагнитни излъчвания. Това е техниката, свързана с екраниране на кабели, помещения, стаи, стени и конструктивни елементи, чието предназначение е да се изолира вътрешната електромагнитна среда от външната среда. Стандартът ТЕМПЕСТ различава два класа на защита на ЕМИ:

- Клас 1 (SS1) – прилагат се методи, елиминиращи възможността от ЕМИ.
- Клас 2 (SS2) – прилагат се методи, ограничаващи възможността за ЕМИ (фиг. 21).

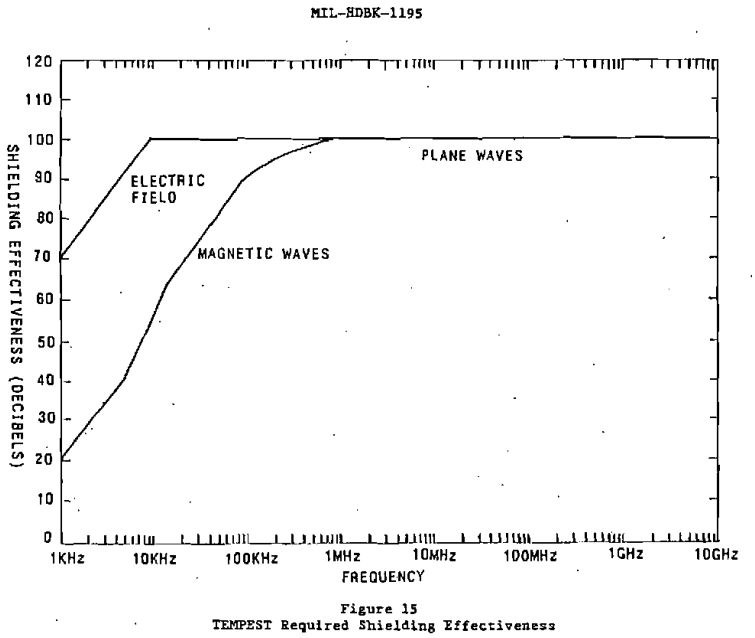
Източник. http://sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf

Фиг. 21. Специална среда с ниско ниво на ЕМИ

3. Използване на разстоянието като защита. Основава се на факта, че с увеличаване на разстоянието от източника на ЕМИ силата на сигнала намаля експоненциално. Това дава възможност чрез подходящо разполагане на критичното оборудване да се предотврати рискът от наличието на нежелано вторично ЕМИ. Стандартът препоръчва някои основни правила:

- Чувствителното оборудване трябва да бъде във вътрешната част на сградата.
- Чувствителното оборудване трябва да бъде по възможност на земята, близо до стени.
- Чувствителното оборудване не трябва да бъде близо до прозорци.

Електромагнитните излъчвания отдавна са сериозна заплаха за ИТ сигурността. Доскоро само развитите икономически страни имат възможност да манипулират и действат в електромагнитна среда. Тъй като технологията е станала по-евтина и по-достъпна, е разумно да се приеме, че включително и търговски организации могат да се занимават с разузнаване и че техните цели могат да бъдат и граждански. Съществуват примери за търговски фирми, които предприемат стъпки, за да се предпазят от нежелани ЕМИ (фиг. 22). На тази фигура е показана диаграма на стандарта ТЕМПЕСТ.



Източник. https://en.wikipedia.org/wiki/Tempest_(codename)#/media/File:TEMPEST_Shielding_Requirements.png

Фиг. 22. Диаграма на представяне на стандарта ТЕМПЕСТ

Таблица 2

Съответствия между стандарти за електромагнитни излъчвания

Descriptive	**Full**	**Intermediate**	**Tactical**
SDIP-27 ***NATO Standard***	Level A	Level B	Level C
previous NATO Laboratory test Standards	AMSG-720B	AMSG-788A	AMSG-784
NATO Zoning Standards	ZONE 0	ZONE 1	ZONE 2
USA NSTISSAM /1-92 Standards	LEVEL I	LEVEL II	LEVEL III
SST Example Products	SC1000TF SC8200TF SN9200TF	SN230TIR SC8200TI SS8270TI	SN790TTR SC8338TTRM SP280TTR

Източник. http://sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf

9. Изграждане на криптосистеми [17, 18]

В практиката са се наложили три основни способа за удовлетворяване потребностите за защита на информацията.

1. Физическа защита – насочена към защита на материалния носител на информацията (хартия, лента, електронно устройство и др., но не и на сигнала) чрез система за контрол и предпазване на носителя – не на информацията, от неоторизиран достъп.

2. Стеганографска защита – насочена към скриване факта на съществуване и предаване на информация (основният метод е маскиране).

3. Защита на информацията чрез криптиране – подмяна на защитаваната информация по специфичен начин и последващото ѝ възстановяване по обратен ред.

Най-масово използваният способ е криптирането. Много често се изграждат системи чрез комбиниране на посочените способи, с което се цели висока степен на защита, но в крайна сметка всяко конкретно решение е въпрос на анализ и точен инженерен разчет на потребности, ресурси и възможности.

Определения.

Криптография – част от приложната математика (криптология), изучаваща модели, методи и алгоритми, програмни и апаратни средства за преобразуване на информацията с цел скриване на нейното съдържание, модифициране или предпазване от неоторизиран достъп.

Криптоанализ – противоположната дейност на криптографията, целяща посредством анализ на криптосистемата да се извлече открита информация.

Шифър – съвкупност от обратими криптографски преобразования между множество открита информация и множество скрита информация чрез множество ключове и преобразуващ алгоритъм.

Криптосистема – съвкупността от преобразуващия алгоритъм и системата за управление на ключове.

Обща класификация.

В съществуващите информационни източници могат да се открият класификации по различни характеристики на криптосистемите, предлагащи детайлизация в определянето на всяка система поотделно. Всички те обаче се основават на една обща класификация, наложила се във времето, където критериите за класифициране са методът на криптиране, конструкцията на алгоритъма за криптиране и преобразованията в алгоритъма за криптиране.

Според метода на криптиране системите се делят на системи със симетрично криптиране (едноключови) и системи с асиметрично криптиране.

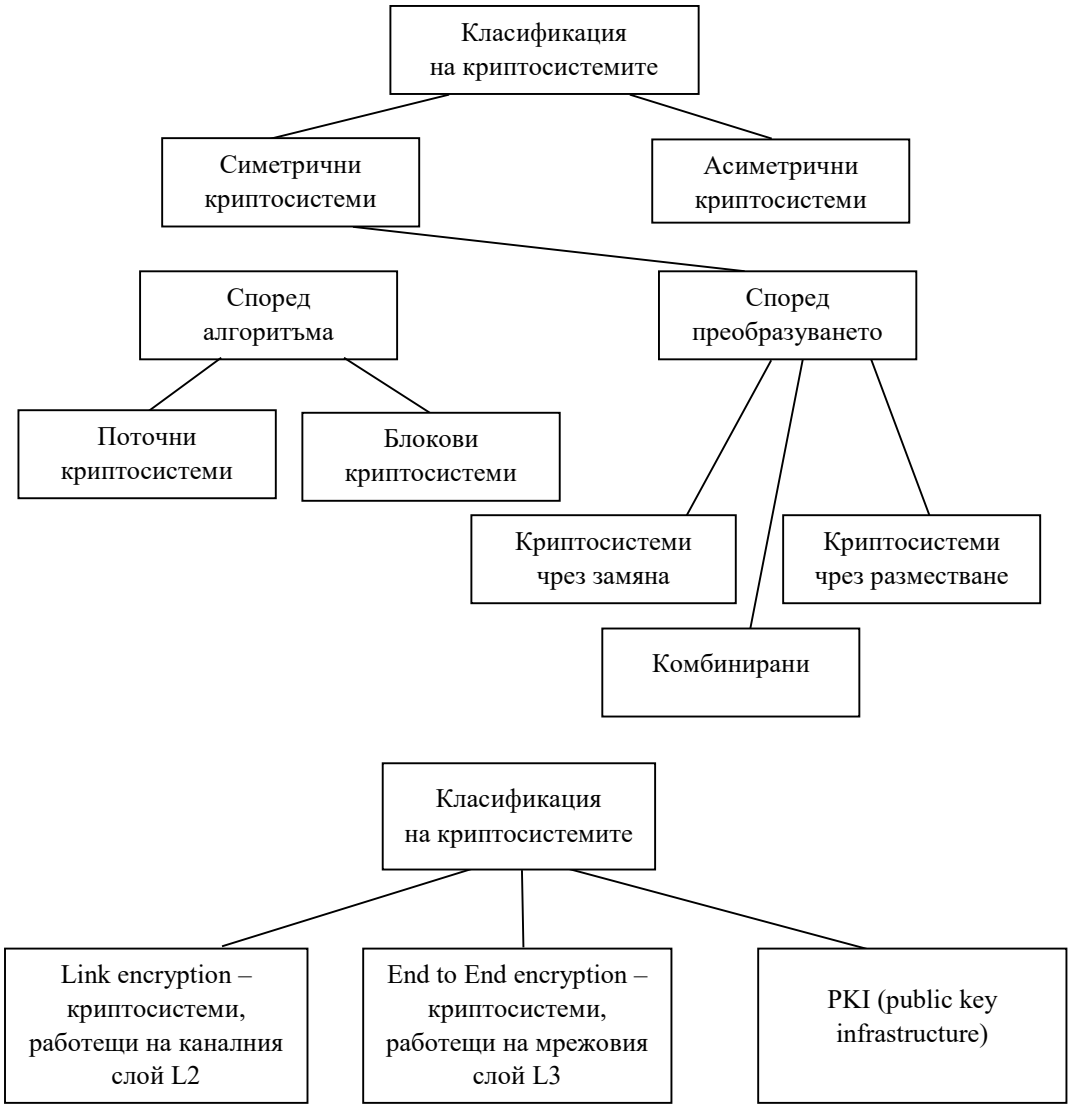
Според алгоритъма за криптиране се делят на поточни криптосистеми и блокови (блочни) криптосистеми.

Според вида на преобразуването се делят на криптосистеми, работещи чрез замяна, разместване или комбинирано.

Съществуват и други класификации на криптосистемите. Например според слоя от OSI модела, в който работят, се делят на:

- криптосистеми, работещи на каналния слой L2 – Link encryption;
- криптосистеми, работещи на мрежовия слой L3 – End to End encryption;

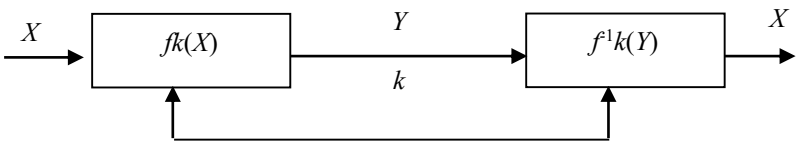
- криптосистеми, работещи върху изградена инфраструктура, поради което могат да се разглеждат като системи, работещи на L7 – PKI (public key infrastructure) (фиг. 23).



Фиг. 23. Класификация на криптосистемите

Симетрични криптосистеми.

При симетричните криптосистеми се използва един и същ ключ (k) за криптиране на съобщението (X) и декриптиране на криптограмата (Y). Основна характеристика на такива системи е, че криптоалгоритъмът $fk(X)$ е известен. Това поставя високи изисквания към системата за управление на ключовете, тъй като, за да работи коректно криптосистемата, ключовете трябва да бъдат доставени на кореспондентите предварително, преди обмена на информация, и то по „таен“ сигурен канал, обикновено различен от канала за комуникация. Принципната схема на функциониране на едноключови криптосистеми е показана на фигура 24.

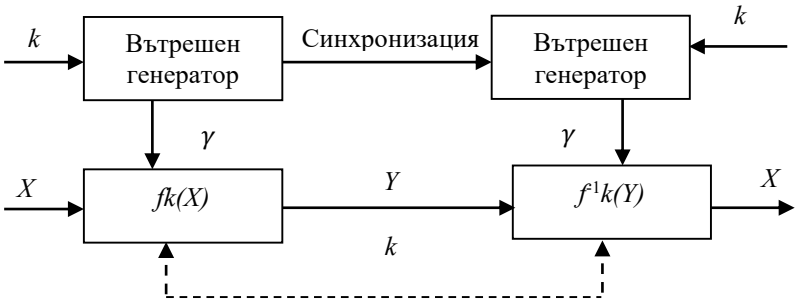


Фиг. 24. Принцип на работа на едноключови симетрични криптосистеми

Симетрични поточни криптосистеми.

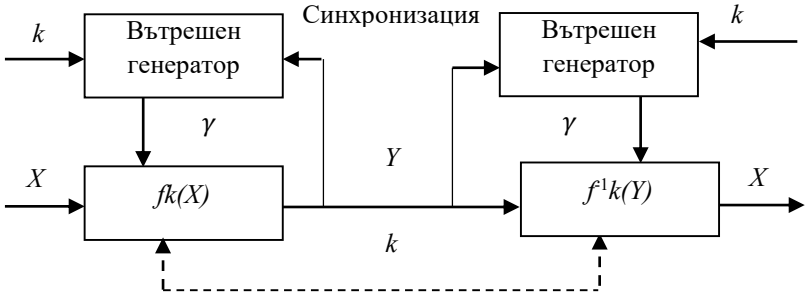
При тези системи всеки символ от откритото съобщение се преобразува в криптограма чрез използвания алгоритъм и ключ. Основният им недостатък е необходимостта от едновременна работа на шифриращото и дешифриращото устройство.

При синхронните поточнокриптиращи системи съществува допълнителна система за синхронизация, която често е твърде сложна и скъпа, но пък те са с голямо бързодействие и времезакъснението е достатъчно малко, за да могат да се използват за услуги, изискващи работа в реален мащаб на времето, като гласови и видеоуслуги (фиг. 25).



Фиг. 25. Поточна криптосистема със синхронизация

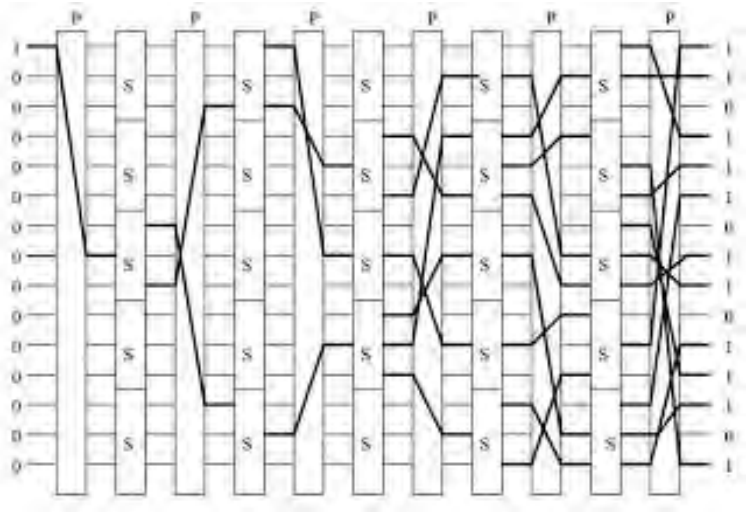
При асинхронните поточни системи системата за синхронизация е с по-проста реализация. При тях се използва ефектът на самосинхронизация посредством въвеждане на специфични маркери в съобщението. Това, от една срана, улеснява техническата реализация, но от друга срана, намалява надеждността на системата посредством ефективна възможност за смущаване на синхромаркера. Освен това системата има ненадеждна идентификация на кореспондентите, тъй като прихванатa и повторена криптограма от „противника“ може да се приеме от кореспондента като автентична (фиг. 26).



Фиг. 26. Поточна криптосистема със самосинхронизация

Симетрични блокови (блочни) криптосистеми.

Симетричните блокови криптосистеми представляват едноключови обратими криптопреобразуващи системи на отделни блокове (части по принцип с фиксирана дължина) на изходното съобщение. Тези системи работят на принципа на поточните системи, но в рамките на отделния блок от съобщението. Последователно блоковете от съобщението се обработват (по принцип нееднократно) чрез преобразования на заместване (S) (substitution) и на разместване (P) (permutation). Такива схеми на преобразуване са получили названието SP мрежи, т.е. мрежи на заместване и разместване. Целта на конструкцията е да се реализира сложна комбинация на преобразуване с относително прости елементи (фиг. 27).



Източник. http://rene-crypto-security.blogspot.bg/2012/10/block-cypher-lucifer.html

Фиг. 27. S-P или SP мрежа

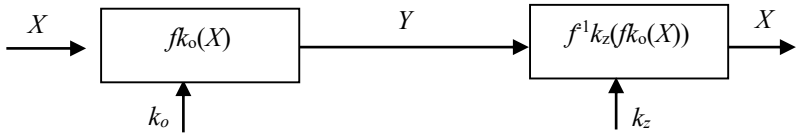
Криптосистеми, работещи чрез разместване.

Принципът на работа на тези системи се състои в преподреждане елементите на съобщението (в съответствие с алгоритъма и ключа) по начин, при който информацията в съобщението да стане нечетима.

Исторически това са едни от първите криптосистеми, използвани за скрит обмен на съобщения. Една от най-популярните е шифърът на Цезар. Идеята на това криптиране е използване на криптоазбука, изместена с няколко позиции спрямо истинската азбука. Всъщност криптоключът е стъпката на изместване на използваната азбука.

Криптосистеми с асиметрично криптиране (криптосистеми с открит ключ).

Специфичното при тези системи е, че криптирането и декриптирането на съобщението се извършва с различни ключове – k_o (открит или публичен) и k_z (таен, закрит или частен) (фиг. 28).



Фиг. 28. Криптосистема с асиметрично криптиране

Криптосистемите с открит ключ се определят от три алгоритъма:

- алгоритъм за генериране на ключове – това позволява да се генерира двойка ключове $k_o \neq k_z$;
- алгоритъм за криптиране $fk_o(X)$;
- алгоритъм за декриптиране $f^1k_z(fk_o(X))$, като се изпълнява условието $X = f^1k_z(fk_o(X))$.

Криптосистемите с открит ключ се базират на шифриращи функции, притежаващи специфичното свойство „еднопосочност“. Еднопосочна е функцията $y = f(x)$, ако притежава следните свойства:

- $y = f(x)$ се изчислява просто;
- има обратна функция;
- обратната функция се изчислява изключително трудно.

Най-общо идеята за асиметричното криптиране се основава на връзката между двата ключа чрез еднопосочна функция. Тогава публичният ключ ще бъде функция (но еднопосочна) от тайния ключ, т.е. $k_o = f(k_z)$. Тъй като функцията е еднопосочна, независимо че е явна, обратната връзка $k_z = f^1(k_o)$ е достатъчно трудна за решаване без информация за k_z, така че може да се приеме за неизчислима. Това свойство позволява само на притежателя на тайния ключ (k_z) да допълни информацията и да реши задачата за декриптиране $X = f^1k_z(fk_o(X))$. Ако евентуалният нарушител не разполага с тази информация, несанкционираното дешифриране на прехванатите шифротекстове ще бъде изключително трудно.

Съществуват множество известни асиметрични криптографски алгоритми. Основните са RSA (Rivest-Shammir-Adelman) на Роналд Ривест, Еди Шамир и Леонард Ейдълман, алгоритъмът на Дифи – Хелман (Diffie-Hellman), алгоритъмът на Полиг – Хелман (Pohlig-Hellman), алгоритъмът „Шнор“ Schnorr на Клаус Шнор (Claus Schnorr), алгоритъмът на Рабин (Rabin), алгоритъмът на Хюг Уйлямс (Hugh Williams), McEliece на Роберт Мак Елис (Robert McEliece) и други. От посочените алгоритми с публичен ключ най-популярен е RSA, следван от алгоритъма на Дифи – Хелман (Diffie-Hellman).

Стандартен алгоритъм DES (Data Encryption Standart).

През 1976 г. в САЩ се приема за държавен стандарт криптоалгоритъмът DES. На основата на използваните елементи в този алгоритъм са разработени множество други алгоритми, като TEA (Tiny Encryption Algorithm), Twofish, IDEA (International Data Encryption Algorithm) и др.

Алгоритъмът е представен от IBM през 1974 г. Създаден е на принципа на SP мрежите и в основата си съдържа няколкократни итеративни преобразования.

Принцип на работа.

Входното съобщение се криптира чрез разместване от P блок, след което се разделя на еднакви блокове (64 или 128 бита). При необходимост се извършва допълване на блоковете.

Всеки блок се разделя на два подблока: L – ляв, и R – десен, с еднакви размери.

Левият подблок се криптира с циклов ключ k_c и функция fc посредством заместване.

Резултатът се сумира по модул 2 (xor) с десния подблок.

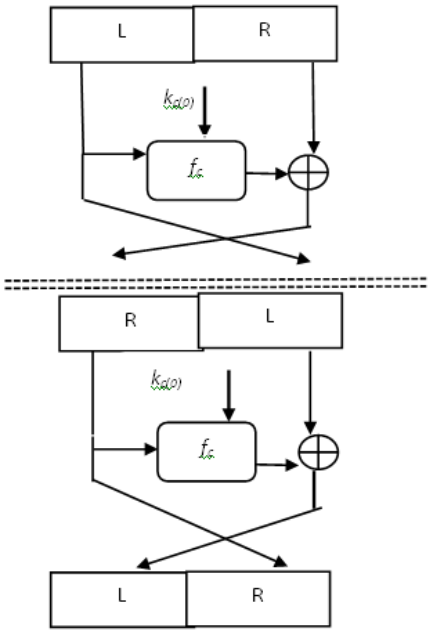
Резултатът от преобразуването на десния подблок се използва в следващия цикъл като ляв подблок.

Левия подблок в текущия цикъл се използва в следващия като десен подблок.

За всеки следващ цикъл по определена зависимост се извлича нов циклов ключ.

Действията се повтарят 16 цикъла.

След преминаването на 16-те цикъла се извършват операцията „конкатенация“ и последно разместване от P блок (фиг. 29).



Фиг. 29. Структура на DES алгоритъм

Посредством многократното прилагане на цикловата функция *fc* се постига достатъчно усложняване на криптоалгоритъма, за да се избегне появата на статистическа зависимост между символите в откритото съобщение, както и между ключа и криптограмата.

Всъщност усложняването се постига в резултат на обединяването на елементарни операции в слоевете на цикловата функция. Всеки слой извършва заместване с цикловия ключ, разместване на входните блокове и реализация на сложна нелинейна зависимост между цикловия ключ и входно-изходните блокове.

Алгоритъмът е развитие на мрежите на Хорст Фейстел, който дефинира основните изисквания към цикловата функция:

- цикловата функция трябва да бъде обратима;
- цикловата функция трябва да бъде нелинейна;

- всеки използван S блок за заместване трябва да предизвиква лавинообразен ефект на усложняване;
- цикловата функция трябва да подържа минимална корелация между откритото съобщение и криптограмата.

Бързото развитие на изчислителната техника през последните десетилетия силно намали разходите за осъществяване на криптоатаки върху алгоритъма DES, поради което използването му се ограничава и дори отхвърля. В настоящия момент приложение намира усложнен вариант на DES, познат като 3 DES (троен DES). В тази модификация се използва 168-битов ключ, значително затрудняващ провеждането на криптоатаки, но алгоритъмът работи около три пъти п-бавно, което за голяма част от потребителите е неприемливо.

Алгоритъм AES.

Криптосистемата Rijndael, известна като AEC (Advanced Encryption Standard), е блоков алгоритъм, неизползващ мрежи на Фейстел. Криптосистемата използва ключове с размери 128, 192 и 256 бита. Блоковете, на които се разделя съобщението, са със същите дължини. Броят цикли, които се прилагат, са 10,12 или 14 в зависимост от дължината на ключа.

Междинните резултати при криптопреобразованията се наричат състояния (state) и се представят под формата на масив от байтове. При големина на блока от 128 бита, равни на 16 байта, масивът има размерност 4x4, а всеки ред или стълб се разглежда като 32-битова дума.

Входните данни се обозначават като байтове на състоянието и след реализацията на целия криптоалгоритъм се представят в нова подредба, в аналогичен по размерност масив.

Данните се представят в масив с брой на стълбовете N_b, определен от дължината на блока, разделена на 32. Шифриращият ключ се представя също в масив с брой на стълбовете N_k, определени от дължината на ключа, разделена на 32.

На фигура 30 са показани формата на данните и ключът при $N_b = 4$ и $N_k = 4$. Броят на циклите, които се прилагат за криптопреобразуване, зависи от N_b и N_k и е даден на фигура 31.

a_{00}	…	a_{03}
…	…	…
a_{30}	…	a_{33}

K_{00}	…	K_{03}
…	…	…
K_{30}	…	K_{33}

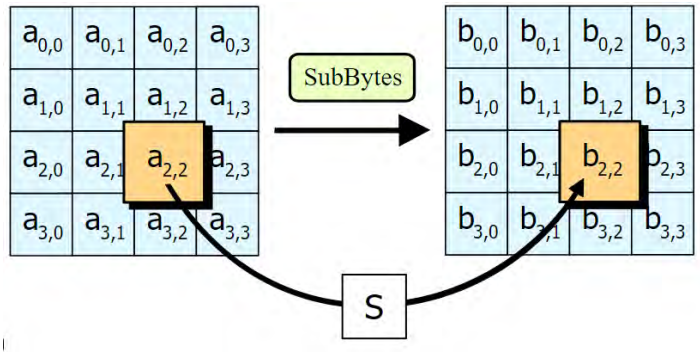
Фиг. 30

N_r	$N_b = 4$	$N_b = 6$	$N_b = 8$
$N_k = 4$	10	12	14
$N_k = 6$	12	12	14
$N_k = 8$	14	14	14

Фиг. 31

Всяко от цикловите преобразования се състои от четири различни действия.

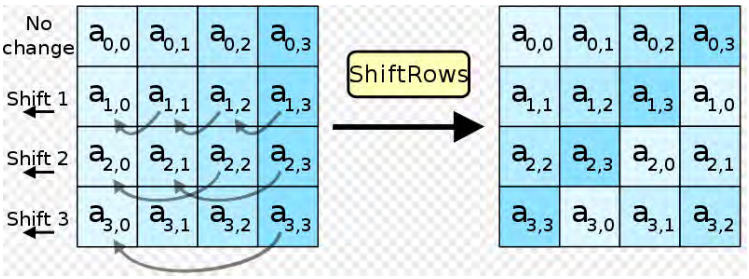
- замяна на байтове SubBytes() – реализира се чрез побайтова замяна в S блок с фиксирана таблица с размерност 8 x 256 (фиг. 32);



Източник. https://upload.wikimedia.org/wikipedia/commons/a/a4/AES-SubBytes.svg

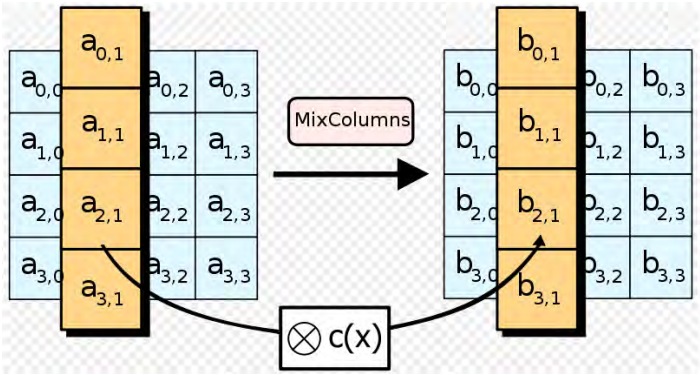
Фиг. 32. SubBytes

- изместване в ред ShiftRows() – побайтово изместване в ред на масива State на различно количество байти (фиг. 33);



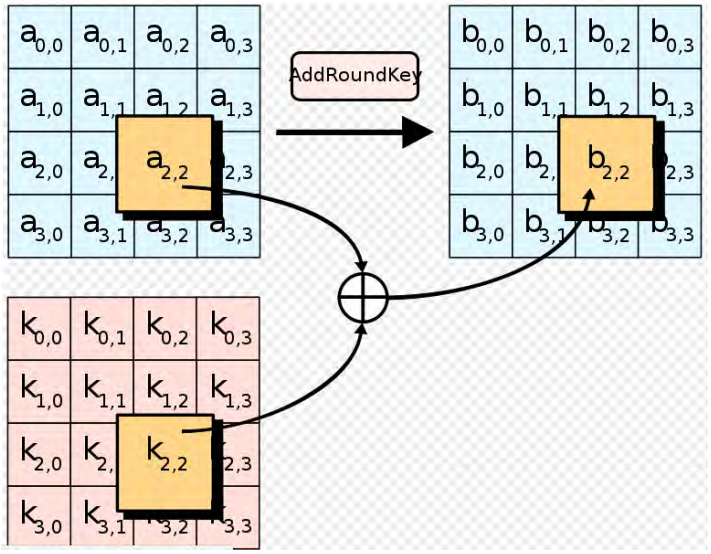
Фиг. 33. ShiftRows

- разместване на стълбовете MixColumns() – реализира се посредством умножение на стълбовете по модул x^4+1 с функция $C(x)$ (фиг. 34);



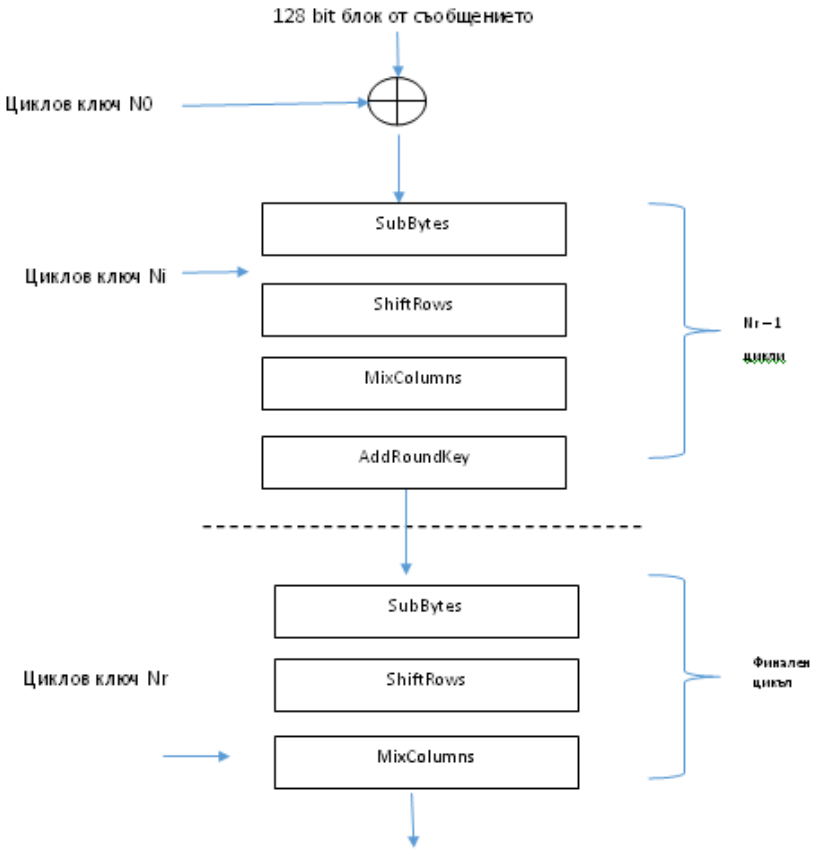
Фиг. 34. MixColumns

- сумиране с цикловия ключ AddRoundKey() – при тази операция стойността на цикловия ключ се добавя (sum mod 2) поразрядно към данните от масива на състоянията (фиг. 35).



Фиг. 35. AddRoundKey

Обобщен схема на функциониране на алгоритъма AES е показана на фигура 36.



Фиг. 36. Структура на алгоритъма AES.

DES vs AES

	DES	AES
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers

Източник. https://thebestvpn.com/advanced-encryption-standard-aes/

Фиг. 37. Сравнение на DES и AES алгоритмите

Изграждане на съвършени криптосистеми.

Проблемите, свързани с определянето на идеалните криптосистеми, за първи път са разгледани систематологично от Шенон през 1949 г. Обект на неговия анализ са вероятностните модели на криптосистема, в която си взаимодействат шифриращ ключ, криптоатака и криптограма.

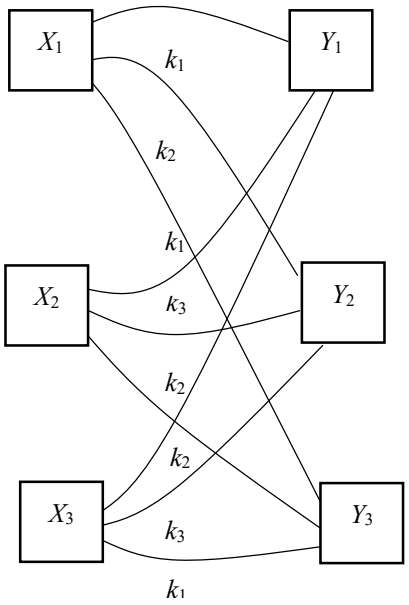
Общата идея за определяне параметрите на идеална криптосистема се изразява в следното.

Приема се, че има крайно множество от открити съобщения $X=\{X_1,X_2,...,X_m\}$, множество от възможни ключове $K=\{k_1,k_2,...,k_l\}$ и множество от криптограми $Y=\{Y_1,Y_2,...,Y_n\}$, всички обвързани с криптопреобразуването $Y_j=f(X_i,k_l)$.

Смята се, че на множеството открити съобщения X е зададено априорно разпределение на вероятности, т.е. $P(X_i), i=\overline{1,m}$, и то е известно на „противника“. Това означава, че при прихванатата от него криптограма Y той би могъл на определи апостериорните вероятности на различните съобщения $P(X_i \mid Y_j)$.

Криптосистемата се приема за съвършена, ако се изпълнява условието $P(X_i \mid Y_j)=P(X_i)$ при всички X_i, Y_j и k_l. В този случай прихванатата криптограма не носи на криптоаналитика никаква информация. Също така няма критерий, по който да се насочат усилията, тъй като всички вероятности, имащи отношение към съдържанието на криптограмата, не се променят. Смисълът на това се състои в липсата на статистическа зависимост между открития текст и криптограмата, т.е. те са статистически независими (фиг. 38).

k_3



Фиг. 38. Идеална криптосистема с три съобщения, три ключа и три криптограми

Абсолютно секретните системи, в които броят на криптограмите е равен на броя на съобщенията, а също и на броя на ключовете, се характеризират със следните две свойства:

- всяко X се свързва с всяко Y само с една линия;
- всички ключове k са равновероятни.

10. Организиране и планиране на криптосистеми [19, 20]

Планирането и организирането на криптосистема е процес на описание на последователността от дейности, подкрепен с необходимата разчетна и графична информация за изграждането и експлоатацията ѝ.

Основните елементи от съдържанието на плана могат да включват решаването на следните задачи:

- определяне типа на криптомрежите;
- определяне броя на криптосъединенията;
- определяне броя на необходимите ключове;
- определяме метода за разпределяне на ключовете;
- определяне мероприятията за възстановяване на криптомрежата при компрометация.

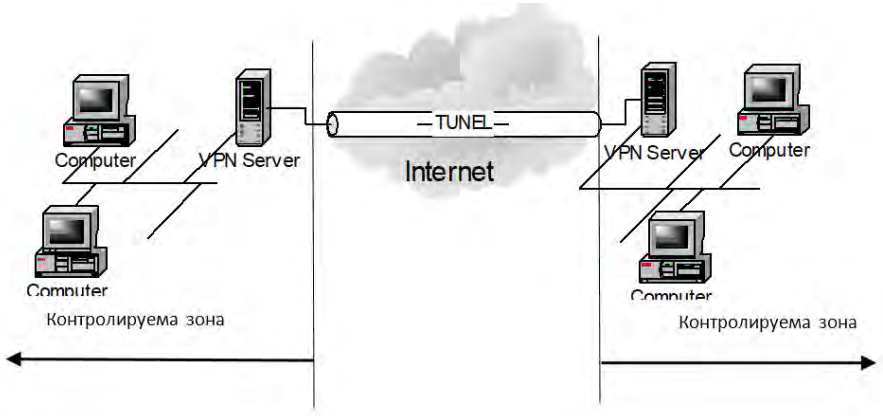
Крайният резултат от процеса е съществуващ план, чиято основна характеристика е организираната система за разпределение на ключове KMS (Key Management System).

Изграждането на определен вид KMS изцяло зависи от класификацията на криптосистемите.

Според тази класификация криптосистемите се разделят в съответствие с нивото от OSI модела, в което те функционират.

На ниво L2.

Едноключови мрежи: Мрежи с канално криптиране – link encryption (фиг. 39).

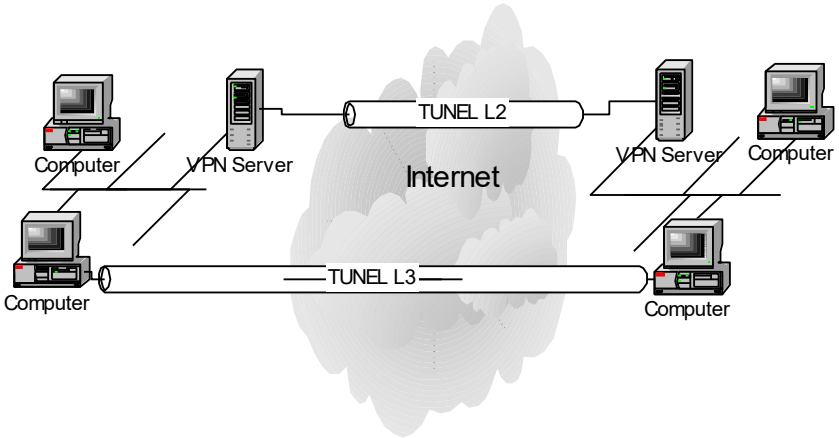


Фиг. 39. Мрежи с канално криптиране

Характерното при планирането на този тип криптомрежи е необходимостта да се съобрази контролируемата зона, която започва от точката на свързване с публичната среда. Много често това се оказва най-скъпият елемент в изграждането на система. Самата технология позволява осигуряване защита на съобщенията само между двата VPN сървъра.

На ниво L3.

Едноключови мрежи: Мрежи с цялостно криптиране – end-to-end (фиг. 40).



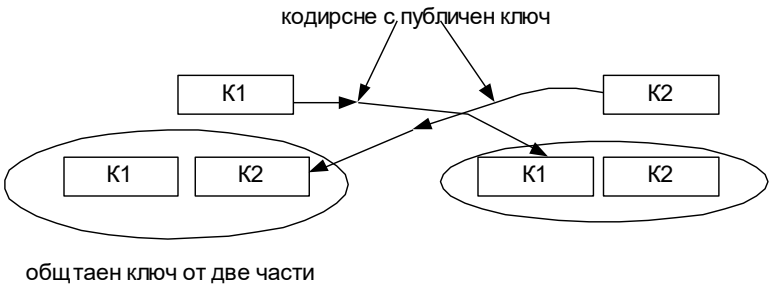
Фиг. 40. Мрежи с цялостно криптиране

При тези мрежи технологията осигурява защита на съобщението между точки от мрежовия слой (например между два IP адреса). Такава гъвкавост при администриране изисква от администраторите на криптомрежата да съобразят и разпространението на политиката за криптиране върху цялата мрежа. Ако в конкретната схема има криптиран обмен на съобщения между двама кореспонденти от две различни мрежи, то между тях и който и да е друг кореспондент в мрежата (подмрежата, домейна) обменът ще бъде некриптиран.

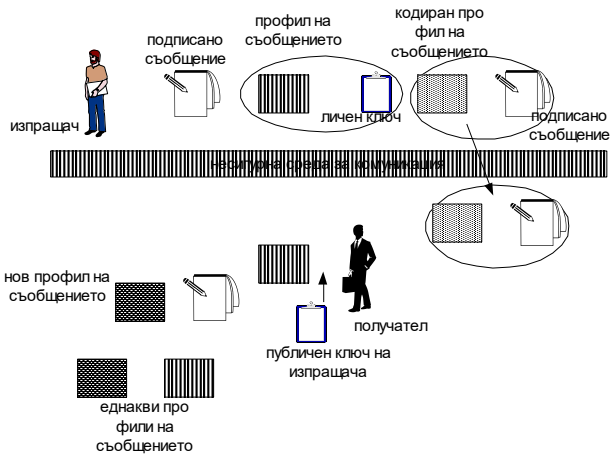
Друга характерна особеност на тази технология е отпадането на необходимостта от контролируема зона. Трябва да се осигури контрол на достъпа само до конкретното терминално устройство.

Криптомрежи с публичен ключ.

Това са криптомрежи, които функционира върху предварително изградена инфраструктура, определена като PKI (Public Key Infrastructure) (фиг. 41).



Електронен подпис.



Фиг. 41. PKI (Public Key Infrastructure).

Тази инфраструктура включва организирането на специфична KMS.

Организиране на едноключови криптомрежи.

Основното предназначение на криптосистемите е да осигурят защитен обмен на съобщения между отдалечени кореспонденти през публична среда. Изпълнението на тази задача винаги е съпътствано с решаването на въпроса за еднозначно разпознаване между кореспондентите.

Нейното реализиране в практиката също е елемент от организацията на мрежата и е задължителна стъпка при първоначално установяване на комуникация и при всеки случай на съмнение за компрометация или явна компрометация на криптосистемата.

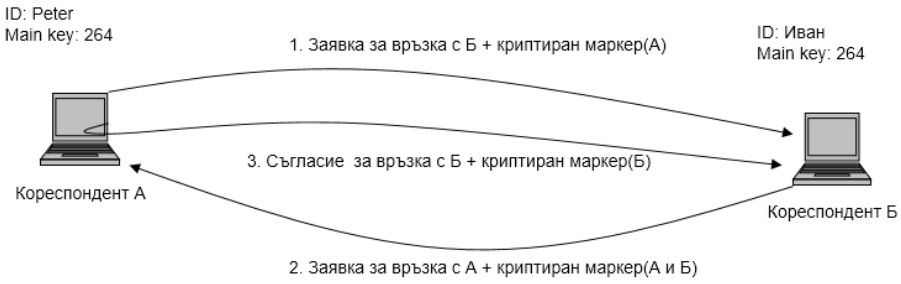
Най-разпространеният алгоритъм за автентификация включва две предварителни условия:

- доставен главен ключ (master key) на кореспондентите;
- познаване името на кореспондента,

и следните стъпки:

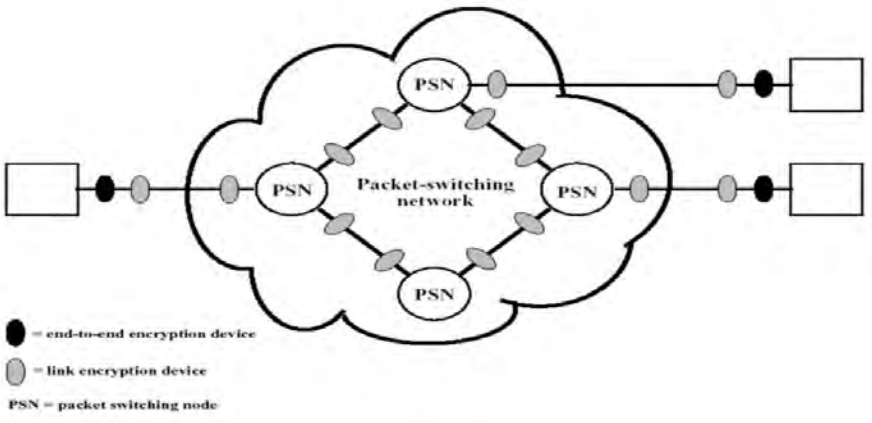
- заявка за връзка на кореспондента А с Б, изпращайки криптиран маркер (А);

- криптирането на маркера става с предварително доставения главен ключ;
- заявка за връзка на кореспондента Б с А, изпращайки криптиран маркер (А и Б);
- кореспондентът Б декриптира маркера от А, към него добавя свой маркер и заедно ги криптира с предварително доставения главен ключ;
- съгласие за връзка на А с Б, изпращайки криптиран маркер (Б);
- кореспондентът А декриптира маркерите, сравнява своя маркер с изпратения и връща отново криптиран маркера на Б (фиг. 42).



Фиг. 42. Алгоритъм за автентификация

Съществена разлика в организацията на криптомрежите, работещи на 2-ро и 3-то ниво, е количеството необходимо оборудване. Примерът, посочен на фигура 43, недвусмислено разкрива преимуществата на мрежите, работещи на 3-то ниво. В конкретния случай на мрежата от 2-ро ниво са необходими 14 криптоустройства, а на мрежата от 3-то ниво – 3 криптоустройства. Очевидните ресурсни преимущества са в резултат на по-сложната система за администриране (фиг. 43).



Източник. https://slideplayer.com/slide/6084019/

Фиг. 43. Криптомрежи, работещи на 2-ро и 3-то ниво

Организация на системата за разпределение на ключове при едноключови криптосистеми.

Разпределението на ключовете може да бъде организирано по няколко начина:

- Ключът може да бъде избран от А и физически доставен на В.
- Ключът може да бъде избран от трета страна и физически да бъде доставен на А и В.
- Ако участниците в обмена А и В използват общ ключ, една от страните може да предаде новия ключ на другата в криптиран вид, като използва стария ключ.
- Ако двете страни имат защитени канали за връзка с трета страна С, тя може да достави ключа на А и В по този канал.

Изграждането на организация за разпределение на ключове изцяло зависи от използваната технология за криптиране. Поради това първите два варианта са приложими при канално криптиране, третият – при канално и крайно криптиране, а четвъртият – само при крайно криптиране.

При мрежи с криптиране end-to-end широко се използва схема за доставката на ключовете с център за разпределение на ключовете (ЦРК). Всеки кореспондент получава уникален ключ, който се използва за криптирана комуникация с ЦРК, откъдето се доставят ключовете.

Връзката между крайните системи се криптира чрез временен ключ, наречен сеансов (session key). Той служи за конкретно логическо съединение и след това не се използва. Получава се от ЦРК по мрежата в криптиран вид, като се използва главният ключ, който е общ за ЦРК и дадената крайна система или конкретен потребител.

Главните ключове трябва да бъдат разпределени по сигурен начин, но те са само *N* на брой и могат да се доставят и по некриптографически начин.

Подобна схема позволява изграждане на йерархична структура на разпределение (фиг. 44).

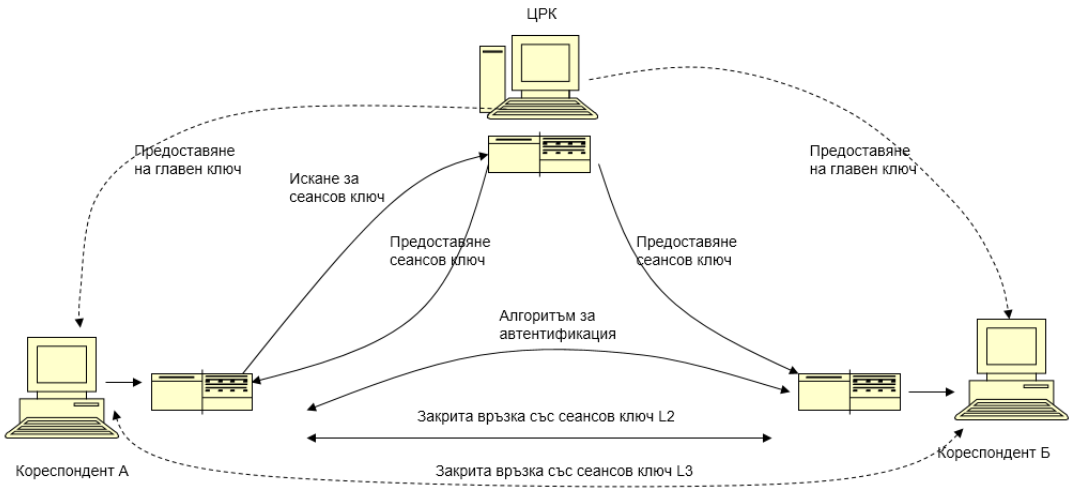
Фиг. 44. Йерархична структура на разпределение на ключове

Възможно е разпределението на ключовете да се прави само от един ЦРК, както и да се създадат локални ЦРК, които отговарят за малки домейни от мрежата. Когато трябва да се установи връзка между кореспонденти от различни домейни, съответните локални ЦРК могат да използват за установяване на връзка глобален център за разпределение на ключовете.

Йерархичната схема минимизира разходите за управление, съкращава времето за реакция и създава добри условия за възстановяване на системата.

Важно условие за устойчивостта на защитата е времето за използване на ключа. Честата му смяна обаче води до увеличаване на служебния трафик.

Съществува необходимост от смяна на ключа и след определена продължителност от време или количество обменени съобщения между кореспондентите (фиг. 45).



Фиг. 45. Организиране на KMS чрез домейнов център за разпределение на ключовете

Друг съществен проблем при организацията на криптомрежите е определянето на необходимия брой ключове за работа на системата. При тяхното количествено определяне трябва да се вземат предвид типът на криптосистемата (работеща на L2, L3 ниво) и необходимият брой резервни ключове и ключове, използвани при компрометация.

Броят на ключовете зависи от броя на свързаните двойки.

$$K = \frac{N(N-1)}{2}, \qquad (12)$$

където K е броят на ключовете;

N – броят на свързаните двойки.

Организация на мрежи с публични ключове.

Криптографските системи с публични ключове се използват за решаването на две задачи:

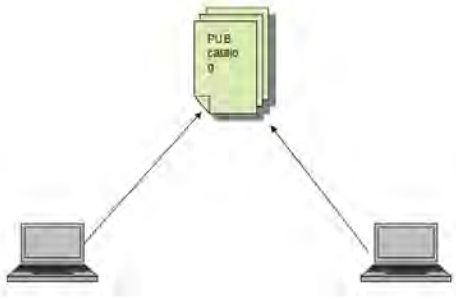
- разпределение на публични ключове;
- разпределение на секретни ключове.

Разпределението на публичните ключове може да стане по няколко метода:

- метод с публична обява;
- публично достъпен каталог;
- авторитетен източник на откритите ключове;
- сертификати на откритите ключове.

Метод с публична обява.

Публичният ключ трябва да бъде общодостъпен. По този начин всяка страна, участваща в обмена, дава своя публичен ключ на другата страна или на всички (фиг. 46).



Фиг. 46. Метод с публична обява

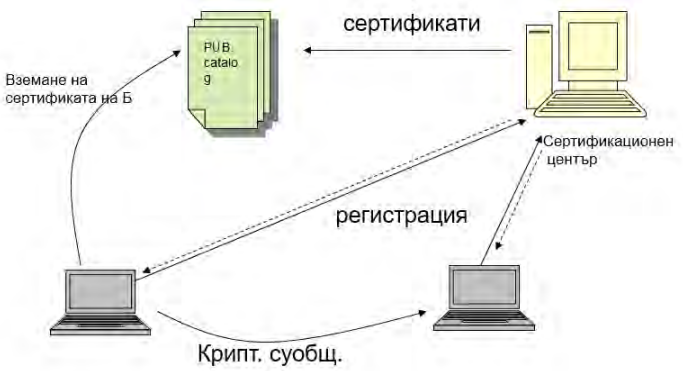
Подобрение на организацията се реализира чрез център, който отговаря и поддържа динамичен каталог на публичните ключове на всички участници в обмена. Всеки участник знае публичния ключ на центъра, но само центърът знае съответния секретен (личен) ключ, който дава на участниците в групата (фиг. 47).

Фиг. 47. Метод с авторитетен източник

Система с раздаване на сертификати.

Всеки сертификат съдържа публичния ключ и допълнителна информация и се създава от авторитетен източник на сертификати. Дава се на участника заедно с частния (личния, секретния) ключ. Един участник в обмена предава информацията за своя ключ посредством сертификата си. Другите участници могат да проверят, че сертификатът е създаден именно от авторитетния източник.

Получателят използва публичния ключ на източника на сертификати (Kuauth), за да декриптира сертификата. Тъй като той може да се прочете само с публичния ключ на източника на сертификати, това дава гаранция, че сертификатът е дошъл именно от този източник (фиг. 48).



Фиг. 48. Система с раздаване на сертификати

Форма и съдържание на плана на криптомрежите.

Форма на плана.

Една примерна форма може да включва:

- Разчети при определяне параметрите на криптомрежата. Това са разчети, свързани с определяне типа на криптомрежите, техния брой и броя свързани двойки.
- Период за смяна на ключовете в съответствие с изискванията. Част от разчета е и определяне броя на ключовете, необходими за нормалното функциониране на мрежата.

Разчетните инструменти, подходящи за този етап от планирането, са:

- Определяне времето за разбиване на ключа по формула (1):

или вероятностният показател формула (2).

- Определяне броя на необходимите ключове по формула (12):
- Оценка на защитеността на системата – отношението на защитените информационни услуги към общото количество услуги в комуникационно-информационната система.

$$K_{\text{скритост}} = \frac{K_{\text{защитени}}}{K_{\text{общо}}} \qquad (15)$$

В резултат на анализа на получените разчетни данни се определя конкретната система за разпределение на ключовете.

Таблица за разпределение на ключовете.

Таблица 3

Таблица за ключовите документи в МС (извлечение за MNB)

Информационно направление	*Вид на комуникационния канал*	*Номер на ключовия документ*	
		основен	*резервен*

Таблица 4

Таблица за разпределение на ключовите документи

№	Наименование на свързаните двойки – номер	Условен номер на ключа	Тип на документа	Номер на ключа	Екз. номер	Забележка

Таблица за състава на криптосъединенията.

Таблица 5

Таблица за състава на криптосъединенията

№	Номер на направлението	Условно наименование	Условен номер на ключа	Условен номер на канала (логич. направление)	Тип на оборудването	Пореден номер на оборудването на възела			Време за работа	Забележка
						възел 1	възел 2	възел 3		

Мероприятия за възстановяване на мрежата при компрометация.

11. Основни принципи за изграждане на система за киберсигурност [21, 22, 23]

Международни стандарти ISO/IEC 27000.

Двадесет принципа за проектиране корпоративна сигурност на информацията.

1. Не се подвеждайте прекалено от политиката за сигурност на друга организация. Всяка организация и мрежа са различни. Само защото нещо работи за някой друг или за тяхната среда, означава, че работи за тях. Добрата хигиена на киберсигурността е важна за всички, но потребностите и уязвимостта на вашата организация са уникални.

2. Поддържайте уязвимите системи и софтуер. В киберсигурността са гарантирани две неща: уязвимости и пробиви. За да се ограничат пробивите, организациите трябва да намерят и да „запушат“ пробивите в своята мрежа. Звучи просто, но изисква процес на организация, който държи хората отговорни за изпълнението на корекции и други поправки.

3. Не използвайте неподходящо съдържание. Проблеми като този трябва да се кажат, но това все още е сериозен проблем. Порнографските сайтове са най-бързият начин за

компрометиране в интернет. Организациите трябва да заявят много ясно да не се използват корпоративни имейл акаунти за запознанства и връзки. От само себе си се разбира, че тези сайтове могат да разрушат компании, кариери и семейства. Интернет има по-голяма памет от тази на слон.

4. Развийте способности за реагиране при инциденти и за киберкриминалистика. Организациите трябва да развиват способности за реагиране при вътрешни инциденти и за киберкриминалистика. Препоръчително е да се формират екипи за реагиране при инциденти, включващи всички представители на технически дисциплини, мениджмънт и ръководител на връзките с обществеността. Като минимум организациите трябва да участват в периодични тренировки за преглед на процедурите за реагиране при инциденти. Уверете се, че вашата организация е готова да се защити. Това води до следващия принцип.

5. Поддържайте всички логфайлове в лесен за достъп вид. За да се изпълнят точен отговор на инциденти и цифрова киберкриминалистика, организациите трябва да разполагат с всеобхватно решение за мониторинг на логфайловете. Те също така трябва да бъдат лесни за претърсване, да се извършват корелации и хората да знаят как да ги използват. Първият път, когато много организации обръщат внимание на способностите си за управление на логфайлове, е след пробив и това е най-лошото време, за да разберете, че не работи.

6. Познавайте вашата DNS дейност. Много организации могат да се съсредоточат и да превъзхождат само в няколко дисциплини. Що се отнася до активността на логването за ефективен отговор на инциденти, мониторингът на DNS е един от най-критичните елементи, но е трудно да се намерят много хора, които да се фокусират върху него. Поставете „Наблюдаване на DNS файлове“ под категорията „Най-голямо качество за вашите пари“. Организациите не могат да реализират правилен отговор на инцидент и анализ на обхвата на проникване, без да разбират какво става с DNS.

7. Подсигурете най-слабата връзка. Представете си, че сте отговорни за безопасно транспортиране на злато от един бездомен човек, който живее на пейка в парка (ще го наречем Linux) до бездомна жена, която живее в другия парк (ще я наричаме Android). Наемете брониран камион, за да транспортирате златото. Името на транспортната компания е Applied Crypto, Inc. Поставете се в ролята на атакуващ, който трябва да открадне златото. Бихте ли атакували камиона Applied Crypto, Inc, бездомника Linux или бездомната жена Android? Доста лесен експеримент, а? (Съвет: Отговорът е „всичко освен криптото“.)

Практиците по сигурността често посочват, че сигурността е верига и точно като веригата е толкова силна, колкото и най-слабата връзка – една система за сигурност е толкова сигурна, колкото и най-слабият ѝ компонент. Атакуващите следват най-слабата точка в системата, а най-слабата точка рядко е функция или атрибут на сигурност. Когато става дума за проектиране на сигурността, не забравяйте да разгледате най-слабата връзка във вашата система и да сте сигурни, че тя е достатъчно сигурна.

8. Защита в дълбочина. Резервирането и слоестата структура обикновено са добро нещо в сигурността. Не се надявайте защитната ви стена да блокира целия злонамерен трафик; използвайте и система за откриване на проникванията. Ако проектирате приложение, блокирайте отделни точки на пробив чрез изграждане на резерв в сигурността и защитни слоеве. Идеята зад дълбоката защита е да се управлява рискът чрез различни отбранителни стратегии, така че, ако един слой от защитата се окаже неадекватен, друг слой от нея ще

предотврати пълен пробив. Това е понятие, преповтаряно от експерти по сигурността на информацията, и с основателна причина: работи.

9. Провалете се „сигурно“. Уверете се, че всяка система, която проектирате, не се „отваря“ при пробив. Пример: продукт на Microsoft от миналото при три неуспешни опита за въвеждане на парола или потребителско име предлагаше въвеждането на нова парола!!! Очевидно по-доброто действие в такава ситуация е да се откаже достъп.

Всяка достатъчно сложна система ще има режими на неизправност. Пробивът е нещо неизбежно и трябва да се очаква/планира. Това, което може да се избегне, са проблеми със сигурността, появили се след пробив. Проблемът е, че когато много системи се провалят по някакъв начин, те проявяват несигурно поведение.

10. Дайте най-ниската привилегия. Когато трябва да дадете разрешение на даден потребител или процес да направи нещо, дайте му възможно най-ниската привилегия. Пример: вашите контакти в Outlook. Ако имате нужда от някой, който да има достъп до контактите ви, за да видите някои данни, дайте му разрешение за четене, но не му давайте разрешение за редактиране. Или по-сложен пример: повечето потребители на дадена система не трябва да имат нужда от root привилегия за ежедневната си работа, така че не я давайте на тях. Избягвайте неволното, нежеланото или неподходящото използване на привилегиите, като ги раздавате пренебрежително.

11. Разграничавайте привилегиите. Пример: система, която разделя фронт-енд автентификацията си на внушителен брой роли с различна степен на достъп до системата. Проблем: когато даден потребител на която и да било роля трябва да извърши бек-енд действие с базата данни, софтуерът предоставя временно де факто администраторска привилегия на всеки потребител. Това не е добре. Дори и най-новият стажант би могъл да спре базата данни.

12. Опростете механизма. Сложността е враг на инженерството по сигурността и приятел на хакера. Прекалено лесно е да се преодолеят нещата в сложна система както от гледна точка на дизайна, така и от гледна точка на изпълнението. Ирония: Искате ли да видите нещо сложно? Разгледайте почти всеки модерен корпоративен софтуер!

13. Не споделяйте механизми. Трябва ли да поставите вашето бек-енд бизнес приложение в публичния облак? Вероятно не, според този принцип. Защо системата ви за удостоверяване да се натоварва със случаен интернет трафик, когато можете да го ограничите до служители, на които се доверявате (предполагаемо)?

14. Не се доверявайте лесно. Предполагайте, че средата, в която функционира вашата система, е враждебна. Не позволявайте на всякого да използва вашите API и със сигурност не позволявайте на никого да получи достъп до тайните ви! Ако разчитате на облачен компонент, поставете някои проверки, за да сте сигурни, че не е фалшив или по друг начин компрометиран. Предвиждайте атаки като инжектиране на команди, кръстосани скриптове и т.н.

Този принцип може да стане труден за използване много бързо. Доверието е транзитивно. След като покажеш известно доверие, често то се предава на всеки, на когото довереното лице може да се довери.

15. Приемете, че тайните ви не са в безопасност. Сигурността не е невидима особено когато става дума за тайни, съхранени във вашия код. Да предположим, че нападателят ще

разбере колкото може повече за вашата система като привилегирован потребител. Наборът от инструменти на атакуващия включва декомпайлери, дисасемблери и всякакви инструменти за анализ. Очаквайте да бъдат насочени към вашата система. Търсили ли сте криптоключ в двоичен код? Анализ на ентропията може да го накара да се появи като коледна елха. Двоичният код е само език.

16. Цялостно посредничество. Всеки достъп и всеки обект трябва да се проверяват всеки път. Уверете се, че системата ви за контрол на достъпа е ефективна и е проектирана да работи в мултиканалния свят, в който живеем днес. Каквото и да правите, убедете се, че ако разрешенията се променят в движение във вашата система, този достъп се преглежда систематично. Не кеширайте резултатите, които дават правомощия или генерират авторитет. В свят, в който големите разпределени системи са широко разпространени и машините с множество процесори са норма, този принцип е главен.

17. Направете сигурността използваема. Ако механизмите ви за сигурност са твърде отблъскващи, вашите потребители ще направят така, че да ги заобиколят или да ги избегнат. Уверете се, че системата ви за сигурност е толкова сигурна, колкото трябва, но не повече. Ако повлияете твърде много на използваемостта, никой няма да използва вашите неща, без значение колко е сигурна системата. Тогава тя ще бъде много сигурна, но и почти безполезна.

18. Насърчаване на неприкосновеността на личния живот. Всички говорят за неприкосновеността на личния живот, но повечето хора всъщност не правят нищо за това. Когато проектирате система, помислете за поверителността на крайните потребители. Събирате ли лична идентифицираща информация само защото някой от маркетинговия екип е казал да се прави? Добре ли е да се направи? Съхранявате ли идентифицираща информация на място, което може да бъде компрометирано? Не трябва ли това да бъде криптирано? Практиците по сигурността на информацията невинаги трябва да предоставят отговори на тези въпроси, свързани с поверителността, но е важно Infosec да изложи тези въпроси, ако никой друг не го прави.

19. Използвайте ресурсите си. „Използвайте ресурсите си“ е принцип с невероятно широко приложение. Ако не сте сигурни дали дизайнът на вашата система е защитен, помолете за помощ. Анализът на архитектурния риск е труден, но има хора, които го правят в продължение на десетилетия. Не се опитвайте да го направите сами, ако не можете. И не се притеснявайте да помолите за помощ; тези неща са трудни.

20) Непрекъснато тествайте защитата си в дълбока архитектура. Въпроси: Вашата мрежа това ли е, което смятате, че е? Ако във вашата мрежа е имало нападател, бихте ли могли успешно да я защитите?

Мрежите се променят непрекъснато и повечето организации не са най-добрите при актуализирането на документацията за това как се реализира тяхната мрежа. Един ден тясното място на мрежата е точно на правилното място, след което конфигурирате нови суичове, които карат целия трафик да заобиколи тази тясна точка. След това нещо се променя в мрежата ви и тя повече не е същата.

Колкото повече устройства и сензори добавяте към уравнението, толкова повече системи не правят това, което трябва да правят. Организациите трябва да въведат процеси за тестване контрола за сигурност, за да са сигурни, че вашата защита в дълбочина върши това, което смятате, че трябва да върши.

Принципи на киберсигурността за индустрията и правителството.

Тъй като промишлеността и правителствата (би следвало да) работят заедно за разработването на правилната политическа рамка за повишаване на киберсигурността, трябва да се следват шест основни принципа:

ПРИНЦИП 1: Усилията за подобряване на киберсигурността трябва да стимулират публично-частните партньорства и да се надграждат върху съществуващите инициативи и ангажименти за поддръжка на ресурси. Чрез партньорство с правителството ИТ индустрията предоставя лидерство, ресурси, иновации и настойничество във всеки аспект на киберсигурността в продължение на повече от 20 години. Усилията в киберсигурността са най-ефективни, когато се използват съществуващите инициативи, инвестиции и партньорства.

ПРИНЦИП 2: Усилията за подобряване на сигурността в киберпространството трябва да отразяват правилно безграничната и глобална природа на днешната киберсреда. Киберпространството е глобална и всеобхватна система, която обхваща географските граници и преминава през националните юрисдикции. Правителството и индустрията следва да играят водеща роля в насърчаването на използването на водещи в отрасъла световнопризнати стандарти, най-добри практики и програми за поддържане сигурността и оперативната съвместимост.

ПРИНЦИП 3: Усилията за подобряване на киберсигурността трябва да могат бързо да се адаптират към възникващите заплахи, технологии и бизнес модели. Информационните технологии са иновативен и динамичен сектор с бързопроменящи се и еволюиращи технологии. Усилията за сигурност в киберпространството трябва да бъдат еднакво динамични и гъвкави, за да се използват ефективно новите технологии и бизнес модели и да се решават нови, постоянно променящи се заплахи.

ПРИНЦИП 4: Усилията за подобряване на киберсигурността трябва да се основават на управлението на риска. Сигурността не е крайно състояние. По-скоро това е средство за постигане и осигуряване на постоянно доверие в различните технологии, които се състоят от киберинфраструктурата. Усилията в киберсигурността трябва да затвърдят способността на организацията да разбира правилно, да оценява и предприема стъпки за управление на продължаващите рискове в тази среда.

ПРИНЦИП 5: Усилията за подобряване на киберсигурността трябва да се съсредоточат върху осведомеността. Собствениците на киберпространството включват всички, които го използват: потребители, фирми, правителства, собственици на инфраструктура и оператори. Усилията за сигурност в киберпространството трябва да подпомогнат тези заинтересовани страни да осъзнаят рисковете за собствеността, репутацията, операциите и понякога за бизнеса и да разберат по-добре важната им роля, като помагат да се справят с тези рискове.

ПРИНЦИП 6: Усилията за подобряване на киберсигурността трябва да се насочат по-пряко към лошите участници и техните заплахи. В киберпространството, както във физическия свят, противниците използват инструменти (в този случай технологии) за извършване на престъпления, шпионаж или война. Политиките за киберсигурност трябва да дават възможност на правителствата да използват по-добре действащите закони, усилия и практики за обмен на информация, за да отговорят на киберпрестъпленията, заплахите и инцидентите в страната и чужбина.

Развитие на международните стандарти за системи за управление на информационната сигурност (ISMS) ISO/IEC 27000

Система за управление на информационната сигурност.

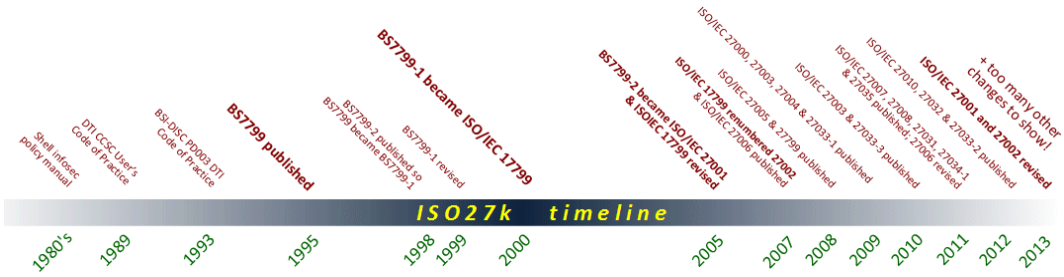
Системата за управление на информационната сигурност е част от цялостната система за управление, базирана на подхода на бизнес риска да създава, прилага, управлява, наблюдава, преглежда, поддържа и подобрява информационната сигурност (определение по ISO).

Забележка. Системата за управление представлява набор от взаимносвързани или взаимодействащи си елементи на организацията за да се създадат политики, цели и процеси за постигането на тези цели.

Обхватът на системата за управление може да включва цялата организация, конкретни и идентифицирани функции на организацията, специфични и идентифицирани сектори на организацията, една или повече функции в рамките на група организации.

Хронология на развитието на международните стандарти за системи за управление на информационната сигурност ISO/IEC 27000.

Стандартите ISO 27000 се появяват през 80-те години на миналия век и продължават да се развиват и променят, отразявайки новите предизвикателства и възникващия консенсус относно добрите практики за информационна сигурност. Съществуват няколко ключови етапа в разработването на основните стандарти (фиг. 49).



Фиг. 49. Етапи в разработването на основните стандарти

1. ISO/IEC 27001:2013 и 27002:2013 – нови версии.

ISO/IEC JTC1/SC 27 – преработени и преиздадени ISO/IEC 27001 и 27002 през 2013 г.

Процесът на ревизиране е труден и бавен, особено на 27002, който става почти невъзможен за поддръжка. 27001 е значително променен, за да се приведе в съответствие с другите стандарти на ISO за управление на системи.

През 2013 г. са публикувани или актуализирани редица други стандарти на ISO 27000.

2. ISO/IEC 27002:2005.

ISO/IEC 17799:2005 е преномериран на ISO/IEC 27002:2005 в средата на 2007 г., за да бъде въведен в семейството стандарти ISO/IEC 27000. Текстът остава същия като на ISO/IEC 17799:2005. За известно време стандартът ISO/IEC 17799 продължава да се доставя на всеки, който е поръчал ISO/IEC 27002, заедно с лист, отбелязващ промяната в номера.

3. ISO/IEC 17799:2005.

През юни 2005 г. версията от 2000 г. е значително актуализирана с нови раздели, които консолидират съветите за управление на риска и инцидентите, както и много други ревизии, които се правят навсякъде. Форматът е променен, за да се вмъкнат „Бележки за изпълнението“ под всеки контрол.

4. ISO/IEC 17799:2000 – първа ISO/IEC версия на BS7799-1.

След тежък период на международно обсъждане и преразглеждане BS 7799, част 1:1999 е окончателно приета от ISO/IEC по ускорен процес и е пусната като ISO/IEC 17799 през декември 2000 г. Някои членове на ISO/IEC JTC1/SC 27 не подкрепят това първо издание, но то е прието като отправна точка до по-нататъшно развитие.

5. BS 7799, част 1:1999 – преработен.

След преглед от BSI стандартът е преработен и преиздаден през 1999 г.

6. BS 7799, част 1:1998 – преименуван.

Към предходния британски стандарт 7799 се присъединява нов сертификационен стандарт, част 2 (по-късно става ISO/IEC 27001), така че първоначалният стандарт е преименуван на част 1 през 1998 г.

7. BS 7799:1995 – първоначално публикуван като британски стандарт.

Британският институт по стандартизация BSI (наричан понастоящем Британски стандарти BSI, част от BSI Group) издава British Standard 7799.

8. 1993:BSI-DISC PD003 – Code of Practice на DTI за управление на информационната сигурност – първо публично издание.

В очакване на приемането му като официален британски стандарт BS 7799 предварително е издаден от Министерството на търговията и индустрията на Великобритания чрез Института за британски стандарти като свободна информационна единица, наречена BSI-DISC PD003 (BSI – доставяинформационни решения за клиенти – публичен документ 003). Професор Едуард Хъмфрис от Националния изчислителен център на Обединеното кралство (NCC) заедно с професионалистите в областта на информационната сигурност от Shell, BOC Group, British Telecom, Marks and Spencer, Midland Bank, Nationwide участват в разработването на PD003. Издаването му се подкрепя от BP, British Aerospace, British Steel, Bull, Cadbury, Schweppes, Cameron Markby Hewitt, Chelsea Building Society, Ciba Geigy, Digital Equipment Corporation, Reuters и TSB Bank. BSI-DISC пускат и някои съвременни безплатни придружаващи брошури, една от които (PD005) има чиста схема от една страница, обобщаваща процеса на внедряване, който, за съжаление, не оцелява до нито един от днешните ISO 27K материали. По-късно DTI стана BERR (Министерство на предприемачеството и регулаторната реформа) и поддържа стандартите ISO 27K и днес.

9. 1989 – Кодекс на практиката на потребителя на DTI CCSC (първа публикация извън Shell).

Използвайки донорския документ на Shell, Центърът за търговска и компютърна сигурност на Министерството на търговията и индустрията в Обединеното кралство разработва и публикува това ръководство за защита на информацията за своите членове. CCSC също така публикува „Зелена книга“, която с помощта на CESG става схема за сертифициране на продуктите за сигурност на ITSEC (ИТ сигурност и оценка), стартирана през 1990 – 1991 г.

10. Късните 80 – Ръководство за политиката за сигурност на Royal Dutch/Shell Group.

BS 7799 и следователно ISO 27000 дължат своето съществуване на този вътрешен документ, предоставен на общността от Shell. Когато се публикува за първи път през 1995 г., акцентът на BS 7799 върху концепциите за сигурността на мейнфрейм и липсата на изрични препратки към интернет говорят за неговия произход през предходното десетилетие. Тази липса на актуалност остава под въпрос и днес при ISO 27000, тъй като процесите по ISO/IEC за обхват, специфициране, изготвяне, договаряне и публикуване на международните стандарти имат времеви цикли от няколко години, докато всяка година се появяват значителни нови проблеми с информационната сигурност. Точно същият проблем засяга организациите, които прилагат стандартите, но поне системата за управление им предоставя инструментите за идентифициране и реагиране на промените в информационните им рискове.

Други стандарти на ISO за системи за управление.

Стандартът ISO/IEC 27001 е набор от стандарти на ISO, които официално специфицират системи за управление. Други стандарти за системите за управление на ISO включват:

- ISO 9001 – за управление на качеството. Произтича от BS 5750 и преди това от подхода „Деминг“ за осигуряване на качеството и непрекъснато усъвършенстване (разглежда търговски, финансов, репутационен и други рискове, свързани с неспособността да се произвеждат стоки и услуги с постоянно високо качество).
- ISO 14001 – за управление на околната среда. Отнася се до съвместимостта, социалните и здравните рискове, свързани с изхвърлянето на отпадъчни води, замърсяването и др.
- ISO 50001 – за управление на енергията. Разглежда проблема с разходите, свързани с неефективното използване на енергията.
- ISO 45001 – за управление на здравето и безопасността на работното място (OHSAS 18001). Третира рискове, свързани с трудови злополуки и смъртни случаи, нездравословни и несигурни условия или практики за работа и др.

Всички стандарти за системи за управление на ISO определят управление на добри практики и подготовка, свързани със съответните им тематични области. Уилям Едуардс Деминг формулира основната идея, според която ръководството първо трябва да поеме контрола, за да оцени и при необходимост систематично да подобрява нещата. Информацията и метриките за управление са от жизненоважно значение заедно с изрично зададените от бизнеса, спрямо които да се измерва и оценява действителното изпълнение, както и управленските структури (като политики и дейности по спазване) да въвеждат или изпълняват необходимите промени за развитието на организацията.

Стандартите за системите за управление са формулирани изчерпателно и типово, така че организациите могат да изберат да бъдат сертифицирани в съответствие с тях от независими органи, в идеалния случай сертифициращи органи, които са надлежно акредитирани, като по този начин дават доверие, почтеност и смисъл на издаваните удостоверения. Организациите могат също да изберат да приемат стандартите, без да бъдат сертифицирани, въпреки че сертифицирането понякога се изисква от собствениците, властите, бизнес партньорите, законите или регламентите като средство за увеличаване на сигурността.

От 2012 г. насам всички стандарти на ISO за управление на системи се изграждат на базата на една и същаосновна структура и общи концепции, използвайки идентични текстове

и термини. Макар да се налагат компромиси, предимството на привеждането в съответствие е, че мениджърите, персоналът, специалистите и одиторите, които опознават всяка една система за управление, се запознават и с останалите, поне в концептуално отношение.

Съществуват и други предимства, като:

- интеграция между системите за управление и ефективност, например подобни форми и процеси и комбинирани одити;
- последователни управленски подходи и терминология;
- оставянето на бизнеса да управлява системите за управление, а не стандартите или специалистите.

Стандарти на ISO за системи за управление – общ преглед.

Следните стандарти за информационна сигурност ISO/IEC 27000 (стандартите ISO 27K) се публикуват или вече са публикувани: ISO/IEC 27000:2016, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC TR 27019:2013.

ISO/IEC 27000:2016, Информационни технологии. Техники за сигурност. Системи за управление на информационната сигурност. Общ преглед и речник.

ISO/IEC 27000 представя „общ преглед на системите за управление на информационната сигурност“ (и по този начин стандартите ISO 27000) и „определя свързани термини“ (речник, който официално и изрично дефинира много от специализираните термини, тъй като те се използват в стандартите ISO 27000).

Състояние на стандарта.

ISO/IEC 27000 е публикуван за първи път през 2009 г. и е актуализиран през 2012, 2014 и 2016 г.

Четвъртото издание (2016 г.) е налице като легитимно безплатно изтегляне на английски и френски език.

Проектът SC 27, поддържащ ISO/IEC 27000, също поддържа вътрешен постоянен документ (WG1 SD6) по терминологията.

ISMS/ISO 27000 – секция РЕЧНИК.

Речникът на внимателно формулираните официални определения обхваща повечето от термините за специализирана информационна сигурност, използвани в стандартите ISO 27000. Информационната сигурност, както и повечето технически обекти, използва сложна мрежа от термини, която постоянно се развива. Няколко основни термина в информационната сигурност (например риск) имат различни значения или интерпретации според контекста, намерението на автора и предразсъдъците на читателя. Малко автори се решават да дефинират точно какво означават, но такава двусмисленост не е особено полезна в областта на стандартите, тъй като води до объркване. Освен всичко друго би било неудобно да се оценява и удостоверява спазването на ISO/IEC 27001, ако специализираните термини означават различни неща за оценителите и оценяваните!

Речникът в ISO/IEC 27000 постепенно се разпространява в сферата на глобалната информационна сигурност, въпреки че някои личности и групи се разграничават, понякога с основателни причини, което води до недоразумения и противоречия. Дори да има несъгласие с определенията в Речника, препоръчително е той да се познава, тъй като някои от ~~вашите~~ професионалните партньори ще приемат ISO/IEC версиите.

ISO/IEC 27000 в голяма степен заменя ISO/IEC Guide 2:1996 „Стандартизация и свързаните с нея дейности. Общ терминологичен речник“, ISO Guide 73:2009 „Управление на риска. Лексикални указания за употреба в стандартите“ и ISO/IEC 2382-8 „Информационни технологии – речник. Част 8: Сигурност“. Той включва дефиниции, взети от няколко ISO стандарта, различни от ISO 27000. Текстовете, които са възпроизведени непроменени от други стандарти на ISO, като ISO 9000, невинаги са напълно подходящи в контекста на информационната сигурност. Те не са задължително използвани в стандартите ISO 27000 в пълно съответствие с първоначалните определения или предвидените значения. Въпреки това, тъй като определенията постепенно се актуализират или заместват, речникът се развива и е в добро състояние в целия пакет ISO 27000 – забележително постижение, като се имат предвид практическите трудности при координирането на усилията на отделни комитети, редактори и мениджъри, редактирането на проекти, и разработването на езика и концепциите в движение.

ISMS/ISO 27000 – секция ПРЕГЛЕД.

Прегледът на системите за управление на сигурността на информацията (ISMS) въвежда информационна сигурност, управление на риска и сигурността и системи за управление.

ISO/IEC 27001:2013, Информационни технологии. Техники за сигурност. Системи за управление на информационната сигурност. Изисквания.

ISO/IEC 27001 официално определя система за управление на сигурността на информацията като съвкупност от дейности, свързани с управлението на информационните рискове (наречени рискове за информационната сигурност в стандарта). ISMS е всеобхватна рамка за управление, чрез която организацията идентифицира, анализира и адресира информационните рискове. Системата ISMS гарантира, че мерките за сигурност са фиксирани, за да поддържат темпото в съответствие с промените в заплахите за сигурността, уязвимостта и бизнес въздействието – важен аспект в такава динамична област и ключово предимство на гъвкавия подход, основаващ се на риска на ISO 27000 в сравнение например с PCI-DSS.

Стандартът обхваща всички видове организации (търговски предприятия, правителствени агенции, нестопански организации), от всякакъв мащаб на дейност (от микропредприятия до огромни мултинационални компании) и всички отрасли или пазари (търговия на дребно, банково дело и др.).

ISO/IEC 27001 формално не налага специфичен контрол за сигурност на информацията, тъй като необходимите контроли се различава значително в широкия кръг организации, приемащи стандарта. Контролът за сигурност на информацията по ISO/IEC 27002 е отбелязан в приложение А към ISO/IEC 27001 като меню. Организациите, приели ISO/IEC 27001, могат да избират специфичните контроли за сигурност на информацията за конкретните информационни рискове от изброените в менюто видове контрол и потенциално ги допълват с други а ла карт опции. Както при ISO/IEC 27002 ключът при избора на приложим контрол е да се направи цялостна оценка на информационните рискове на организацията, която е един от жизненоважните елементи на системата за управление на информационната сигурност. Освен това ръководството може да избере да избегне, прехвърли или приеме информационни рискове, а не да ги смекчи чрез контрол – решение за третиране на риска в рамките на процеса на управление на риска.

Структура на стандарта.

ISO/IEC 27001:2013 има следните раздели:

0. Въведение – стандартът използва процесен подход.

1. Обхват – определя общи изисквания за ISMS (СУИС - системата за управление на информационната сигурност) подходящи за организации от всякакъв вид, мащаб или природа.

2. Нормативни препоръки – само ISO/IEC 27000 се смята за абсолютно задължителен за потребителите на 27001. Останалите стандарти ISO 27K са незадължителни.

3. Условия и дефиниции – кратък формализиран речник, който предстои да бъде заменен от ISO/IEC 27000.

4. Контекст на организацията – разбиране на организационния контекст, потребностите и очакванията на заинтересованите страни и определяне обхвата на СУИС. Раздел 4.4 ясно заявява, че „организацията създава, прилага, поддържа и непрекъснато подобрява“ съответстващата системата за управление на информационната сигурност.

5. Лидерство – висшият мениджмънт трябва да демонстрира лидерство и ангажираност към СУИС, и да определя ролите, отговорностите и органите за сигурност на информацията.

6. Планиране – очертава процеса на идентифициране, анализ и планиране на третирането на информационните рискове и изясняването на целите за информационна сигурност.

7. Подкрепа – трябва да бъдат назначени адекватни, компетентни ресурси, повишена информираност, подготвена и контролирана документация.

8. Операция – малко по-подробно за оценката и третирането на информационните рискове, управлението на промените и документирането на нещата (отчасти за да могат да бъдат одитирани от сертифициращите одитори).

9. Оценка на ефективността – наблюдение, измерване, анализ и оценка (одит), преглед на контрола, процесите и системата за управление на информацията, за да се направят системни подобрения, когато е уместно.

10. Подобряване – адресиране на резултатите от одита и прегледите (например несъответствия и коригиращи действия), непрекъснато усъвършенстване на системата за управление на информационната сигурност.

Приложение А, Референтни цели за контрол –от списък от заглавия на контролните секции в ISO/IEC 27002. Приложението е нормативно, което означава, че сертифицираните организации се очаква да го използват, но те са свободни да се отклоняват или да го допълват, за да отговорят на специфичните информационни рискове.

Библиография – включва петте свързани стандарта заедно с част 1 на директивите ISO/IEC, за повече информация. В допълнение ISO/IEC 27000 присъства в стандарта като нормативен (основен) стандарт и има няколко позовавания на ISO 31000 за управление на риска.

Задължителни изисквания за сертифициране.

ISO/IEC 27001 е формализирана спецификация за СУИС с две различни цели:

- определя на високо ниво какво може да направи дадена организация, за да въведе системата за управление на информационната сигурност ;
- може (по избор) да бъде използвана като основа за официална оценка на съответствието от акредитирани одитори за сертифициране, за да бъде сертифицирана организацията.

За сертифициране е изрично необходима следната задължителна документация (документирана информация в понятийния апарат на стандарта):

1. Обхват на СУИС (клауза 4.3).

2. Политика за сигурност на информацията (клауза 5.2).

3. Процес на оценка на информационния риск (клауза 6.1.2).

4. Процес на третиране на информационния риск (клауза 6.1.3).

5. Цели на информационната сигурност (клауза 6.2).

6. Доказателство за компетентността на хората, работещи в областта на информационната сигурност (клауза 7.2).

7. Други документи, свързани със СУИС, които организацията смята за необходими (клауза 7.5.1б).

8. Документи за оперативно планиране и контрол (клауза 8.1).

9. Резултати от оценките на риска (клауза 8.2).

10. Решения относно третирането на риска (клауза 8.3).

11. Доказателства за мониторинга и измерването на информационната сигурност (клауза 9.1).

12. Програма за вътрешен одит на СУИС и резултати от проведените одити (клауза 9.2).

13. Доказателства за прегледи от ръководството на СУИС (клауза 9.3).

14. Доказателство за установени несъответствия и възникнали коригиращи действия (клауза 10.1).

15. Различни други: Приложение А, което е нормативно, посочва, но не уточнява напълно допълнителната документация, включително правилата за приемливо използване на активите, политиката за контрол на достъпа, оперативните процедури, конфиденциалността или споразуменията за неоповестяване, взаимоотношенията с доставчиците, процедурите за реагиране при инциденти по сигурността на информацията, съответните закони, подзаконови актове и договорни задължения плюс свързаните с тях процедури за съответствие и процедурите за непрекъснатост на информацията.

Сертифициращите одитори почти сигурно ще проверят дали тези петнадесет вида документи са (а) налични и (б) подходящи за целта. Стандартът не уточнява точно каква трябва да бъде формата на документацията, но в раздел 7.5.2 се говори за аспекти като заглавия, автори, формати, медии, преглед и одобрение, докато раздел 7.5.3 се отнася до контрола на документите, което предполага сравнително формален стил тип ISO 9000. Електронните документи (като интранет страници) са също толкова добри, колкото хартиените, всъщност по-добри в смисъл, че са по-лесни за контролиране.

Обхват на системата за управление на информационната сигурност и декларация за приложимост (SoA).

Докато стандартът е предназначен да стимулира въвеждането на цялостна СУИС в организацията, като се гарантира, че всички ѝ структури се възползват, като се справят с информационните си рискове по подходящ и систематично управляван начин (клауза 4.3). Документиран обхват на СУИС е едно от задължителните изисквания за сертифициране.

Въпреки че декларацията за приложимост не е изрично определена, това е задължително изискване на раздел 6.1.3. Това често срещано понятие се отнася до резултатите от оценката на риска за информацията и по-специално до решенията за третиране на тези

рискове. Декларацията за приложимост може да бъде под формата на матрица, идентифицираща различните видове информационни рискове и вариантите за тяхното третиране и може би кой е отговорен за тях. Тя обикновено препраща към съответните контроли от ISO/IEC 27002, но организацията може да използва различна рамка, като NIST SP800-55, COBIT, стандарта ISF, BMIS или потребителски подход. Целите и инструментите за контрол на информационната сигурност от ISO/IEC 27002 са предоставени като контролен списък в приложение А, за да се избегне „пренебрегване на необходимите контролни инструменти“.

Обхватът на системата за управление на информационната сигурност и декларацията за приложимост е от решаващо значение, ако трета страна възнамерява да придаде някаква зависимост на сертификата за съответствие на организация ISO/IEC 27001. Ако в обхвата на ISO/IEC 27001 на организацията се отбелязва само „Acme Отдел X“, свързаният с нея сертификат не казва абсолютно нищо за състоянието на информационната сигурност в „Acme Отдел У“ ООД или „Acme Ltd. “ цяло. По подобен начин, ако по някаква причина ръководството реши да приеме рискове от злонамерен софтуер, без да прилага конвенционални антивирусни средства, одиторите могат да оспорят това решение. При условие обаче че свързаните с тях анализи и решения са правилни, това само по себе си не би било основание да се откаже сертифициране, тъй като антивирусните проверки не са задължителни.

Сертифициране.

Сертифицирането по ISO/IEC 27001 от акредитиран и уважаван сертифициращ орган е изцяло факултативно, но все повече се изисква от доставчици и бизнес партньори от организации, които са загрижени за сигурността на своята информация, както и на информацията в цялата верига за доставки или комуникационни и информационни мрежи.

Според проучване на ISO от 2016 г. в световен мащаб има над 33 000 сертификата по ISO/IEC 27001, около 20% повече годишно.

Сертифицирането носи редица предимства, които надхвърлят простото съответствие по същия начин, по който сертификатът по серия ISO 9000 казва повече, отколкото „ние сме организация с качество“. Независимата оценка задължително дава известна строгост и формалност на процеса на внедряване (което предполага подобрение на информационната сигурност и всички ползи и съответно намаляване на риска) и неизменно изисква одобрението на висшето ръководство (което е предимство най-малкото в областта на осведомеността за сигурността).

Сертификатът има маркетингов потенциал и показва, че организацията се отнася сериозно към управлението на информационната сигурност. Въпреки това, както беше посочено, стойността на удостоверението за сигурност силно зависи от обхвата на СУИС и SoA, с други думи, не се доверявайте прекалено много на сертификата за съответствие ISO/IEC 27001 на организацията, ако сте силно зависими от нейната информационна сигурност. Както сертифицираното съответствие с PCI-DSS не означава „гарантираме да защитаваме данни за кредитни карти и друга лична информация“, така сертифицираното съответствие със стандарта ISO/IEC 27001 е положителен знак, но не и твърда гаранция за информационната сигурност на организацията. В него се казва „разполагаме със съответстваща СУИС на място“, а не „ние сме сигурни“. Това е важно разграничение.

Състояние на стандарта.

ISO/IEC 27001 е напълно пренаписан и издаден отново през септември 2013 г. Това е много повече от промяна на съдържанието на изданието от 2005 г., тъй като ISO/IEC JTC1 настоява за съществени промени, за да се приведе стандартът в съответствие с други стандарти за системи за управление, опазването на околната среда и т.н. Идеята е, че мениджърите, запознати с някоя от системите за управление на ISO, ще разберат основните принципи на системата за управление на информационната сигурност. Концепции като сертифициране, политика, несъответствие, контрол на документи, вътрешен одит и прегледи от ръководството са общи за всички стандарти на системите за управление и процесите в голяма степен могат да бъдат стандартизирани в рамките на организацията.

ISO/IEC 27001:2013 вече се предлага от обичайните търговски обекти.

ISO/IEC 27002 е обновен и преиздаден, поради което и приложение А към ISO/IEC 27001 е напълно актуализирано (вижте страницата ISO/IEC 27002 за повече информация).

Техническа поправка, публикувана през октомври 2014 г., пояснява, че информацията в крайна сметка е актив. През декември 2015 г. е публикувана втора техническа поправка, според която организациите са официално задължени да идентифицират състоянието на изпълнението на контрола за сигурност на информацията в декларация за приложимост.

ISO/IEC 27002:2013, Информационни технологии. Техники за сигурност. Кодекс за практика за контрол на информационната сигурност

Обхват на стандарта.

Подобно на управлението на риска управлението на информационната сигурност е широкообхватна тема с влияние във всички организации. Информационната сигурност и следователно ISO/IEC 27002 са от значение за всички видове организации, включително търговски предприятия от всякакъв мащаб (от еднолични търговци до многонационални гиганти), нестопански организации, благотворителни организации, правителствени служби и квазиавтономни органи – всъщност всяка организация, която работи със и зависи от информацията. Специфичните изисквания за информационен риск и контрол на информацията могат да се различават в подробности, но имат много общи основания. Например повечето организации трябва да се справят с информационните рискове, свързани с техните служители плюс изпълнителите, консултантите и външните доставчици на информационни услуги.

Стандартът изрично се занимава с информационната сигурност, което означава сигурността на всички форми на информация (компютърни данни, документация, знания и интелектуална собственост), а не само компютърна сигурност или киберсигурност, както е популярно днес.

Връзка с ISO/IEC 27001.

ISO/IEC 27001 официално определя задължителните изисквания за система за управление на информационната сигурност. Той използва стандарт ISO/IEC 27002, за да посочи подходящ контрол за сигурност на информацията в системата за управление на безопасността, но тъй като ISO/IEC 27002 е кодекс на практика/насока, а не стандарт за сертифициране, организациите са свободни да избират и прилагат други контроли, пълни комплекти от контроли за сигурност на информацията, които смятат за подходящи. ISO/IEC 27001 включва обобщение (всъщност малко повече от заглавията на разделите) на контролите

от стандарт ISO/IEC 27002 в приложение А. По принцип повечето организации, които приемат ISO/IEC 27001, също приемат ISO/IEC 27002.

Структура и формат на ISO/IEC 27002:2013.

ISO/IEC 27002 е кодекс на практиката – общ консултативен документ, а не формална спецификация като ISO/IEC 27001. Той препоръчва контрол на информационната сигурност, насочен към целите на контрола на информационната сигурност, произтичащи от рискове за поверителността, целостта и достъпността на информацията. Организациите, приели стандарт ISO/IEC 27002, трябва да оценят собствените си информационни рискове, да изяснят своите контролни цели и да прилагат подходящ контрол (или дори други форми на третиране на риска), като използват стандарта за ориентиране.

Стандартът е структуриран логически около групи, свързани с контрола за сигурност. Много контроли биха могли да бъдат поставени в няколко раздела, но за да се избегнат дублирането и конфликтите, те произволно са присвоени на един, а в някои случаи кръстосани от другаде. Например система за контрол на достъпа чрез карта, компютърна зала или архив/сейф са както контрол на достъпа, така и физически контрол, който включва технология и свързаните с нея процедури и политики за управление/администриране и използване. Това поражда двусмислици (например раздел 6.2 за мобилните устройства и работата по телефона, които са част от раздел 6 за организацията на информационната сигурност), но поне е разумна цялостна структура. Тя може да не е перфектна, но е достатъчно добра като цяло.

Съдържание на ISO/IEC 27002:2013.

Съдържанието на стандарта е разпределено в 19 раздела (21, ако се включат предговорът и библиографията).

Предговор – накратко се представят ISO/IEC JTC1/SC 27, комисията, написала стандарта, и се отбелязва, че това „второ издание отменя и заменя първото издание (ISO/IEC 27002:2005), което е технически и структурно преработено“.

Раздел 0. Въведение – представя историята, споменава три източника на изисквания за сигурност на информацията, отбелязва, че стандартът предлага общи и потенциално непълни указания, които трябва да бъдат интерпретирани в контекста на организацията, показва жизнения цикъл на информацията и информационната система и посочва ISO/IEC 27000 за цялостната структура и речник за ISO 27K.

Раздел 1. Обхват – стандартът дава препоръки на тези, които отговарят за избора, внедряването и управлението на информационната сигурност. Тя може или не може да бъде използвана в подкрепа на СУИС, посочена в ISO/IEC 27001.

Раздел 2. Нормативни позовавания – ISO/IEC 27000 е единственият стандарт, смятан за абсолютно необходим за използването на ISO/IEC 27002. В стандарта обаче са посочени различни други стандарти и има библиография.

Раздел 3. Условия и определения – всички специализирани термини и дефиниции са дефинирани в ISO/IEC 27000 и най-много се прилагат в цялото семейство стандарти ISO 27K.

Раздел 4: Структура – клаузи за контрол на сигурността. От 21 раздела на стандарта 14 посочват контролните цели и контролите. Тези 14 раздела са клаузите за контрол на сигурността. Всяка клауза за контрол има стандартна структура: един или повече подраздели от първо ниво, като всеки посочва цел на контрола и всяка цел на контрола се подпомага от

една или повече декларирани контроли, всеки контрол, последван от свързаните с тях инструкции за прилагане и в някои случаи допълнителни обяснителни бележки.

ISO/IEC 27002 определя около 35 контролни цели (по една за „категория за контрол на сигурност“), отнасящи се до необходимостта от защита на поверителността, целостта и наличието на информация. Контролните цели са на доста високо ниво и съдържат спецификации за общи функционални изисквания за архитектурата на организацията за управление на информационната сигурност. Малко професионалисти биха оспорили сериозно валидността на целите на контрола, т.е. би било трудно да се твърди, че дадена организация не трябва да отговаря на поставените цели на контрола като цяло. Някои цели на контрола обаче не са приложими във всички случаи и е малко вероятно тяхното общо формулиране да отразява точните изисквания на всяка организация, особено предвид многообразието от организации и отрасли, за които се прилага стандартът. Ето защо ISO/IEC 27001 изисква декларация за приложимост (SoA), която ясно посочва кои контроли за информационна сигурност се или не се изискват от организацията, както и тяхното състояние на изпълнение.

Всяка от целите на контрола се поддържа от поне един контрол, като общо са 114. Въпреки това заглавието е донякъде подвеждащо, тъй като ръководството за изпълнение препоръчва многобройни действителни контроли в детайлите. Контролната цел, свързана с относително простия подраздел 9.4.2. Процедури за сигурност при влизане, например се поддържа чрез избиране, прилагане и използване на подходящи техники за удостоверяване, като не се разкрива чувствителна информация при влизане, валидиране на входни данни, защита срещу брут форс атаки, логване, непредставяне на пароли в мрежата, времеви ограничения на сесия при неактивност и ограничения във времето за достъп, независимо дали това се приема за един или няколко контрола. Може да се твърди, че ISO/IEC 27002 препоръчва буквално стотици отделни контроли за сигурност на информацията, въпреки че някои поддържат множество цели на контрола, с други думи, някои контроли имат няколко цели. Освен това формулировката в целия стандарт ясно заявява, че това не е напълно изчерпателен набор. Организацията може да има леко различни или изцяло нови цели за контрол на информационната сигурност, които изискват други контроли (понякога известни като набор за разширено контролиране) вместо посочените в стандарта или в допълнение към тях.

Раздел 5. Политика за информационна сигурност.

5.1. Управление на информационната сигурност – ръководството трябва да определи набор от политики, за да изясни посоката и поддръжката за сигурността на информацията. На първо ниво трябва да има цялостна политика за информационна сигурност, както е посочено в ISO/IEC 27001, точка 5.2.

Раздел 6. Организация на информационната сигурност.

6.1. Вътрешна организация – организацията трябва да очертае ролите и отговорностите за сигурността на информацията и да ги разпредели между персонала. Където е уместно, задълженията следва да бъдат разделени на роли и лица, за да се избегнат конфликти на интереси и да се предотвратят неподходящи дейности. Необходимо е да има контакти със съответните външни органи (CERT и специални групи по интереси) по въпросите на информационната сигурност. Информационната сигурност трябва да бъде неразделна част от управлението на всички видове проекти.

6.2. Мобилни устройства и работа от разстояние – изисква се да има политики за сигурност и контрол за мобилни устройства (лаптопи, таблетни компютри, носими ICT устройства, смартфони, USB устройства и други) и телеработа (домашна работа, работа от дома, виртуални работни места).

Раздел 7: Сигурност на човешките ресурси.

7.1. Преди наемане на работа – отговорностите за сигурността на информацията следва да бъдат взети предвид при наемането на постоянни служители, изпълнители и временно наети служители (например чрез подходящи длъжностни характеристики, проверка преди наемане на работа) и включени в договорите (например условия на заетост и други подписани споразумения, определящи ролите и отговорностите по сигурността, задължения за спазване и т.н.).

7.2. По време на работа – мениджърите трябва да гарантират, че служителите и изпълнителите са информирани и мотивирани да спазват своите задължения за информационна сигурност. Официалният дисциплинарен процес е необходим, за да се справят с инциденти, свързани с сигурността на информацията, за които се твърди.

7.3. Прекратяване и промяна на заетостта – следва да се управляват аспектите на сигурността при напускането на организацията от работника или значителни при промени в нейните роли.

Раздел 8. Управление на активи.

8.1. Отговорност за активите – необходимо е всички информационни активи да бъдат инвентаризирани и собствениците да бъдат идентифицирани, за да бъдат държани отговорни за тяхната сигурност. Трябва да се определят политиките за приемливо използване и активите да се връщат, когато някой напуска организацията.

8.2. Класификация на информацията – информацията трябва да бъде класифицирана и етикетирана от нейните собственици в съответствие с необходимата защита и да се борави адекватно с нея.

8.3. Работа с медиите – средствата за съхраняване на информация трябва да бъдат управлявани, контролирани, премествани и изхвърляни по такъв начин, че информационното съдържание да не бъде компрометирано.

Раздел 9: Контрол на достъпа.

9.1. Бизнес изисквания за контрол на достъпа – изискванията на организацията за контролиране на достъпа до информационни активи трябва да бъдат ясно документирани в политиката и процедурите за контрол на достъпа. Мрежовият достъп и връзките трябва да бъдат ограничени.

9.2. Управление на достъпа за потребители – разпределението на правата за достъп на потребителите следва да се контролира от първоначалната регистрация на потребителя до премахването на правата за достъп, когато вече не се изисква, включително специални ограничения за привилегировани права за достъп и управление на пароли (тайна информация за автентификация), актуализации на правата за достъп.

9.3. Отговорности на потребителя – потребителите трябва да бъдат осведомени за отговорностите им за поддържане на ефективен контрол на достъпа, например избирайки силни пароли и запазвайки ги поверителни.

9.4. Контрол на достъпа до системата и приложението – достъпът до информация трябва да бъде ограничен в съответствие с правилата за контрол на достъпа например чрез сигурно влизане, управление на пароли, контрол на привилегировани помощни програми и ограничен достъп до програмен код.

Раздел 10. Криптография.

10.1. Криптографски контроли – необходимо е да има политика за използването на криптиране и криптографски контрол на автентичността и целостта, като цифрови подписи и кодове за разпознаване на съобщения и управление на криптографски ключове.

Раздел 11. Физическа и екологична сигурност.

11.1. Защитени зони – определените физически периметри и бариери с физически контрол и работни процедури трябва да защитават помещенията, офисите, зоните за доставка/зареждане и др. от неразрешен достъп. Следва да се потърси съвет от специалисти по отношение на защитата от пожари, наводнения, земетресения, бомби и т.н.

11.2. Оборудване – трябва да се осигури и поддържа оборудване (най-вече за информационни и комуникационни технологии) заедно с помощни комунални услуги (като електричество и климатизация) и окабеляване. Оборудването и информацията не трябва да се изнасят от защитеното място, освен ако не са разрешени, и трябва да бъдат адекватно защитени както на място, така и извън него. Информацията от оборудването трябва да бъде унищожена, преди то да се изхвърли или да се използва повторно. Необслужваното оборудване трябва да бъде защитено и трябва да има политики „чисто бюро“ и „чист екран“.

Раздел 12. Сигурност на операциите.

12.1. Оперативни процедури и отговорности – работните отговорности и процедурите по ИТ трябва да бъдат документирани. Трябва да се контролират промените в информационните съоръжения и системи. Капацитетът и ефективността трябва да се управляват. Системите за разработване, изпитване и експлоатация трябва да бъдат разделени.

12.2. Защита от злонамерен софтуер – необходими са контроли за злонамерен софтуер, включително информираност на потребителите

12.3. Архивиране – подходящите резервни копия трябва да бъдат взети и задържани в съответствие с политика за резервиране.

12.4. Проучване и мониторинг – действията на системния потребител и администратора/оператора, изключенията, грешките и събитията за сигурност на информацията трябва да бъдат записани и защитени. Часовниците трябва да бъдат синхронизирани.

12.5. Контрол на оперативния софтуер – инсталирането на софтуер на операционни системи трябва да се контролира.

12.6. Управление на техническите уязвимости – техническите уязвимости трябва да бъдат коригирани и трябва да има правила, уреждащи инсталирането на софтуер от потребителите.

12.7. Съображения за одит на информационните системи – ИТ одитите трябва да бъдат планирани и контролирани, за да се сведат до минимум неблагоприятните ефекти върху производствените системи или неподходящият достъп до данните.

13. Комуникационна сигурност.

13.1. Управление на мрежовата сигурност – мрежите и мрежовите услуги трябва да бъдат осигурени например чрез сегрегация.

13.2. Обмен на информация – трябва да има политики, процедури и споразумения (като споразумения за неразкриване на информация) относно прехвърлянето на информация към/от трети страни, включително електронни съобщения.

Раздел 14. Система за придобиване, разработване и поддръжка.

14.1. Изисквания за сигурност на информационните системи – трябва да се анализират и уточнят изискванията за контрол на сигурността, включително уебприложения и трансакции.

14.2. Сигурност в процесите на развитие и подкрепа – правилата за сигурния софтуер/разработване на системи трябва да се определят като политика. Промените в системите (както на приложенията, така и на операционните системи) трябва да бъдат контролирани. Софтуерните пакети в идеалния случай не трябва да се променят и трябва да се следват защитените принципи на системното инженерство. Следва да се осигури средата за развитие и да се контролира развитието на външни изпълнители. Сигурността на системата трябва да бъде тествана и критериите за приемане да бъдат определени така, че да включват аспекти на сигурността.

14.3. Тестови данни – тестовите данни трябва да бъдат внимателно подбрани/генерирани и контролирани.

15. Връзки с доставчиците.

15.1. Информационна сигурност в отношенията с доставчиците – трябва да има политики, процедури, осведоменост и т.н., за да се защити информацията на организацията, която е достъпна за ИТ аутсорсистите и други външни доставчици по цялата верига на доставки, договорена в рамките на договорите или споразуменията.

15.2. Управление на доставчиците на услуги – извършването на услуги от външни доставчици следва да бъде наблюдавано и преразглеждано/одитирано по договори/споразумения. Промените в услугите трябва да бъдат контролирани. (Същото важи и за услугите, предоставяни от вътрешните доставчици!)

Раздел 16. Управление на инциденти по сигурността на информацията.

16.1. Управление на инциденти и подобрения в информационната сигурност – трябва да има отговорности и процедури, които да управляват (докладват, оценяват, отговарят и да се учат) събития, инциденти и слабости по сигурността на информацията последователно и ефективно и да събират съдебни доказателства.

Раздел 17. Аспекти на сигурността на информацията в управлението на непрекъснатостта на бизнеса.

17.1. Непрекъснатост на информационната сигурност – непрекъснатостта на информационната сигурност трябва да бъде планирана, приложена и преразгледана като неразделна част от системите за управление на непрекъснатостта на организацията.

17.2. Резервиране – ИТ съоръженията трябва да имат достатъчно резервиране, за да удовлетворят изискванията за наличност.

Раздел 18. Съответствие.

18.1. Съответствие с правни и договорни изисквания – организацията трябва да идентифицира и документира задълженията си към външни органи и други трети страни по

отношение на информационната сигурност, включително интелектуална собственост, (бизнес) записи, лична информация и криптография.

18.2. Прегледи за сигурността на информацията – разпоредбите за организацията в областта на информационната сигурност следва да бъдат независимо прегледани (одитирани) и докладвани на ръководството. Мениджърите трябва също редовно да преглеждат спазването им от страна на служителите, процедурите за сигурност и т.н. и да предприемат коригиращи действия, когато е необходимо.

Библиография.

Стандартът завършва със списък от 27 (!) съответни стандарта ISO/IEC, повече от половината от които са други стандарти ISO 27K.

Състояние на стандарта.

Стандартът в момента се преработва, за да отрази промените в информационната сигурност – появата на BYOD, облачните технологии, виртуализацията, crypto-ransomware, социалните мрежи, например Pocket ICT и IoT. Вместо директно да направи актуализациите, SC 27 отново преразглежда цялата структура на стандарта. В момента се разглеждат паралелно два подхода:

1. Контролите ще бъдат групирани в теми, които образуват клаузи в основното тяло на стандарта, и ще бъдат маркирани с атрибути, които могат да бъдат използвани за избор от тях (например превантивни контроли). Ще бъде осигурен набор от приложения, като се избират контроли, използващи различни маркери.

2. Основното тяло на стандарта ще предложи няколко гледни точки, които представят различни класификации или групи от контроли за сигурност на информацията според техните етикети, като самото маркиране на контролите е изложено в приложението.

Съществуващите контроли вероятно ще бъдат прегледани и може би пренаписани, като се имат предвид различните контексти. Те могат също да бъдат консолидирани, докато поддържащите контроли могат да бъдат идентифицирани като такива.

ISO/IEC TR 27019:2013, Информационни технологии. Техники за сигурност. Насоки за управление на информационната сигурност въз основа на ISO/IEC 27002 за системи за управление на процеси, специфични за сектора на енергетиката.

Въведение.

Този стандарт (технически доклад) има за цел да помогне на организациите в енергийната индустрия да интерпретират и прилагат ISO/IEC 27002:2005, за да осигурят своите електронни системи за управление на процесите.

Обхват и цел.

Въвеждането на проекта на стандарта гласи: „В центъра на приложението на този документ са системите и мрежите за контрол и надзор на производството, преноса и разпределението на електроенергия, газ и топлина в комбинация с контрола на поддържащите процеси. Това включва системи за управление и автоматизация, системи за защита и безопасност и системи за измерване, включително свързаните с тях комуникационни и телеконтролни приложения“.

Управлението на информационната сигурност представя фундаментално същите предизвикателства, свързани с управлението на риска във всички контексти, но характерът на системите за контрол на процесите в реално време и безопасността и екологичната критичност

правят някои от предизвикателствата особено критични за организациите в енергийната индустрия. Следователно стандартът предоставя допълнителни, по-конкретни указания за управление на информационната сигурност, отколкото общите и познати съвети, предоставени от ISO/IEC 27002.

Структура и съдържание.

Стандартът е развит от германския стандарт DIN SPEC 27009:2012-04, който се основава на ISO/IEC 27002:2005. Той следва стриктно структурата на ISO/IEC 27002, като предоставя допълнителни насоки, когато това е уместно.

Необходимо е да се подчертае, че ISO/IEC TR 27019 трябва да се използва заедно с ISO/IEC 27002, тъй като не включва неговото съдържание. Други стандарти на ISO 27K също се препоръчват да се изпълнят в по-широк контекст, например ISO/IEC 27001 за всеобхватна система за управление на информационната сигурност, която включва контрола на процесите, както и общите търговски системи, мрежи и процеси заедно с ISO/IEC 27005 за практики за управление на информационния риск.

Коментари.

Глобалната енергийна индустрия има висока култура на безопасност, тъй като физическите въздействия, предизвикани от експлозии, разливи на нефт и химикали, радиоактивни изхвърляния и т.н. са очевидни (Бопал, Чернобил, Ексон Валдиз, Мексиканският залив, Фукушима). Индустрията също така е подробно осведомена за своите екологични задължения както по отношение на собствените си операции, така и по отношение на въздействието на някои от продуктите надолу по веригата. Освен това индустрията има висока култура на физическа и информационна сигурност поради значителните рискове, произтичащи от:

- Заплахи като природни бедствия, умишлени атаки (саботаж) от хакери, зловреден софтуер, социален инженеринг, терористи, вътрешни лица, групи на натиск и чужди държави, както и заплахи от произшествия, конкуренти, електромеханични повреди, злонамерен софтуер и др.
- Уязвимости, присъщи на техните системи и процеси. Системите за управление на процесите, които са свързани по някакъв начин, изложени са на достъп до интернет или други мрежи, са уязвими от пълната гама киберзаплахи, включително произтичащи от проектантски слабости и програмни грешки особено ако не са добре проектирани, управлявани и поддържани (например стабилизирането на сигурността е предизвикателство за критичните за безопасността системи).
- Въздействия, по-специално ограничена наличност и/или цялост на критичната за бизнеса или безопасността информация, водеща до прекъсвания на доставките (прекъсвания на захранването), доставки извън спецификацията (например доставки над/под напрежение) на огромни количества енергия и екологични инциденти (например изтичане на петрол/газ/химикали). Организациите от енергийния сектор, както публични, така и частни, обикновено се класифицират като част от критичните национални инфраструктури поради очевидното им стратегическо значение.

Състояние на стандарта.

Стандартът е публикуван през 2013 г. с бързото приемане на DIN SPEC 27009:2012-04.

Проектът за ревизия е в процес на хармонизиране на 27019 с версиите на ISO/IEC 27001 и 27002 плюс IEC TC 57, IEC TC 65 (IEC 62443-2-1) и IEC SC45A (IEC 62645). Публикуването на стандарта би трябвало вече да е факт.

Редакторите предлагат обединяването на проекта с IEC 62443-2-1, за да се избегне ненужно дублиране, водещо до двойно номериран стандарт.

Състояние: ревизията е на етап FDIS. Това ще стане пълен международен стандарт. Обхватът ще включва генериране, съхранение, пренос и разпределение на електроенергия, газ, нефт и топлинна енергия, но не ядрена енергия (изрично изключване). Той ще има ново заглавие: „Управление на сигурността на информацията за индустрията за енергийни услуги“. Ревизията е на път да бъде публикувана в края на 2017 г.

Нови контролни инструмента в ISO 27019 са:

- физическа охрана;
- управление на мрежовата сигурност;
- управление на комуникации и операции;
- контрол за достъп до мрежата;
- управление на бизнес непрекъснатост.

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ЕМВ	електромагнитни вълни
ЕМИ	електромагнитни излъчвания
ЕМП	електромагнитни импулси
ИС	информационна система
ИТ	информационни технологии
КИС	комуникационно-информационна система
ЛВР	лице, вземащо решение
РС	персонален компютър
СМО	система за масово обслужване
СУЗ	система за управление на знания
СУИС	система за управление на информационната сигурност
СУ	система за управление
ЦРК	център за разпределение на ключовете
C2	Command and Control
DoS	Denial of Service
C4I	Command, Control, Communications, Computers and Intelligence
FCS	Future Combat Systems
GPS	Global Positioning System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ICMP	Internet Control Message Protocol
KMS	Key Management System
NIST	National Institute of Standards and Technology
NIDS	Network Intrusion Detection Systems
NIPS	Network Intrusion Prevention Systems
PKI	Public Key Infrastructure
RTUs	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
UML	Unified Modeling Language
UDP	User Datagram Protocol

БИБЛИОГРАФИЯ

1. Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria – Orange Book. https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

2. Dexter, John. The Cyber Security Management System: A Conceptual Mapping. // The SANS Institute, 2002. https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591

3. Пандов, Емил. Организация на киберзащитата в Българската армия. – публикация ВА – 2012 г.

4. A CERT-UK PUBLICATION, 2014. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Denial-of-service-attacks-what-you-need-to-know1.pdf

5. DDoS Attack Types: Glossary of Terms. // Corero. https://www.corero.com/pdf/DDoS%20Glossary%20of%20Terms.pdf

6. The Top 10 DDoS Attack Trends. // Imperva, 2015. https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf

7. Хофман, Л. Современние методи защити информации. Москва: Советское радио, 1982.

8. Сапунджиев, Георги. Вземане на решение в системите за управление. София: ТУ, 1998.

9. Aminzade, Michael. Risk Assessment: The First Step in Improving Cyber Security. // HELPNETSECURUTY, 2017. https://www.helpnetsecurity.com/2017/11/13/risk-assessment/

10. Häring, Ivo. Risk Analysis and Management: Engineering Resilience. Springer, 2015.

11. NIST Special Publication 800-53. Revision 4, 2015.

12. Шепитько, Григорий. Теория информационной безопасности и методология защиты информации. Москва: РГСУ, 2012.

13. https://inductiveautomation.com/what-is-scada

14. TALES “Cyber Security for SCADA Systems”. Autumn 2013. https://www.thalesgroup.com/sites/default/files/asset/document/thales-cyber-security-for-scada-systems.pdf (към месец май 2018 г.)

15. http://sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf

16. https://www.infosecwriters.com/Papers/CGates_TEMPEST.pdf

17. Barakat, Mohamed, Christian Eder, Timo Hanke. An Introduction to Cryptography. University of Kaiserslautern, 2018. http://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf

18. Адигеев, Михаил. Введение в криптографию. Ростов-на-Дону: Издательство Ростовский государственный университет, 2002. http://www.ict.edu.ru/ft/004793/Crypto-1.pdf

19. Barker, Elaine, Miles Smid, Dennis Branstad, Santosh Chokhani. NIST Special Publication 800-130 – “A Framework for Designing Cryptographic Key Management Systems”. August 2013. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-130.pdf

20. Menezes, Alfred, Paul van Oorschot, and Scott Vanstone. Handbook of Applied Cryptography. CRC Press, 1996. http://cacr.uwaterloo.ca/hac/about/chap13.pdf

21. Cybersecurity Framework, Version 1.0, 2014.
22. ISO/IEC 27001:2013.
23. ISO/IEC 27004:2016.

Камен Калчев
Костадин Цветков

КИБЕРСИГУРНОСТ

Българска
Първо издание

Редактор
Пенка Димитрова

Печат – Военна академия „Г. С. Раковски“

ISBN 978-619-7478-90-7