УДК 342.9

ДОВГАЛЬ Ю.С.

ОСОБЛИВОСТІ ПОБУДОВИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті досліджено актуальність питання побудови захисту інформаційних систем. Розглянуто два основні підходи до оцінки поточного стану захисту інформаційних систем. Визначено шкалу інформаційної безпеки відповідної комплексної інформації захисту інформації, а також розглянуто підходи щодо рівня захищеності інформаційних ресурсів на усіх етапах проектування та повсякденної організації інформаційної системи.

Ключові слова: *ідентифікація, ініціалізація, інформаційна безпека, інформаційна система, інформаційні ресурси, комплексна система захисту інформації, оцінка ризиків.*

В статье исследуется актуальность вопроса построения защиты информационных систем. Рассматриваются два основных подхода к оценке текущего состояния защиты информационных систем. Определена шкала информационной безопасности соответствующей комплексной информации защиты информации, а также рассмотрены подходы по уровню защищенности информационных ресурсов на всех этапах проектирования и повседневной организации информационной системы.

Ключевые слова: *идентификация, инициализация, информационная безопасность, информационная система, информационные ресурсы, комплексная система защиты информации, оценка рисков.*

This article examines the relevance of the question of building of protection information systems. We consider two basic approaches to assessing the current state of protection of information systems. Defined information security appropriate scale complex information protection information and discussed approaches to the protection of information resources in all phases of design and everyday information system.

Key words: *identification, initialization, information security, information systems, information resources, integrated system of information security, risk assessment.*

Вступ. Інформація та інформаційні системи, мережеве оточення, у яких вони функціонують, є невід'ємними складовими сучасного бізнес-середовища. Їх доступність, цілісність і конфіденційність можуть мати вирішальне значення для забезпечення конкурентоспроможності підприємств, установ, організацій незалежно від форм власності, руху коштів, рентабельності, відповідності правовим нормам і стандартам. Водночас унаслідок посилення залежності від інформаційних, комунікаційних систем і сервісів вони стають вразливішими до порушень режиму безпеки. Поширення інформаційних і комунікаційних систем надає нові можливості несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи обмежує можливості фахівців централізовано контролювати зазначені інформаційні системи.

Постановка завдання. Аналіз сучасного стану розвитку та особливості побудови захисту інформаційних систем є особливо актуальним питанням, адже успішне функціонування організації та її захист від сторонніх осіб значною мірою залежить від вдалого керівництва, яке базується на обґрунтуванні перспективних концепцій розвитку згідно з своєчасною, достовірною та повною інформацією, яку може поставляти відповідна інформаційна система. Тому метою статті є дослідження особливості побудови інформаційних систем.

Аналіз останніх досліджень та виокремлення нерозв'язаних проблем. Серед праць, які присвячені дослідженням методологічних, сутнісних та змістовних основ інформаційної безпеки, особливе місце займають теоретичні розробки Е. Бєляєва, М. Бусленка, С. Гриняєва, О. Данильяна, О. Дзьобаня, Г. Ємельянова, В. Лопатіна, О. Позднякова, Л. Сергієнка, В. Циганкова, М. Чеснокова та ін. Дослідженню питань правового регулювання телекомунікацій та інформатизацією приділяють значну увагу в науковій літературі такі автори, як В. Авер'янов, О. Амосов, Г. Атаманчук, І. Арістова, В. Афанасьєв, В. Бакуменко, В. Брижко, О. Бухтатий, Є. Григоніс, Л. Григорян, В. Дзюндзюк, Н. Єси-

© ДОВГАЛЬ Ю.С. – аспірант кафедри конституційного, адміністративного права та суспільних наук (Інститут права та суспільних відносин Відкритого міжнародного університету розвитку людини «Україна»)

пчук, В. Корженко, О. Крюков, О. Радченко, Ю. Тихомиров, В. Фурашев, О. Фурашев, В. Цимбалюк, М. Швець Л. Юзьков, О. Федорчак та інші дослідники.

Результати досліджень. Порушення режиму безпеки інформаційних систем може істотно ускладнити реалізацію виробничих завдань, тому вирішення проблеми формування ефективної системи захисту інформації набуває щораз важливого значення в умовах розширеного використання інформаційних систем. Це пояснюється тим, що у процесах розроблення й удосконалення систем захисту інформації є чимало недостатньо вивчених і досліджених аспектів, які можуть негативно впливати на показники ефективності та надійності функціонування інформаційної системи безпеки загалом.

Діяльність будь-якої сучасної організації багато в чому залежить від мережі Інтернет і тих сервісів, які вона надає. Водночас дуже гостро ставиться питання про можливість використання всіх привілеїв та переваг, що надає мережа Інтернет, з мінімальним ризиком для діяльності організації. Тому сьогодні на перший план виходить проблема забезпечення безпеки комп'ютерних інформаційних систем з боку мережевого впливу [1]. Цей сегмент удосконалюється і постійно розвивається, причому дуже динамічно.

Основними засобами захисту комп'ютерних інформаційних систем були, є і залишаються мережеві екрани (брандмауер, firewall, фільтрувальні маршрутизатори тощо). Мережеві екрани є лише інструментом системи безпеки. Вони надають певний рівень захисту і є засобом реалізації політики безпеки на мережевому рівні. Рівень безпеки, що надає мережевий екран, може варіюватися залежно від вимог безпеки. Існує традиційний компроміс між безпекою, простотою використання, вартістю, складністю тощо. Мережевий екран є одним з декількох механізмів, що використовують для управління і спостереження за доступом до мережі з метою її захисту [2].

Сьогодні ніхто не заперечуватиме важливості системи антивірусної безпеки в інформаційній інфраструктурі будь-якого підприємства, установи чи організації незалежно від форми власності. Це здебільшого найактуальніша система зі всіх розгорнутих систем забезпечення безпеки інформаційної системи. Звичайно, така ситуація виникла не сама собою, а зумовлена передусім обвальним зростанням кількості нових комп'ютерних вірусів.

Інформаційна безпека – це стан захищеності потреб інформації особистістю, суспільством і державою, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [3].

Варто відзначити, що задоволення потреб в інформації приводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і, як наслідок, – обґрунтованість рішень та дій, що ухвалюються [3].

Законодавчі заходи щодо захисту інформаційної системи, що полягають у виконанні чинних у державі або введенні нових законів, нормативних документів, настанов, що регулюють правову відповідальність посадових осіб за втрату або зміну інформації, що підлягає захисту, зокрема за спроби виконувати аналогічні дії за межами своїх повноважень, а також відповідальність сторонніх осіб за спробу несанкціонованого доступу до інформації. Мета правових заходів полягає у запобіганні можливим правопорушенням і встановленні відповідальності за здійснені правопорушення [4].

В Україні діє близько 60 нормативних актів, які безпосередньо або опосередковано стосуються регулювання відносин у сфері інформаційної безпеки. Окрім цього, діє низка відомчих актів, тлумачень, методик, які є обов'язковими для виконання всіма державними органами, підприємствами, установами, організаціями під час виконання функцій із забезпечення захисту інформації з обмеженим доступом, насамперед, це стосується державної таємниці. Регулятивно-правову основу забезпечення захисту інформації в інформаційних системах підприємств України різної форми власності становлять: Конституція України [5]; Концепція національної безпеки України [6]; Закони України «Про державну таємницю» [7]; «Про доступ до публічної інформації» [8]; «Про інформацію» [9]; «Про науково-технічну інформацію» [10] та інші Закони України, акти Президента України та постанови Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні угоди України з питань технічного захисту інформаційних систем, згода на обов'язковість яких надана Верховною Радою України.

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [11]. Саме на неї нормативними документами комплексної системи захисту інформаційних систем покладається завдання забезпечення вже згаданих функціональних властивостей захищених автоматизованих систем. Це завдання вирішується як технічними, так і програмними засобами базового і прикладного програмного забезпечення, а також з використанням спеціально розроблених програмних і апаратних засобів.

Для кожної конкретної інформаційної системи склад, структура та вимоги до комплексної системи захисту інформації визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації.

Організаційно-правовими заходами реалізується комплекс відповідних в нормативно-правовій базі держави адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності та засобів технічного захисту інформації, а також шляхом створення служб (або призначення адміністраторів технічного захисту інформації), відповідальних за їх реалізацію. До таких заходів належать також визначення контрольованих зон та організація контролю доступу в ці зони. Для реалізації заходів цієї групи в більшості випадків немає необхідності використання засобів, що є компонентами автономної системи [12].

Із кожним об'єктом інформаційної системи пов'язана деяка інформація, що однозначно ідентифікує його. Це можуть бути число, рядок символів, алгоритм, що підтверджують дійсність об'єкта. Визначимо таку інформацію як ідентифікатор об'єкта. Процес верифікації цього ідентифікатора назвемо ідентифікацією об'єкта. Якщо об'єкт має деякий ідентифікатор, зарезервований у мережі, він називається легальним об'єктом; інші об'єкти належать до нелегального [13].

Ідентифікація захищеного об'єкта – одна з функцій підсистеми захисту, що виконується в першу чергу, коли об'єкт намагається ввійти в мережу. Якщо процедура завершується успішно, об'єкт є легальним для цієї мережі.

Наступний крок – верифікація ідентифікатора об'єкта, що встановлює, що передбачуваний легальним об'єкт дійсно такий, яким себе повідомляє.

Після того як об'єкт ідентифікований і верифікований, мають бути встановлені його сфера діяльності і доступні ресурси інформаційної системи. Така процедура називається наданням повноважень. Перераховані три процедури ініціалізації належать до єдиного об'єкта інформаційної системи, і тому їх варто віднести до засобів захисту самого об'єкта.

Основними функціями, що мають здійснювати в цих цілях засоби захисту, є: ідентифікація суб'єктів і об'єкта; розмежування, а за потреби і повна ізоляція доступу до обчислювальних ресурсів та інформації; реєстрація дій у системі. Процедура ідентифікації і підтвердження дійсності припускає перевірку, чи є суб'єкт, що здійснює доступ до об'єкта, до якого здійснюється доступ, тим, за кого себе видає. У системах, що забезпечують високу безпеку, може знадобитися періодичний повторний огляд дійсності.

У процедурі ідентифікації використовуються різні методи: прості, складні чи одноразові паролі, обмін питаннями й відповідями з адміністратором через відповідну програму, ключі, магнітні карти, значки, жетони, засоби аналізу індивідуальних характеристик (голосу, відбитків пальців, геометричних параметрів рук чи обличчя), спеціальних ідентифікаторів чи контрольних сум для апаратури, програм і даних. Засоби реєстрації, як і засоби контролю доступу, належать до ефективних заходів протидії несанкціонованим діям. Однак якщо засоби контролю доступу призначені для запобігання таких дій, то завдання реєстрації – знайти вже виконані дії чи їхні спроби [13].

Як правило, для оцінки рівня захисту потрібно спочатку визначити поточний стан безпеки інформаційної системи. Сьогодні існують два підходи оцінки поточного стану безпеки інформаційної системи, а саме «дослідження знизу догори» та «дослідження згори донизу».

Використання першого підходу полягає у тому, що адміністратори починають перевіряти систему захисту на всі відомі їм види атак. Отже, адміністратори виступають в ролі зловмисників, які роблять спроби порушити захист інформаційної системи. Але відразу стає зрозуміло, що найталановитіші адміністратори не можуть знати усі можливі методи злому, а також усі програмно-апаратні засоби зловмисників [14].

Підхід «згори донизу» ґрунтується на детальному аналізі усіх відомих схем зберігання та обробки даних. Спочатку визначають інформаційні об'єкти та потоки захисту, а потім досліджують сучасний стан інформаційного захисту системи з метою визначення реалізованих методик захисту зазначених ресурсів, а також їх стан та рівень. Далі проводиться класифікація всіх інформаційних об'єктів за класами відповідно до їх конфіденційності, вимог до доступності та цілісності.

Останнім кроком є «оцінка ризику», що полягає у визначенні розміру збитків фірми через порушення захисту кожного конкретного інформаційного ресурсу. Наближеним ризиком називається добуток «можливого збитку від атаки» на «ймовірність цієї атаки». Як правило, оцінка ризику складається з аналізу ризиків та оцінювання збитку [14].

Під час аналізу ризиків проводиться інвентаризація та впорядкування інформаційних ресурсів, з'ясовуються нормативні, технічні, договірні вимоги до ресурсів у сфері безпеки інформаційної системи, після чого з урахуванням цих вимог визначають вартість ресурсів. У вартість входять усі потенційні витрати, пов'язані з можливим несанкціонованим доступом до інформаційних ресурсів, що захищаються. Наступним етапом аналізу ризиків є складання переліку переважних загроз та перелік вразливостей до них кожного інформаційного ресурсу, а потім обчислюється ймовірність реалізації можливих загроз чи атак. За стандартом [12] загрози інформаційної безпеки мають подвійне тлумачення, а саме: умова реалізації вразливості ресурсу (у цьому випадку вразливості та погрози ідентифікуються окремо); загальна потенційна подія, здатна привести до несанкціонованого доступу до інформаційного ресурсу (коли наявність можливості реалізації вразливості і є загрозою).

Встановлене значення ризику дає змогу визначити важливість для компанії кожного інформаційного ресурсу. Усі сучасні стандарти у сфері безпеки відображають сформований у міжнародній практиці загальний підхід до організації управління ризиками. Управління ризиками розглядається як базова частина системи менеджменту якості організації. Стандарти мають відверто концептуальний характер, що дає змогу експертам з інформаційної безпеки реалізувати будь-які методи, засоби й технології оцінки, відпрацювання та управління ризиками. У різних стандартах допускається використання кількісних та якісних методів оцінки ризику інформаційної безпеки, але немає обґрунтування та рекомендацій щодо вибору математичного та методологічного апарату. У додатку до стандарту [15] наводиться приклад якісного методу оцінювання, а саме використання три– та п'ятибальної оцінних шкал. За п'ятибальною шкалою рівні вартості ідентифікованого ресурсу оцінюють як «незначний», «низький», «середній», «високий», «дуже високий». За трибальною шкалою – як «низький», «середній», «високий». Загальні критерії оцінки безпеки мають застосовуватись на єдиній загальній методологічній основі, що ґрунтується на синтезі заходів, засобів та сервісів безпеки для мінімізації інформаційних ризиків. Використовують загальну методологію оцінки інформаційної безпеки експерти, розробники та замовники для оцінки й контролю інформаційної безпеки ресурсів [16].

На заключному етапі здійснюється всебічний аналіз технічного звіту оцінки органом контролю на предмет його відповідності загальним критеріям загальної методології та вимогам схем оцінки безпеки. На основі технічного звіту формується підсумковий звіт з оцінювання з рішенням про відповідність необхідним вимогам. Усі залучені в процес оцінювання сторони вивчають підсумковий звіт та мають право вимагати відповідних пояснень [14].

Більшість організацій з різних причин не мають можливості здійснити повну оцінку захисту інформаційних ресурсів, тому пропонується використовувати кількісну оцінку рівня захищеності. Її використання можливе на стадії впровадження. У результаті застосування кількісної оцінки є можливість точніше порівняти декілька варіантів захисту, що дає змогу вибрати найефективніший. Для її застосування визначають ймовірність виникнення загроз та вразливості інформаційних ресурсів, вартість ресурсів, що захищаються (оцінка втрати в разі виходу з ладу інформаційного ресурсу) та частоту загроз кожного виду в загальному потоці загроз. Обов'язковим є визначення обмежень на вартість системи захисту інформації та зниження рівня продуктивності системи [14].

Фактично рівень захисту визначається як відношення ризиків у захищеній системі до ризиків у незахищеній системі. Такий підхід дає змогу точніше описувати інформаційні ресурси через характерні для них вразливості, вартість самих ресурсів, ранжувати ризики та інформаційні ресурси за ступенем критичності для діяльності організації.

Висновки. На основі проведеного дослідження можна стверджувати, що основним проблемами під час розробки моделей захисту інформації комп'ютерної мережі автоматизованих систем є низький рівень аналітичної діяльності і хибність підходу, що пов'язаний у відсутності розгляду всіх структурних елементів та зв'язків між ними як системи. Потрібно чітко усвідомлювати, що основні складові системи є також взаємопов'язаними системами, що створює додаткові проблеми під час розробки моделей, та вимагає залучення висококваліфікованих та вузькоспеціалізованих спеціалістів з предметних областей, що охоплює система загалом. Потрібно використовувати вже наявні методи та моделі інформаційної безпеки, а також модернізувати їх та розробляти нові для конкретного завдання.

Точність результату встановлення ступеня захищеності інформаційної системи залежить передусім від повноти списку загроз і уражень як основних складових ризику, точності оцінки інформаційних ресурсів, а також точності оцінки ймовірнісних характеристик реалізації загроз. Перевагами такого підходу є нескладна реалізація, поширений математичний апарат, доступність для розуміння. Як недоліки можна зазначити, що цей підхід не забезпечує врахування особливостей функціональної взаємодії засобів захисту. Застосування розглянутого підходу щодо оцінки захисту інформаційних ресурсів зменшить витрати організації та забезпечить вибір найкращого засобу захисту.

Список використаних джерел:

1. Форристал Д. Защита от хакеров WEB-приложений. – ДМК, 2004. – 496 с.

2. Норткатт С. Защита сетевого периметра: наиболее полное руководство по брандмауэрам, виртуальным частным сетям, маршрутизаторам и системам обнаружения вторжений / С. Норткатт и др. ; науч. ред. Н.И. Алишов. – К.; М.; СПб. : DiaSoft, 2004. – 664 с.

3. Алишов Н.И. Организации безопасности информационных ресурсов в системах телекоммуникаций // Праці 4-ї Міжнародної науково-техничної конференції по телекомунікаціям – Телеком-99. – Одеса, 1999. – С. 112–115.

4. 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.

5. Конституція України : Закон України від 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

6. Про Концепцію національної безпеки України : Постанова Верховної Ради України від 16 січня 1997 р. №3/97-ВР // Відомості Верховної Ради України. – 1997. – № 10. – Ст. 85.

7. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/3855-12.

8. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. №2939-VI // Відомості Верховної Ради України. – № 16. – Ст. 93.

9. Про інформацію : Закон України від 2 жовтня 1992 р. №2657-XII [Електронний ресурс]. – Режим доступу : zakon.rada.gov.ua.

10. Про науково-технічну інформацію : Закон України від 25 червня 1993 р. №3322-XII // Відомості Верховної Ради України. – № 48. – Ст. 650.

11. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

12. Клеха О.В. Основні проблеми при побудові моделей захисту інформації в комп'ютерній мережі автоматизованих системах // Міжвузівський збірник «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». – Луцьк, 2012. – Вип. 8. – С. 42–46.

13. Козачок В.А. Особливості побудови комплексних систем захисту інформації в розподілених корпоративних мережах / В.А. Козачок, Ю.Б. Коваленко // Сучасний захист інформації. – 2015. – № 1. – С. 41–47.

14. Кононова В.О. Оцінка засобів захисту інформаційних ресурсів / В.О. Кононова, О.В. Харкянен, С.В. Грибков // Вісник Національного університету «Львівська політехніка». – 2014. – С. 99–105.

15. ISO/IEC 15408-2:1999 – Information technology – Security techniques – Code of practice for information security management.

16. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model.