Міжнародно-правові науки

УДК 336.719

Тертичний Самір Сахільович
студент
Національного авіаційного університету
Тертычный Самир Сахилевич
студент
Национального авиационного университета
Tertichniy Samir
Student of the
National Aviation University

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ ЗАКОРДОННОГО ДОСВІДУ ЗАХИСТУ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИМПЛЕМЕНТАЦИИ ЗАРУБЕЖНОГО ОПЫТА ЗАЩИТЫ ЕЛЕКТРОННОЙ ИНФОРМАЦИИ
PROBLEMS AND THE PROSPECTS OF IMPLEMENTATION OF FOREIGN EXPERIENSE OF PROTECTION OF ELECTRONIC INFORMATION

Анотація. *У статті окреслені основні проблеми й перспективи імплементації закордонного досвіду захисту електронної інформації. Виявлено, що закордонний досвід захисту електронної інформації будується на певних стандартах і критеріях. З'ясовано, що закордоном активно розробляються й удосконалюються критерії оцінки інформаційної безпеки, які почали застосовуватися із розробки критеріїв оцінки довірених комп'ютерних систем у США. Встановлено, що одним із можливих каналів*

імплементації закордонного досвіду захисту електронної інформації є вивчення досвіду захисту інформації у представництвах іноземних держав, розташованих в Україні. Сформульовано базові теоретичні принципи, якими можна керуватися при побудові систем захисту інформації в міжнародних представництвах. Як свідчить іноземний досвід, проведення роботи в галузі захисту інформації дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки організації, виробити рекомендації щодо забезпечення інформаційної безпеки організації, знизити потенційні втрати підприємства чи організації через підвищення стійкості функціонування корпоративної мережі, розробити концепцію та політику безпеки установи, а також запропонувати плани захисту конфіденційної інформації організації, що передається по відкритих каналах зв'язку, захисту інформації закладу від навмисного спотворення, несанкціонованого доступу до неї, її копіювання чи використання.

Ключові слова: *інформація, документ, інформаційна безпека, електронна інформація, зарубіжний досвід, світовий інформаційний простір, стандарти, критерії, технічний захист інформації, принципи.*

Аннотация. *В статье обозначены основные проблемы и перспективы имплементации зарубежного опыта защиты электронной информации. Выявлено, что иностранный опыт защиты электронной информации строится на определенных стандартах и критериях. Выяснено, что заграницей активно разрабатываются и совершенствуются критерии оценки информационной безопасности, которые начали применяться с разработки критериев оценки компьютерных систем в США. Установлено, что одним из возможных каналов имплементации зарубежного опыта защиты электронной информации является изучение опыта защиты информации в представительствах иностранных государств, расположенных в Украине. Сформулировано базовые*

теоретические принципа, которыми можно руководствоваться при построении систем защиты информации в международных представительствах. Как свидетельствует иностранный опыт, проведение работы в сфере защиты информации позволяет оценить или переоценить уровень текущего состояния информационной безопасности организации, выработать рекомендации относительно обеспечения информационной безопасности организации, снизить потенциальные потери предприятия или организации путем повышения стойкости функционирования корпоративной сети, разработать концепцию и политику безопасности учреждения, а также предложить планы защиты конфиденциальной информации организации, которая передается по открытым каналам связи, защиты информации учреждения от намеренного искажения, несанкционированного доступа к ней, ее копирования или использования.

Ключевые слова: *информация, документ, информационная безопасность, электронная информация, зарубежный опыт, мировое информационное пространство, стандарты, критерии, техническая защита информации, принципы.*

Summary. *In article the main problems and the prospects of implementation of foreign experience of protection of electronic information are designated. It is revealed that foreign experience of protection of electronic information is based on certain standards and criteria. It is found out that the abroad actively develops and improves criteria for evaluation of information security which began to be applied with development of criteria for evaluation of computer systems in the USA. It is established that one of possible channels of implementation of foreign experience of protection of electronic information is studying of experience of information security in representative offices of the foreign states located in Ukraine. It is formulated basic theoretical the principle*

by which it is possible to be guided at creation of systems of information security in the international representative offices. As foreign experience testifies, carrying out work in the field of information protection allows to evaluate or revaluate the level of a current status of information security of the organization, to develop recommendations concerning information security support of the organization, to reduce potential losses of the enterprise or organization by increase in firmness of functioning of corporate network, to develop the concept and security policy of organization and also to offer plans of confidential information protection of the organization which is transferred on open communication links, information protection of organization from intended distortion, illegal access to it, its copying or use.

Key words: *information, document, information security, electronic information, foreign experience, world information space, standards, criteria, technical information security, principles.*

Постановка проблеми. Інформація – один з найважливіших сучасних світових ресурсів: «Хто володіє інформацією, той володіє світом. Певне повідомлення коштує дорожче за життя» (У. Черчілль). Її своєчасне отримання, ефективне використання, належне зберігання й безпечна передача відіграють визначальну роль у діяльності провідних державних і недержавних структур у провідних країнах світу.

Сьогодні для роботи з інформацією використовуються найрізноманітніші технічні пристрої. Але найчастіше – це комп'ютер (або мережа комп'ютерів), підключений до Інтернет мережі. Переоцінити ефективність ПК і швидкість передачі даних через Інтернет важко. Жодні паперові документи не здатні вмістити стільки інформації й жоден факс не передасть її так швидко. У цьому безсумнівний плюс сучасних комп'ютерних технологій.

З огляду на вказане, важливим є вивчення зарубіжного досвіду побудови систем захисту електронної інформації.

Аналіз останніх досліджень і публікацій. Питанням розробки і функціонування систем захисту інформації пракордоном исвячено значну кількість праці В. О. Хорошка [1], В. Б. Дудикевича [2; 3], О. С. Петрова [1] та ін.

Питання сучасних загроз інформаційної безпеки для державних та приватних українських установ, міжнародні стандарти безпеки дослідженні в роботах А. В. Платоненко, А. О. Аносова [4], О. В. Сєвєрінова, В. І. Черниша, М. Є. Молчанова [5-6] та ін. Крім того, в Україні виданий термінологічний словник з питань технічного захисту інформації [7].

Віддаючи належне вже проведеним дослідженням, науковцям слід і у подальшому продовжувати поглиблювати систему знань про загрози інформаційній безпеці та протидію ним.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є виявлення основних принципів побудови захисту інформаційних систем закордоном та можливостей використання цього досвіду Україною

Виклад основного матеріалу. Нині в Україні у зв'язку з входженням у світовий інформаційний простір швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені мережами стільникового зв'язку, факсимільний зв'язок став доступний для широкого кола користувачів. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Аналіз стану захисту інформації – це комплексне вивчення фактів, подій, процесів, явищ, пов'язаних з проблемами захисту інформації, у тому числі даних про стан роботи по виявленню можливих

каналів витоку інформації, про причини й обставини, що сприяють витоку і порушень режиму секретності (конфіденційності) у ході повсякденної діяльності організації / підприємства.

Вищевикладене дає підстави стверджувати, що система захисту інформації в інформаційних системах (ІС) підприємств повинна будуватися на засадах комплексності й адаптивності.

Контроль за реалізацією організаційно-технічних заходів щодо технічного захисту інформації (ТЗІ) у виділених приміщеннях, ІС та корпоративних мережах, повнотою та достатністю робіт з атестування виділених приміщень повинен включати перевірку відповідності виконання цих заходів вимогам чинного законодавства України, нормативно-правових актів з питань.

Закордонний досвід захисту електронної інформації будується на певних стандартах і критеріях. Базовим міжнародним стандартом з інформаційної безпеки, розробленим спільно Міжнародною організацією зі стандартизації й Міжнародною електротехнічною комісією є ISO/IEC 27001. Підготовлений до випуску підкомітетом SC27 Об'єднаного технічного комітету JTC 1, стандарт містить вимоги у сфері інформаційної безпеки для створення, розвитку й підтримки Системи менеджменту інформаційної безпеки (СМІБ) [8].

У стандарті ISO/IEC 27001 (ISO 27001) зібрані описи кращих світових практик у сфері управління інформаційною безпекою. ISO 27001 установлює вимоги до системи менеджменту інформаційної безпеки для демонстрації спроможності організації захищати власні інформаційні ресурси. Даний стандарт підготовлений як модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки й поліпшення СМІБ.

Як свідчить закордонний досвід, організація може бути сертифікована акредитованими агентствами відповідно до цього стандарту. Процес сертифікації складається із трьох стадій:

– стадія 1 – вивчення аудитором ключових документів системи менеджменту інформаційної безпеки – положення про застосовність (Soa), план обробки ризиків (RTP) тощо. Може виконуватися як на території організації так і шляхом висилки цих документів зовнішньому аудиторові;

– стадія 2 – детальний, глибокий аудит, включаючи тестування впроваджених заходів і оцінка їх ефективності. Включає повне вивчення документів, які вимагає стандарт;

– стадія 3 – виконання інспекційного аудита для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується на періодичній основі.

Процедура системи менеджменту за кожним із міжнародних стандартів або їх комбінації розподіляється на 4 етапи:

1) підготовка до сертифікації;
2) аудит 1-го щабля (перевірка готовності до сертифікації);
3) аудит 2-го щабля (сертифікаційний аудит);
4) видача сертифіката й нагляд.

Крім того, закордоном активно розробляються й удосконалюються критерії оцінки інформаційної безпеки, які почали застосовуватися із розробки критеріїв оцінки довірених комп'ютерних систем у США (т.зв. «Помаранчева книга»).

На початку 70-х рр. XX століття Девід Белл і Леонард Ла Падула розробили модель безпеки для операцій, що здійснюються на комп'ютері. Ця модель базувалася на урядовій концепції рівнів класифікації інформації (несекретна, конфіденційна, секретна, цілком таємна) та рівнів допуску. Якщо людина (суб'єкт) мав рівень допуску вище, ніж рівень файлу (об'єкта) за класифікацією, то вона отримувала доступ до файлу, в іншому випадку

доступ відхилявся. Ця концепція знайшла свою реалізацію в стандарті 5200.28 «Trusted Computing System Evaluation Criteria» (TCSEC) («Критерій оцінки безпеки комп'ютерних систем»), розробленому в 1983 р. Міністерством оборони США. Через колір обкладинки він отримав назву «Помаранчева книга» [2, с. 60].

«Помаранчева книга» ранжувала комп'ютерні системи у відповідності з наступною шкалою:

D Мінімальна захист (ненормованим)

C1 Захист на розсуд

C2 Контрольований захист доступу

B1 Захист з мітками безпеки

B2 Структурована захист

B3 Захист доменів

A1 Розробка, що перевіряються

Сучасна концепція інформаційної безпеки США втілена у американських «Федеральних критеріях» (відомі як Common Criteria – «Загальні критерії») в 1992 р. Головна ідея зосереджена у так званих профілях захисту, що визначають різні середовища безпеки, в які може бути розміщена комп'ютерна система. Продукти проходять оцінку на відповідність цим профілями і сертифікуються. При покупці системи організація має можливість вибрати профіль, що найбільш повно відповідає її потребам, і підібрати продукти, сертифіковані за цим профілем. Сертифікат продукту включає також рівень довіри, тобто рівень секретності, закладений оцінювачами, відповідає профілю функціональних можливостей.

Надійний фізичний захист необхідний для забезпечення збереження матеріальних активів – паперових носіїв і систем. Захист комунікацій (COMSEC) відповідає за безпеку при передачі інформації. Захист випромінювання (EMSEC) необхідний, якщо супротивник має потужну

апаратуру для читання електронної емісії від комп'ютерних систем. Комп'ютерна безпека (COMPUSEC) потрібна для управління доступом у комп'ютерних системах, а безпека мережі (NETSEC) – для захисту локальних мереж. У сукупності всі види захисту забезпечують інформаційну безпеку (INFOSEC).

До теперішнього часу не розроблено процес сертифікації комп'ютерних систем, що підтверджує забезпечувану безпеку. Для більшості пропонованих рішень технології занадто швидко пішли вперед. Лабораторією техніки безпеки США (Underwriters Laboratory) була запропонована нова концепція безпеки, відповідно до якої необхідно створити центр сертифікації, що засвідчує безпеку різних продуктів. Якщо вчинено проникнення в систему, користувачі якої працювали з несертифікованим продуктом, то це слід розцінювати як недбале ставлення до безпеки адміністраторів цієї системи [3, с. 145].

При складанні інших критеріїв були зроблені спроби розділити функціональні вимоги і вимоги гарантованості. Ці розробки увійшли до «Зеленої книги» Німеччини в 1989 р., в «Критерії Канади» в 1990 р., «Критерії оцінки безпеки інформаційних технологій» (ITSEC) в 1991 р. і в «Федеральні критерії» (відомі як Common Criteria – «Загальні критерії») в 1992 р. Кожен стандарт пропонував свій спосіб сертифікації безпеки комп'ютерних систем. ITSEC і Common Criteria просунулися далі інших, залишивши функціональні вимоги фактично не визначеними.

В 1995 році Європейським Союзом була прийнята Директива щодо Захисту особистості з дотриманням режиму персональних даних та вільного руху таких даних. Директива спрямована на впорядкування практики захисту інформації в межах Європейського Союзу. Однією з вимог, адресованих державам-учасникам, є вимога прийняти закони щодо захисту персональної інформації, як в публічному, так і в приватному секторі. Зазначені закони мають також включати тимчасове блокування

переміщення інформації до державне членів Європейського Союзу, які не встановили «адекватного» рівня захисту інформації.

Як доповнення до цієї Директиви в 1996 році була прийнята Директива, яка забезпечує гармонізацію в державах-членах умов, необхідних для того, щоб гарантувати еквівалентний рівень захисту фундаментальних прав та свобод, в тому числі специфічного права на секретність відносно обробки персональних даних в секторі телезв'язку, та гарантувати вільний рух таких даних, та обладнання телезв'язку та послуг в Співдружності (законом України «Про інформацію» до основних персональних даних віднесено національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Офіційним тлумаченням окремих статей цього закону даний перелік доповнено ще й майновим станом) [4, с.88].

Відповідно до Директиви щодо Захисту особистості з дотриманням режиму персональних даних та вільного руху таких даних (Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 95/46/EC), та конкретизуючої її Директиви від 1996 року, були внесені зміни до національного Законодавства держав-учасників Європейського Союзу.

Відповідно до загальних принципів Акту Захисту Інформації в Телекомунікаціях (Teleservices Data Protection Act) (TDPA), збирання, обробка та використання інформації дозволяється лише у випадках, коли воно дозволене законом або здійснюється за наявності згоди користувача обслуговування. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач. Згода користувача не може виступати в якості умов для надання послуг. Інформація за договором може бути зібрана, оброблена та використана в тому обсязі, який є необхідним для виконання договору. Дані використання та бухгалтерського обліку не повинні передаватися третім

особам. Однак деякі з зазначених вище типів даних можуть бути передані для певної мети обслуговування постачальників від постачальників, через яких здійснений доступ до послуг [4, с. 90].

Одним із можливих каналів імплементації закордонного досвіду захисту електронної інформації є вивчення досвіду захисту інформації у представництвах іноземних держав, розташованих в Україні.

Інформація, що зберігається в ПК міжнародних представництв й передається його співробітниками через Інтернет, перебуває під загрозою: її можуть знищити, вкрасти, навмисне видалити або спотворити. Вихід з ладу комп'ютерної техніки також загрожує втратою інформаційних даних. Тому вони повинні бути відповідним образом захищені. Захищені комплексно, від всіх можливих ризиків.

Типова інформаційна система, що використовується в міжнародних представництвах, складається із трьох взаємозалежних рівнів:

1. Рівень устаткування й технічних засобів. На даному рівні розташовані комп'ютери, сервери, периферійне обладнання (із прикладними й системними програмами, що забезпечують їх роботу).

Саме з даним рівнем взаємодіють авторизовані користувачі інформаційних систем, що здійснюють санкціонований доступ до її ресурсів. На рівні розташовані також копії програмного забезпечення, інстальованого безпосередньо на робочі станції користувачів. Об'єкти, що перебувають на даному рівні, прив'язані до фізичних структур – будинків, у яких розміщена система.

2. Рівень транспортного середовища. На цьому рівні розміщені структуровані кабельні системи, мережі зв'язку й телекомунікацій тощо.

З даним рівнем взаємодіють не самі користувачі інформаційних систем, а користувальницьке обладнання з першого рівня. Функціонування об'єктів, розміщених на рівні, також залежить від особливостей будинків, у яких розміщена система.

3. Рівень прикладних програм. На цьому рівні перебуває прикладне й загальносистемне програмне забезпечення, призначене для забезпечення роботи обладнання і користувачів інформаційних систем.

Зловмисники (порушники режиму інформаційної безпеки), намагаючись отримати несанкціонований доступ (НСД) до її ресурсів, вживають спроби НСД на всіх трьох рівнях типової моделі.

Виходячи із запропонованої трьохрівневої структури типової інформаційної системи, типова система захисту інформації повинна повинна складатись із трьох підсистем і відповідати за захист кожного з рівнів інформаційної системи організації:

1. Підсистема захисту комплексу обладнання й технічних засобів. Підсистема призначена для захисту серверів, автоматизованих робочих місць, обладнання зв'язку й телекомунікацій тощо.

2. Підсистема захисту транспортного середовища. Завданням підсистеми є захист вузлів доступу для роботи із зовнішніми мережами (включаючи Інтернет), структурованих кабельних мереж, мереж і систем зв'язку й телекомунікацій та ін.

3. Підсистема захисту прикладних програмних засобів і системного програмного забезпечення. Підсистема призначена для захисту мережевих операційних систем, мережних баз даних, систем керування базами даних, програмних систем рішення функціональних завдань і т.п. Як було показано вище, існування другого рівня неможливо без наявності першого, який, у свою чергу, пов'язаний із третім рівнем типової моделі.

Сформулюємо три базових теоретичних принципи, якими можна керуватися при побудові систем захисту інформації в міжнародних представництвах:

– принцип побудови єдиної й неподільної системи захисту інформації; суть підходу полягає в тому, що всі можливі види загроз відбиваються за допомогою системи захисту інформації (СЗІ), що

представляє собою єдиний і неподільний (монолітний) блок, у який об'єднані всі захисні ресурси й механізми, якими можна захистити інформаційну систему (ІС);

– блоковий принцип побудови системи захисту інформації; він припускає, що система будується із трьох функціональних блоків, кожний з яких є єдиним і неподільним («монолітним») та призначений для захисту тільки одного з рівнів моделі ІС;

– модульний принцип побудови системи захисту інформації; система, побудована відповідно до цього принципу, не просто складається із трьох функціональних блоків, кожен блок розбитий на менші за розміром елементи – модулі захисту. В результаті, у порівнянні з монолітної та блоковою СЗІ, у модульній менша глибина захисту, але вище мобільність – вона може відбивати велику кількість атак, що одночасно відбуваються з різних напрямків і на різних рівнях, і може оперативно реагувати на будь-які зміни складу технічних і програмних засобів всередині рівнів ІС.

Як свідчить іноземний досвід, організаційно-технічні заходи технічного захисту інформації (ТЗІ) у виділених приміщеннях, ІС та периметру корпоративних мереж, роботи з атестування виділених приміщень виконуються власними силами або передаються на аутсорсинг суб'єктам підприємницької діяльності у галузі захисту інформації, які мають дозвіл і ліцензію. Керівник компанії зобов'язаний вжити невідкладних заходів з усунення недоліків і реалізації пропозицій комісії відповідно до вимог нормативно-правових актів.

Також важливо зазначити, що у більшості випадків захист інформації як об'єкт досліджень не враховує аспект людської діяльності, або ж йому приділяється не достатньо велика увага. Проте, діяльнісний аспект відіграє значну роль в інформаційній безпеці, і сьогодні можна із впевненістю казати, що серед фахівців формується певний інтерес до розглядання проблем інформаційної безпеки у рамках системо-діяльнісного підходу.

Розглядаючи захист інформації як діяльність, слід зазначити, що ця системна категорія характеризується певними властивостями та характеристиками. Властивості – це об'єктивні особливості діяльності, які проявляються під час її здійснення. Захист інформації в свою чергу може бути охарактеризований з точки зору ефективності, цілеспрямованості, безперервності, організованості, керованості, узгодженості тощо.

Захист інформації має бути цілеспрямованим, стабільним, безперервним, організованим, керованим, узгодженим та вмотивованим, забезпечувати максимальну ефективність, бути адекватним загрозам та ризикам безпеки, сприйнятим та гнучким в реалізації, здійсненним на різних рівнях забезпечення безпеки інформації, достатньо простим в адміністративному забезпеченні.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Отже, як свідчить іноземний досвід, проведення роботи в галузі захисту інформації дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки організації, виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки організації, знизити потенційні втрати підприємства чи організації через підвищення стійкості функціонування корпоративної мережі, розробити концепцію та політику безпеки установи, а також запропонувати плани захисту конфіденційної інформації організації, що передається по відкритих каналах зв'язку, захисту інформації закладу від навмисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання чи використання.

Загалом кожен з принципів системи захисту інформації має свої переваги та недоліки, саме тому сьогодні на перший план висувається завдання розробки комплексних рішень на основі аналізу всіх процесів в СЗІ, включаючи зовнішні зв'язки, системи документообігу, організаційну структуру міжнародного представництва. При цьому система захисту

повинна бути максимально гнучкою й будуватися на принципах масштабованості та наступності впроваджуваних рішень.

Перспективи подальших досліджень у цій темі передбачають розгляд найбільш сучасних іноземних практик захисту електронної інформації та оцінки можливостей використання відповідного зарубіжного досвіду в Україні.

Література

1. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак; За ред. проф. В.О. Хорошка. – К. : ДУІКТ, 2008. – 533 с.
2. Гарасимчук О. І. Комплексні системи санкціонованого доступу / О. І. Гарасимчук, В. Б. Дудикевич, В. А. Ромака. – Львів : Львівська політехніка, 2010. – 212 с.
3. Системи менеджменту інформаційної безпеки / В. А. Ромака, В. Б. Дудикевич, Ю. Р. Гарасим, П. І. Гаранюк, І. О. Козлюк. – Львів: Львівська політехніка, 2012. – 232 с.
4. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, А. В. Платоненко // Сучасний захист інформації. – 2017. – № 2. – С. 90 – 94
5. Северинов А. В. Анализ угроз и рисков безопасности информации в беспроводных сетях / А. В. Северинов, В. И. Черныш // Системи управління, навігації та зв'язку. – Вип. 1. – К. : ЦНДІ НіУ, 2011. – С. 229 – 232.
6. Сєвєрінов О. В. Управління інформаційною безпекою згідно міжнародних стандартів / О. В. Сєвєрінов, В. І. Черниш, М. Є. Молчанова // Системи управління, навігації та зв'язку. – Вип. 4. – К. : ЦНДІ НіУ, 2011. – С. 250-253

7. Термінологічний словник з питань технічного захисту інформації /за ред. проф. В. О. Хорошка – 3-є видання. – К. : Поліграф Колсалтинг, 2012. – 268 с.
8. ISO 27001 Британского института стандартов [Электронный ресурс]. – Режим доступа: http://www.standardsdirect.org/iso17799.htm.