Establishing effective Information Security Management System in public administration through ISO 27001:2005

Kiril Anguelov[1]

Изграждане на ефективна Система за управление на информационната сигурност в публичната администрация посредством ISO 27001:2005

Кирил Ангелов[1]

Abstract. The paper analyses the possibilities of optimization of the organization and management of the information security of unclassified information in the public administration. The author considers the nature and significance of the problem, the influencing factors of the decision and makes concrete proposals to establish an effective Information Security Management System, based on the international standard ISO 27001:2005.

Key words: information security, Information Security Management Systems, ISO 27001:2005.

Анотация. В изследването се анализират възможностите за оптимизация на организацията и управлението на информационната сигурност на некласифицирана информация в публичната администрация. Разглеждат се последователно: същността и значимостта на проблема, влияещите на решението фактори и се правят конкретни предложения изграждане на ефективна система за управление на информационната сигурност основана на международния стандарт ISO 27001:2005.

Ключови думи: информационна сигурност, системи за управление на информационната сигурност, ISO 27001:2005.

I. СЪШНОСТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ПУБЛИЧНАТА АДМИНИСТРАЦИЯ

Информационната сигурност се дефинира като аспект на националната сигурност, като от гледна точка на Закона за електронното управление тя придобива следното измерение: защита на информационните масиви за служебно ползване в публичната администрация от неоторизиран достъп, осигуряване на висока степен на надеждност на изпълнението на операциите с информация и гарантиране на оперативна съвместимост между различните администрации при изпълнение на общи **АДМИНИСТРАТИВНИ** процеси. Неоторизираният достъп може да има следните последици:

1. Незаконно придобиване на информация, с цел използването й във вреда на обществото. Много често корупцията е свързана директно с „търговия" със служебна информация на длъжностни лица. Вредите за обществото от нерегламентираното придобиване на служебна информация са очевидни, като има проекции във всяка сфера на обществена дейност: от националната сигурност до извършване на административна услуга в община. При управлението на фондове и програми финансирани със средства от националния бюджет и от ЕС, корупционният натиск за получаване на служебна информация е засилен, с оглед на големите предимства, което би имало физическо или юридическо лице, разполагащо с нея.

[1]Кирил Ангелов, доц. д-р ик.н., ТУ-София, Стопански факултет, катедра Икономика, индустриален инженеринг и мениджмънт

Придобиването на неоторизирана информация от участник в търг за възлагане на обществена поръчка от самосебе си опорочава цялата процедура. „Търговията" със служебна информация в митниците се отразява на националната сигурност посредством силно намалените постъпления от данъци (възстановяване на Данък добавена стойност), такси и акцизи. Не може да бъде подмината и опасността от рекет над физически и юридически лица, вследствие запознаване с тяхното имуществено и финансово състояние.

2. Незаконно заличаване на информация от информационните масиви. Най-често тази корупция е свързана с премахване от базите данни на администрацията на информация за нарушение или престъпления на физически и юридически лица.

3. Незаконно редактиране или добавяне на информация в информационните масиви. Неоторизираното редактиране на служебна информация има за цел да бъде заблудена администрацията за действителното състояние на даден обект на интерес, като се добавят неверни данни или обстоятелства. Промяната на данните в

базите на администрациите, управляващи фондове и програми, може да резултира в:

- допускане до участие на кандидат-бенефициенти без правно основание;
- завишаване на оценката на даден кандидат бенефициент, и класирането на проекта му за финансиране;
- реализиране на многократно финансиране на една и съща дейност, извършена от един бенефициент;
- опорочаване на процедурата по мониторинг и др.

4. Незаконното забавяне на актуализацията на информационните масиви. Резултатът от тази дейност е аналогичен на предишните две. Очевидно само въз основа на пълна и актуална информация могат да бъдат вземани компетентни управленски решения.

Закона за електронното управление поставя принципно нови изисквания към начина на извършване на документооборота в публичната администрация в следните три направления:

1. Предоставянето на административни услуги, насочени към гражданите и юридическите лица с използване на съвременни информационни и комуникационни технологии ИКТ (релации администрация – граждани и администрация – юридически лица);
2. Спецификата при работата с електронни документи в рамките на една администрация;
3. Изискванията при взаимодействието между структури на администрацията (релация администрация – администрация).

Начинът за осъществяване на информирането и/или комуникацията дефинират четири групи електронни административни услуги (информиране, еднопосочно взаимодействие, асинхронно двупосочно взаимодействие и синхронно двупосочно взаимодействие [1]), които от своя страна предявяват специфични организационно-технически изисквания пред информационните и комуникационните системи на администрациите.

Друга особеност е изискването за еднократно събиране и създаване на данни от физическите и юридическите лица. Публичната администрация, в лицето на административен орган, който по силата на закон събира или създава данни за физически или юридически лица за първи път и изменя или заличава тези данни, може да изисква еднократно предоставяне на дадена информация, като тя се използва при предоставяне на административни услуги. Последното законово регламентирано изискване [7, чл.2] рефлектира на потребността от интензивен информационен обмен между различните администрации, респективно техните информационни и комуникационни системи. Засиленият информационен обмен при липса определена степен на надежност на информационните и комуникационните системи и оперативна съвместимост може да рефлектира в различни неблагоприятни явления като например пренос на уязвимост от една система в друга или блокиране на електронна административна услуга на една система при нарушена достъпност на друга и т.н.

Друг постулат електронното управление е създаване на организационно-управленски възможности за ускоряването на административните процеси и в частност на предоставянето на електронни административни услуги. Ускоряването на административните процеси не може да се реализира за сметка на загуба на конфиденцялност, а обратно в условия на засилена информационна сигурност.

Изброените принципно нови изисквания водят до нови значително по-високи изисквания към информационната сигурност в държавната администрация при работа с некласифицирана информация. Тези изисквания са в следните две насоки:

1. Осигуряването на висока степен на надеждност на изпълнението на операциите с информация.
2. Осигуряване на оперативна съвместимост между различните администрации при изпълнение на общи административни процеси.

Необходимостта от създаване на Система за управление на информационната сигурност произтича от една страна от наличието на нормативни документи, насочени към сигурността на информацията (Закон за защита на класифицираната информация, Закон за защита на личните данни и др.) и от нарасналия обществен интерес от запазване на конфиденцялност на класифицирана и част от некласифицираната информация. Понастоящем с разрастването от една страна на компютърните измами и световната конкуренция, а от друга на международния тероръзм все повече нараства значимостта на изграждане на ефективна и ефикасна система за управление на защитата на информацията.

II. Осигуряване на информационната сигурност в администрацията въз основа на ISO 27001:2005

Осигуряването на информационната сигурност в административни организации има три взаимнодопълващи се аспекти:

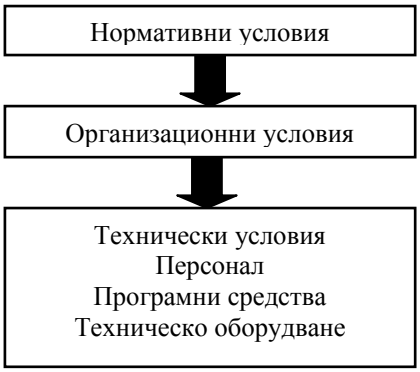
1. Осигуряване на конфиденциалност на информацията.
2. Осигуряване на достъпността до информацията.
3. Осигуряване на актуалност и цялостност на информацията.

Първият аспект е свързан със защита на базите от данни от нерегламентиран достъп и възпрепятства незаконното придобиване на информация. Вторият осигурява ползването на информационните масиви от служителите в администрацията, съобразно с техните компетенции. Третият аспект е свързан със средствата срещу незаконното заличаване или редактиране на данни и със забавяне актуализацията на информационните масиви. За да бъдат гарантирани тези аспекти на информационната

сигурност в администрацията е необходимо изпълнението на взаимообвързани условия (фигура 1):

1. Нормативни условия – закони, постановления на Министерски съвет и наредби, формиращи нормативната рамка в Република България по осигуряване на информационната сигурност.

2. Организационни условия – международно признати стандарти и разпоредби и правила в административната институция по организация и управление на информационната сигурност.



Фигура 1, Условия за реализация на информационната сигурност чрез ИКТ

3. Технически условия – комплекс от техническото оборудване (сървъри, мрежови устройства, устройства за засекретяване на информацията и част от работните станции в помещения, защитени от електромагнитни излъчвания и контролиран достъп), програмните средства и персонал, изпълняващ задължения, свързани с информационната сигурност.

По отношение на административни процеси с данни непредставляващи класифицирана информация по смисъла на Закона за защита на класифицираната информация е необходимо да с съблюдават изискванията на Закона за електронното управление и шестте наредби към него, които регламентират дейността на административните органи при предоставяне на електронни административни услуги и при работа с електронни документи. Така във връзка с осигуряване на информационна сигурност и оперативна съвместимост между различните администрации е необходимо да се изпълняят изискванията в:

- Закона за електронното управление;
- Наредбата за електронните административни услуги;
- Наредбата за регистрите на информационните обекти и на електронните услуги;
- Наредбата за вътрешния оборот на електронните документи и документи на хартиен носител в администрациите;
- Наредбата за електрония подпис в администрациите;
- Наредба за изискванията към единната среда за обмен на електронни документи;
- Наредба за общите изисквания за оперативна съвместимост и информационна сигурност.

Независимо от факта, че Законът за електронното управление не се прилага при „работата с електронни документи, които съдържат класифицирана информация" [7, чл. 1 ал.3] е необходимо информационните и комуникационните системи да отговарят и на някои от изискванията поставени в Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация. В тази връзка е необходимо да се направи ясно разграничение между класифицирана и некласифицирана информация по отношение на законодателна рамка, изисквания органите отговорни по отношение на гарантиране на информационната сигурност. На фигура 2 схематично е представена информацията ранжирана по отношение на степентта й на конфиденциалност.

Класифицирана информация по смисъла на Закона за защита на класифицираната информация е информацията, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация. Държавната тайна е такава информация "нерегламентираният достъп до която би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред", а именно[9]:

- Информация, свързана с отбраната на страната;
- Информация, свързана с външната политика и вътрешната сигурност на страната;
- Информация, свързана с икономическата сигурност на страната.

В [9, чл. 26. (1)] служебната тайна се дефинира, като "информацията, създавана или съхранявана от държавните органи или органите на местното самоуправление, която не е държавна тайна, нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правнозащитен интерес". В Закона за защита на класифицираната информация е предвидено информацията, подлежаща на класификация като служебна тайна, да бъде определена със закон или закони регулиращи сферата на дейност на административната структура. Според [9, чл. 26] служебна тайна могат да създават държавните органи и органите на местното самоуправление, а според Правилника за прилагане на Закона за защита на класифицираната информация [18, чл. 21] служебна тайна могат да създават и търговски дружества с повече от 51 на сто държавно участие. Окончателния списък на информация класифицирана, като служебна тайна се определя от ръководителя на съответната администратция или стопанска организация. Може да се констатира липсата на общи изисквания за класифициране на информация в много от сферите с засилен интерес за националната сигурност, каквато е например управлението на средства от европейски фондове, за които няма регаментирано третиране, като служебна тайна, въпреки националната значимост на проблематиката и изпълнението на

тази функция в различни административни организации. Незаконното заличаване или редактиране на данни в информационните масиви на правосъдната, отбранителната, финансовата и митническата системи, на МВР и ДАНС влияе пряко на националната сигурност на Р. България.

Различни аспекти на информационната сигурност в информационни и комуникационни системи използвани за отбрана и в системата за защита на националната сигурност е обект на изследване в разработките на Ц. Семерджиев, П. Павлов, Ст. Денчев, Г. Павлов, В. Шаламанов, Ю.Каракънева, П. Милев и др., позволяващи да се изгради цялостен подход в тази област.

Информацията третирана като некласифицирана според Закона за електронното управление се подразделя в 4 нива на защита според Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност [15, чл. 34 и допълнителни разпоредби]:

1. Ниво "0" или "D" обхваща открита и общодостъпна информация (например публикувана на интернет страниците на администрациите). То предполага анонимно ползване на информацията и липса на средства за конфиденциалност.

2. Ниво "1" или "C" изисква:

а) достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели;

б) ползвателите да се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп. За установяване на идентичността трябва да се използва защитен механизъм от типа идентификатор/парола. Няма изисквания за доказателство за идентичността при регистрация;

в) идентифициращата информация трябва да бъде защитена от нерегламентиран достъп;

г) доверителната изчислителна система, т.е. функционалността на информационната система, която управлява достъпа до ресурсите й, трябва да поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи ходът на работата;

д) информационната система трябва да разполага с технически и/или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система;

е) защитните механизми трябва да са преминали тест, който да потвърди, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.

3. Ниво "2" или "B" изисква в допълнение към изискванията към предишното ниво:

а) като механизъм за проверка на идентичността да се използва удостоверение за електронен подпис, независимо дали е издадено за вътрешноведомствени нужди в рамките на вътрешна инфраструктура на публичния ключ, или е издадено от външен доставчик на удостоверителни услуги;

б) при издаване на удостоверението издаващият орган проверява съществените данни за личността на ползвателя, без да е необходимо личното му присъствие;

в) доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти;

г) доверителната изчислителна система трябва да осигури взаимна изолация на процесите чрез разделяне на адресните им пространства.

4. Ниво "3" или "A" изисква в допълнение към изискванията към предишното ниво:

а) като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;

б) при издаване на удостоверението да е гарантирана физическата идентичност на лицето;

в) доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;

г) комуникацията между потребителя и системата да се осъществява единствено чрез протокол Transport Layer Security (TLS) или Secure Sockets Layer (SSL), като минималната дължина на симетричния ключ трябва да е 128 бита;

д) доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.

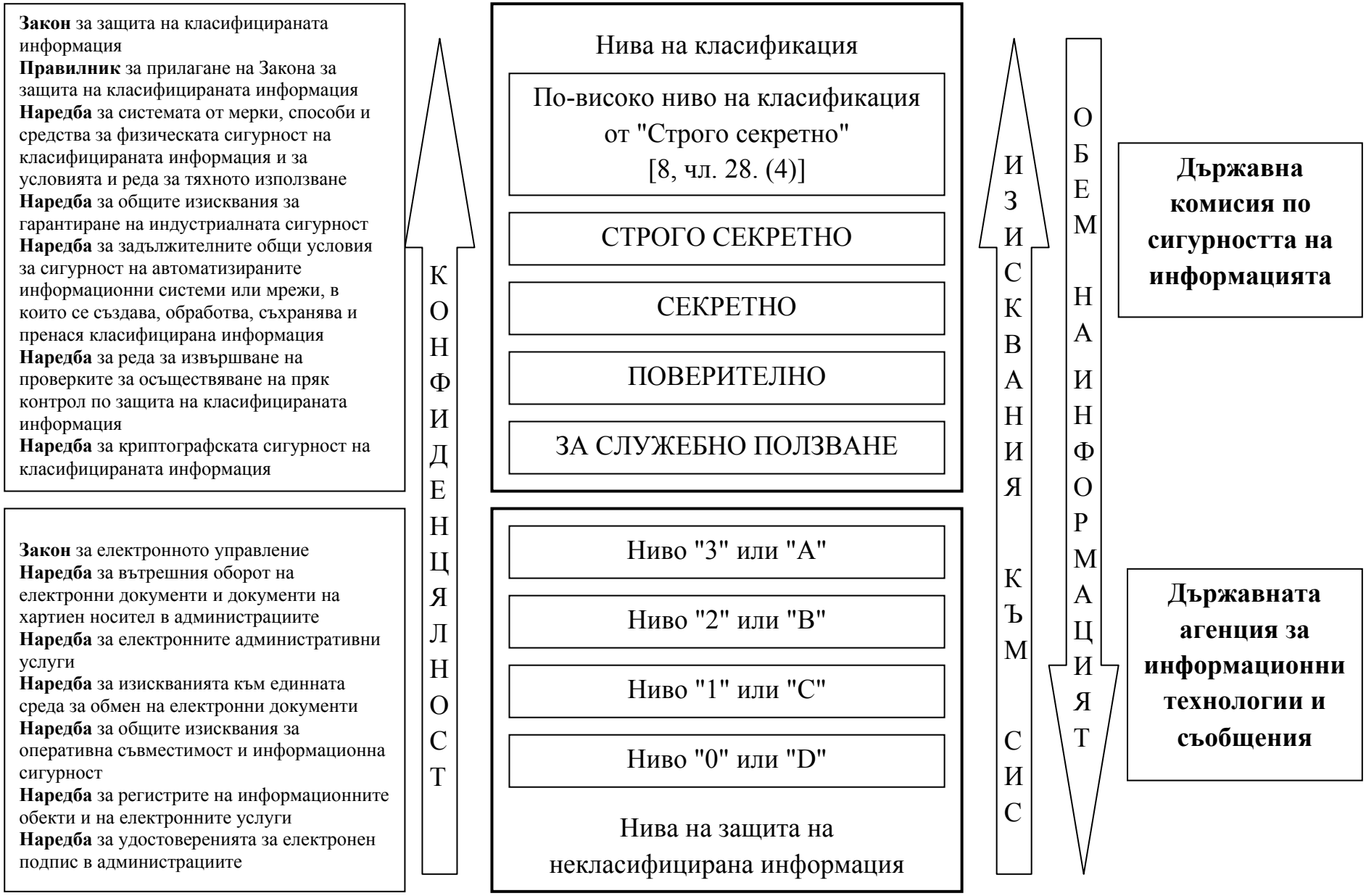
Разликите между системата за управление на информационна сигурност на класифицирана и некласифицираната информация се различават значително по обхват и използвани организационно технически похвати. Не може да не се отбележи същевременно че от съществено значение е отговорността на служителите работещи с класифицирана и некласифицирана информация. Някои аспекти на тази отговорност са дадени в [5].

Четирите нива на защита според Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност поставят специфични изисквания към системата за управление на информационна сигурност. За да бъде отговорено на тези изисквания трябва да се идентифицират заплахите и предложи ефективна и ефикасна система за тяхното отстраняване. Международните стандарти ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335:20001 изчерпателно дефинират основните заплахи пред осигуряване на конфиденциалност, достъпност и актуалност и цялостност на информацията, като те се обобщават в Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност:

1. Подслушване, изразяващо се в достъп до служебна информация чрез прихващане на електронни съобщения независимо от използваната технология.

2. Електромагнитно излъчване, изразяващо се в действия на трето лице, целящо да получи знание за обменяни данни посредством информационна система.

3. Нежелан код, който може да доведе до загуба на конфиденциалността чрез записването и разкриването на пароли и до нарушаване на интегритета при интервенции от трети лица, осъществили нерегламентиран достъп с помощта на



Фигура 2, Класифицирана и некласифицирана информация, нормативна база, органи по защита на информацията

такъв код. Нежелан код може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кодът може да доведе до загуба на достъпността, когато данните или файловете са разрушени от лицето, получило нерегламентиран достъп с помощта на нежелан код.

4. Маскиране на потребителската идентичност може да доведе до заобикаляне на проверката за достоверност и всички услуги и защитни функции, свързани с нея.

5. Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалност, ако се осъществи нерегламентиран достъп от трети лица. Погрешното насочване или пренасочване на съобщенията може да доведе и до нарушаване на интегритета, ако погрешно насочените съобщения са променени и след това насочени към първоначалния адресат. Погрешното насочване на съобщения води до загуба на достъпността до тези съобщения.6. Софтуерни грешки могат да застрашат конфиденциалността, ако софтуерът е създаден с контрол на достъпа или за криптиране или ако грешка в софтуера осигури възможност за нежелан достъп в информационна система.

7. Кражбата на информационни активи може да доведе до разкриване на информация, която представлява служебна или друга защитена от закона тайна. Кражбата може да застраши достъпността до данните или информационното оборудване.

8. Нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на поверителни данни и до нарушаване интегритета на тези данни, ако нерегламентираната им промяна е възможна. Нерегламентираният достъп до компютри, данни, услуги и приложения може да наруши достъпността до данните, ако тяхното изтриване или заличаване е възможно.

9. Нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни.

10. Повреждане на носител на информация може да наруши интегритета и достъпността до данните, които се съхраняват на този носител.

11. Грешка при поддръжката. Неизвършването на редовна поддръжка на информационните системи или допускане на грешки по време на процеса по поддръжка може да доведе до нарушаване на достъпността до данни.

12. Аварии в електрозахранване и климатични инсталации могат да доведат до нарушаване на интегритета и достъпността до данни, ако вследствие на настъпването на авариите са увредени информационни системи или носители на данни.

13. Технически аварии (например аварии в мрежите) могат да нарушат интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа.

14. Грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност.

15. Употреба на нерегламентирани програми и информация могат да нарушат интегритета и достъпността до данните, съхранявани и разпространявани чрез информационната система, в която е настъпило такова събитие, и програмите и информацията се използват, за да се изменят съществуващи програми и данни по неразрешен начин или ако те съдържат нежелан код.

16. Потребителски грешки могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие.

17. Липса на потвърждаване може да застраши интегритета на данните. Предпазните мерки за предотвратяване на непотвърждаването трябва да се прилагат в случаите, когато е важно да се получи доказателство за това, че дадено съобщение е изпратено и е/не е получено, както и за това, че мрежата е пренесла съобщението.

18. Интервенции срещу интегритета на данните могат да доведат до тяхното сериозно увреждане и до невъзможност от по-нататъшното им използване.

19. Аварии в комуникационното оборудване и услуги могат да увредят достъпността на данните, предавана чрез тези услуги.

20. Външни въздействия с огън, вода, химикали и др. могат да доведат до увреждане или унищожаване на информационното оборудване.

21. Злоупотреба с ресурси може да доведе до недостъпност до данни или услуги.

22. Природни бедствия могат да доведат до унищожаване на данни и информационни системи.

23. Претоварване на комуникационния трафик може да доведе до нарушаване на достъпността до обменяни данни.

Приетият подход за гарантиране на информационната сигурост в информационните системи работещи с некласифицирана информация е посредством внедряване на международния стандарт ISO 27001/2005 [15,чл. 3]. ISO 27001:2005 "Системи за управление на информационната сигурност. Изисквания" (Information technology - Security techniques - Information security management systems - Requirements) ISMS е международен стандарт, който поставя специфични изисквания към Системите за управление на информационната сигурност и е проложим за всички видове организации: в стопански, административни, неправителствени. Същевременно ISO 27001:2005 притежава ефективна степен на приложимост при:

1. определяне на изискванията и целите на информационната сигурност;

2. гарантиране на ефективното управление на информационния риск;

3. анализ на съществуващи процеси за управление на информацията от гледна точка на гарантиране на информационната сигурност;

4. разработване и реинженеринг на нови процеси за управление на информацията при гарантиране на информационната сигурност;

5. установяване на съответствие между политиките на организацията и националното законодателство в тази сфера;

6. гарантиране на устойчива информационна сигурност;

В тази връзка ISO 27001:2005 създава множество предпоставки за:

1. класификация на информационните активи;
2. управление на достъпа;
3. мониторинг и управление на инциденти;
4. мерки за физическа сигурност;
5. защита срещу нежелан софтуер;
6. сигурност на персонала.

Въвеждането на система за управление на информационната сигурност изисква извършването на сертификация на информационни системи в администрациите. Тази сертификация се извършва на две нива. На експертно ниво акредитирани оценители извършват сертификация на информационни системи и продукти, въз основа на изискванията на ISO 27001:2005 и на Наредбата за оперативна съвместимост и информационна сигурност. На национално ниво акредитацията е в правомощията на Председателя на Държавната агенция за информационни технологии и съобщения, който извършва цялотен подбор и мониторинг на дейността на акредитираните лица извършващи сертификацията на експертно ниво.

Заключение

Настоящата публикация представя резултатите от анализа на подходите за осъществяване на ефективна информациона сигурност на системите работещи с некласифицирана информация в публичната администрация. Дефинирани и анализирани са основните организационно-управленски фактори, влияещи на степента на ефикасност на информационната сигурност, като е направена съпоставка в това отношение между информационната сигурност на класифицирана и некласифицирана информация. Направените изводи и предложения, резултат от този анализ, изясняват възможностите за изграждане на ефективни системи за управление на информационната сигурност основаващи се на международния стандарт ISO 27001:2005.

Литература

[1] Ангелов, Кирил, Информационните и комуникационните технологии, като стратегия за превенция на корупцията, София, 2008

[2] Денчев Стоян, Драгомир Паргов, Ирена Петева, Белла Тетевенска, Прозрачност и сигурност наинформацията при корпоративните комуникации в информационното общество, Военен журнал, бр. 5, 2008

[3] Денчев Стоян, Цветан Семерджиев, Иван Попов, Н. Костова, Концепция и политика за информационна сигурност. С., 2006

[4] Павлов Георги, Проблеми на сигурността и защитата на класифицираната информация в АИС и мрежи, Икономически алтернативи, бр.5, 2005

[5] Русанов, Л., Л. Мечкаров. Относно някои аспекти на административната отговорност в трудовите отношения. Научни известия на НТСМ, ISSN-1310-3946, Год. XIV, 2007, Брой 2 (97), с. 233-235.

[6] Закон за достъп до обществена информация, Обн., ДВ, бр. 55 от 7.07.2000 г., изм., бр. 1 от 4.01.2002 г., в сила от 1.01.2002 г., бр. 45 от 30.04.2002 г., бр. 103 от 23.12.2005 г., изм. и доп., бр. 24 от 21.03.2006 г., изм., бр. 30 от 11.04.2006 г., в сила от 12.07.2006 г., бр. 59 от 21.07.2006 г., в сила от деня на влизане в сила на Договора за присъединяване на Република България към Европейския съюз - 1.01.2007 г., изм. и доп., бр. 49 от 19.06.2007 г., изм., бр. 57 от 13.07.2007 г., в сила от 13.07.2007

[7] Закон за електронното управление, 13.06.2008 г., ДВ. бр.46 от 12 Юни 2007г.

[8] Закон за електронния документ и електронния подпис, ДВ. бр.34 от 6 април 2001г., изм. ДВ. бр.112 от 29 декември 2001г., изм. ДВ. бр.30 от 11 април 2006г., изм. ДВ. бр.34 от 25 април 2006г., изм. ДВ. бр.38 от 11 май 2007г.

[9] Закон за защита на класифицираната информация, Обн. ДВ. бр.45 от 30 Април 2002г., попр. ДВ. бр.5 от 17 Януари 2003г., изм. ДВ. бр.31 от 4 Април 2003г., изм. ДВ. бр.52 от 18 Юни 2004г., доп. ДВ. бр.55 от 25 Юни 2004г., доп. ДВ. бр.89 от 12 Октомври 2004г., изм. ДВ. бр.17 от 24 Февруари 2006г., изм. ДВ. бр.82 от 10 Октомври 2006г., изм. ДВ. бр.46 от 12 Юни 2007г., изм. ДВ. бр.57 от 13 Юли 2007г., изм. ДВ. бр.95 от 20 Ноември 2007г., изм. ДВ. бр.109 от 20 Декември 2007г., изм. ДВ. бр.36 от 4 Април 2008, изм. ДВ. бр.66 от 25 Юли 2008г., изм. ДВ. бр.69 от 5 Август 2008

[10] Закон за защита на личните данни, в сила от 01.01.2002 г. Обн. ДВ. бр.1 от 4 Януари 2002г., изм. ДВ. бр.70 от 10 Август 2004г., изм. ДВ. бр.93 от 19 Октомври 2004г., изм. ДВ. бр.43 от 20 Май 2005г., изм. ДВ. бр.103 от 23 Декември 2005г., изм. ДВ. бр.30 от 11 Април 2006г., изм. ДВ. бр.91 от 10 Ноември 2006г., изм. ДВ. бр.57 от 13 Юли 2007г.

[11] Наредба за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, Обн. ДВ. бр.48 от 23 Май 2008г.

[12] Наредба за електронните административни услуги, Обн. ДВ бр. 48 от 23 май 2008

[13] Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, Обн. ДВ бр. 44 от 09 май 2008

[14] Наредба за изискванията към единната среда за обмен на електронни документи, Обн. ДВ бр. 62 от 11 юли 2008г.

[15] Наредба за общите изисквания за оперативна съвместимост и информационна сигурност, Обн. ДВ бр. 101 от 25 ноември 2008

[16] Наредба за регистрите на информационните обекти и на електронните услуги, Обн. ДВ. бр.48 от 23 Май 2008г.

[17] Наредба за удостоверенията за електронен подпис в администрациите, Обн. ДВ. бр.48 от 23 Май 2008г.

[18] Правилник за прилагане на закона за защита на класифицираната информация, Обн. ДВ. бр.115 от 10 Декември 2002г., изм. ДВ. бр.22 от 11 Март 2003г., доп. ДВ. бр.6 от 23 Януари 2004г., изм. ДВ. бр.56 от 11 Юли 2006г., изм. ДВ. бр.84 от 19 Октомври 2007г., изм. ДВ. бр.44 от 9 Май 2008г., изм. ДВ. бр.91 от 21 Октомври 2008г., изм. ДВ. бр.7 от 27 Януари 2009г.

[19] ISO/IEC ISO 27001:2005, 15 октомври 2005

[20] ISO/IEC TR 13335-3:1998

[21] ISO/IEC TR 13335-4:2000