Steps to Success
Пътят към успеха

ЗАЩИТА НА ИНФОРМАЦИЯТА В АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ В ОБЛАСТТА НА СИГУРНОСТТА И ОТБРАНАТА

Иванка Димитрова[1)]
Висше училище по телекомуникации и пощи – България

Резюме.Текстът разглежда какво представлява защитената информационна система, какво представлява системата за защита на информацията и какви изисквания се предявяват към нея; какви са заплахите и причините за нарушаване на сигурността на информационните технологии; какви са функциите на защитата и по какъв начин трябва да се реализират, как се противодейства на заплахите и как се отстраняват причините за нарушения на сигурността; как да се построи комплексна система за защита на информацията; как да се достигне високо ниво на сигурност при приемливи разходи на средства за защита на информацията.

Keywords: security; defense; information; army

Новата среда за сигурност извежда на преден план извода, че нито една държава не може да се справи сама с рисковете и заплахите за сигурността си. Трудностите, които се пораждат при трансформирането на средата за сигурност в международен план, се проявяват като несигурност в икономическата, социалната, етническата, военната и други области на държавното и общественото устройство. Изграждането на сигурни комуникационно-информационни системи е немислимо без създаването и внедряването на процедури за сигурност в областта на компютърните мрежи, изготвени на базата на политика за сигурност на комуникационно-информационните системи. Анализът и обобщението на съществуващата нормативна база и добрите практики извеждат на преден план основни характеристики и изисквания за постигане на дълготрайни и ефикасни резултати в сферата на сигурността на информацията. Този подход дава възможност за създаване на цялостна визия за състоянието на сигурността на информацията в една организация (ведомство, фирма, министерство и др.). Предмет на разглеждане в изследването са правните, управленските и организационните аспекти на

СИ, както и стандартите и процедурите за гарантиране на сигурността на информацията и защитата ѝ.

Ключовите сектори на модерното общество, които са жизненоважни за националната сигурност и за основното функциониране на индустриалните икономики, зависят от редица взаимнозависими национални и международни софтуерни управленски системи, за да работят гладко, надеждно и продължително. Тази информационна инфраструктура подсилва много елементи от критичната инфраструктура (КрИ) и затова се нарича критична информационна инфраструктура (КрИИ). По своята същност КрИ включва всички системи и активи, чиято неправоспособност или унищожение ще имат дестабилизиращ ефект върху националната сигурност, икономическото и социалното благоденствие на нацията. КрИИ включва компоненти, като телекомуникации, компютри/софтуер, интернет, сателити, оптически комуникации и др. Терминът се използва за целостта от взаимосвързани компютри и мрежи и техните потоци от критична информация.[1)] От казаното дотук и на основание ЗЗКИ може да се постави знак за равенство между понятието „критична информация“ и информацията, класифицирана като „държавна тайна“.

Ето защо защитата на критичната информация е част от защитата на критичната инфраструктура и е фокусирана върху защитата на системи и активи включително компоненти, като телекомуникации, компютри/софтуер, интернет, сателити, оптически комуникации и др., и на взаимосвързани компютри и мрежи и услугите, които те осигуряват.

Технологичните подобрения в информационните технологии продължават да съкращават времето и разстоянията, като фактори, и осигуряват все по-бързи темпове за обмен на информация. Създава се глобална мрежа от информационни системи и мрежи в областта на сигурността и отбраната, свързващи информационни бази данни и центрове за обработка и анализ на информацията, които са достъпни за служителите навсякъде и по всяко време при изпълнение на задачи от различен характер. Обменяната в тях информация в по-голямата си част представлява държавна или служебна тайна, която по смисъла на ЗЗКИ (Закон за защита на класифицираната информация) е „класифицирана“ и подлежи на защита от нерегламентиран достъп и компрометиране.

С термина класифицирана информация се означават материали и документи, съдържащи информация, класифицирана като държавна или служебна тайна. Тя може да е от политически, военен и икономически характер, от промишлено, научно или технологично естество.

При обмена на класифицирана информация в автоматизираните информационни системи (АИС) и мрежи основен фактор се явява нейната защита. С цел нейното осигуряване се планира система от мерки, които се различават според нивото на класификация на информацията, която ще се създава, обра-

ботва, съхранява и пренася, а именно „строго секретно“, „секретно“, „поверително“ или „за служебно ползване“.

Постигането на сигурността е резултат от дейности по запазване на конфиденциалността на обменяната и съхранявана информация, нейната цялостност и ограниченост за достъп, както и такива, недопускащи възможността за отричане на принадлежността ѝ (отказ от авторство).

Защитата на АИС и мрежи (като елемент на комуникационно-информационната система на сигурността и отбраната) е процес, свързан с изпълнението на мероприятия и дейности, произтичащи от изискванията на държавните и ведомствените нормативни документи по опазване на държавната и служебната тайна от случайно или преднамерено разкриване, неправомерно използване или унищожаване, както и спазването на поетите ангажименти в областта по международни договорености.

При дефиниране на общата система за сигурност на автоматизираните информационни системи и мрежи в отбраната и при участие в международни операции от различен характер се открояват следните елементи: физическа сигурност, персонална сигурност, документална сигурност, комуникационна и криптографска сигурност, защита от паразитни електромагнитни излъчвания, компютърна сигурност.

Тези мерки се реализират чрез възможностите на техническите и програмните средства на компютърните системи и на специализирани средства.

Важен елемент на сигурността на информацията е и определянето на отговорните длъжностни лица и техните функционални задължения: служител по сигурността на АИС и мрежи в организационната единица; орган за развитие и експлоатация (ОРЕ) на АИС и мрежите; администратор по сигурността на АИС и мрежи; администратори на АИС (системни администратори), администратори на приложенията и базите данни; потребители на АИС и мрежи.

Внимание заслужава и въпросът за свързването на АИС и мрежи в отбраната, в които се създава, съхранява, обработва и пренася класифицирана информация, към други АИС и мрежи. Според закона е забранено те да бъдат свързвани към интернет или други публични мрежи. Интересен е случаят, при който е необходимо да се свържат АИС и мрежи с различно ниво на класификация на информацията, обработвана в тях – например „поверително“ към „за служебно ползване“. На настоящия етап в националното законодателство този въпрос е недостатъчно уреден, а националният Орган по акредитация на сигурността (ОАС) в лицето на ДАНС няма одобрени технически устройства и регламент за прилагането им.

Съгласно ЗЗКИ и „Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация“ всяка АИС и

мрежа, в която се създава, обработва, съхранява и пренася класифицирана информация, трябва да е акредитирана и да притежава сертификат за сигурност.

Според ЗЗКИ в процеса на акредитация се изготвят следните задължителни документи по сигурността: анализ на риска за сигурността на АИС и мрежите, специфични изисквания за сигурност, процедури за сигурност на АИС и мрежите.

Анализ на риска за сигурността на АИС и мрежите се изготвя само за мрежи с ниво на класификация „секретно“ и по-високо. В този документ се описват заплахите и уязвимите места на АИС и мрежите, вероятността за осъществяване на заплахите при конкретните ресурси и работна среда и се оценяват последствията при тяхното реализиране. Посредством анализа на риска се цели определяне на необходимите мерки за сигурност (защита); ефективно комбиниране на видовете мерки за сигурност (защита); правилна оценка на остатъчния риск.

Специфичните изисквания за сигурност (СИС**)** се формулират по време на най-ранния стадий от проектирането на системата и се детайлизират и развиват в процеса на разработване и изпълнение на проекта на компютърните мрежи. Степента на детайлизация зависи от сложността на системата и мрежата, от режима на сигурност, в който се експлоатира, и от нивото на класификация на обработваната информация. В своя завършен вид СИС определят как се постига, управлява и контролира сигурността на АИС и мрежите

Процедурите за сигурност на АИС и мрежите са подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на утвърдените мерки за сигурност на АИС и мрежите. Те включват: организация на сигурността, персонална сигурност, физическа сигурност, документална сигурност, компютърна сигурност, комуникационна сигурност, сигурност при осигуряването със средства за АИС или мрежата, действия при критични по отношение на сигурността ситуации, управление на конфигурацията, отговорности и задължения на потребителите.

Правните мерки включват – юридически нормативни актове (законови и подзаконови) и други нормативни документи, регламентиращи достъпа до информация и отговорността в случай на нарушения. Всяка страна създава своя нормативна база от документи. Както във всички развити страни, така и в нашата страна са приети редица документи: ЗЗКИ, „Закон за достъп до обществената информация“, „Закон за защита на личните данни“, ППЗЗКИ, „Наредба за криптографска сигурност на класифицирана информация“, „Наредба за задължителните общи условия за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация“ и др. Тъй като сме страни членки на НАТО, се прилагат и директивите на НАТО по сигурността. По-специално: AC/322-D(2004)0030 – Директива за изпълнение на избора на прилагането на инструментариум по сигурността, AC/35-D/1014

REV 1 – Структура и съдържание на оперативните процедури по сигурността на КИС, AC/35-D/2004 – Директива по INFOSEC, AC/322-D/l6 – Ръководство по прилагането и използването на инструментариум по управлението на сигурността, AD 70-1 – Директива по сигурността на Обединеното командване по операциите. ЗЗКИ до голяма степен припокрива директивите в областта на защита на АИС и мрежи, като дори е по-рестриктивен.

Заключение. Всяка организация, независимо от сферата си на дейност, била тя цивилна или военна, ползваща АИС, в които се обработва класифицирана информация, следва да спазва политики за информационна сигурност.

Стандартите в областта на информационната сигурност се разработват с цел осигуряване на съвместимост на подсистемите и определяне на единни правила. Обикновено, независимо от типа на дейност на дадена организация, използваните стандарти са международни.

Процедурите за сигурност на АИС и мрежи са най-ниското ниво на прилагане на политиките за информационна сигурност. Те представляват подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на утвърдените мерки за сигурност на АИС или мрежата. Те следва да съдържат следните раздели: организация на сигурността; персонална сигурност; физическа сигурност; документална сигурност; компютърна сигурност; комуникационна сигурност; сигурност при осигуряването със средства за АИС или мрежата; действия при критични по отношение на сигурността ситуации; управление на конфигурацията; отговорности и задължения на потребителите.

NOTES/БЕЛЕЖКИ

1. Авторът е студент във Висше училище по телекомуникации и пощи.

Консултант при разработване на настоящия текст е проф.д.т.н. Димитър Радев, Висше училище по телекомуникации и пощи. E-mail: dradev@abv.bg

REFERENCES/ЛИТЕРАТУРА

Semerdzhiev, C. (2007). *Upravlenienasigurnosttanainformatsiyata*. Sofia: Softtrade. [Семерджиев, Ц. (2007). *Управление на сигурността на информацията*. София: Софттрейд.]

Armencheva I. (2010). *Politikazasigurnost i zashtitanaklasifitsiranatainform atsiya v avtomatiziraniinformatsionnisistemi i mrezhi*.Disertatsionentrud. Sofia: Voennaakademiya „G. S. Rakovski". [Арменчева И. (2010). *Политика за сигурност и защита на класифицираната информация в автоматизирани информационни системи и мрежи*. Дисертационен труд. София: Военна академия „Г. С. Раковски".]

Stoyko, M. (2007). Aspekti na transformatsiyata na sistemata za sigurnost. Sofia: Voenno izdatelstvo. [Стойко, М. (2007). *Аспекти на трансформацията на системата за сигурност*. София: Военно издателство.]
Semerdzhiev, Ts. (2007). *Sigurnost i zashtita na informatsiyata*. Sofia: KlasikaiStil. [Семерджиев, Ц. (2007). *Сигурност и защита на информацията*. София: Класика и Стил.]
Peltier, T. *Information Security Fundamentals.*Abingdon (UK): CRC Press

DATA PROTECTION IN AUTOMATED INFORMATION SYSTEMS IN THE SECURITY AND DEFENCE FIELD

Abstract. The article discusses what is a secure information system; what is information protection system and what requirements brought thereto; what are the threats and causes security breach of information technology; What are the functions of protection and how should realize how counteract the threats and how to eliminate the causes of security breaches; how to build a complex system of information protection; how to achieve a high level of security at acceptable cost of funds for the protection of information.

✉ **Ms. Ivanka Dimitrova**
University of Telecommunications and Post
Sofia, Bulgaria
E-mail: ivnikdim77@gmail.com