УДК 004.056.5

Особливості організації інформаційної безпеки сучасної інформаційної системи та її економічна доцільність

Костюченко В.В.
магістр
Київського національного університету технологій та дизайну
Шиковець К.О.
доцент кафедри економічної кібернетики та маркетингу
Київського національного університету технологій та дизайну

У статті досліджено та класифіковано джерела загроз у процесі використання інформаційних ресурсів, запропоновано шляхи збереження цінності ресурсів та оцінено економічну ефективність витрат на інформційну безпеку. Розглянуто зростаючий вплив загроз інформаційній безпеці сучасної інформаційної системи та запропоновано способи її ефективного захисту. Узагальнено головні етапи побудови політики інформаційної безпеки, виділено підсистеми ефективного захисту інформації, розроблено рекомендації щодо проектування політики інформаційної безпеки.

Ключові слова: захист інформації, інформаційна система, інформаційна безпека, інформаційна технологія, антивірусний захист, політика інформаційної безпеки, конфіденційність інформації, цілісність інформації, криптографічний захист, несанкціонований доступ, економічна доцільність.

Костюченко В.В., Шиковец К.А. ОСОБЕННОСТИ ОРАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ЕЕ ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ

В статье исследованы и классифицированы источники угроз в процессе использования информационных ресурсов, предложены пути сохранения ценности информационных ресурсов и оценена экономическая эффективность затрат на информационную безопасность. Рассмотрено растущее влияние угроз информационной безопасности современной информационной системы и предложены способы ее эффективной защиты. Обобщены главные этапы построения политики информационной безопасности, выделены подсистемы эффективной защиты информации, разработаны рекомендации по проектированию политики информационной безопасности.

Ключевые слова: защита информации, информационная система, информационная безопасность, информационная технология, антивирусная защита, политика информационной безопасности, конфиденциальность информации, целостность информации, криптографическая защита, несанкционированный доступ, экономическая целесообразность.

Kostiuchenko V.V., Shikovets K.O. PECULIARITIES OF ORANIZING INFORMATION SECURITY OF THE CONTEMPORARY INFORMATION SYSTEM AND ITS ECONOMIC PERFORMANCE

The article explores and classifies the sources of threats in the process of using information resources, suggests ways to preserve the value of information resources, and assesses the economic effectiveness of costs for information security. The growing influence of threats to the information security of the modern information system is considered and methods for its effective protection are proposed. And also generalized the main stages of building the information security policy; The subsystems of effective information protection are allocated, recommendations on designing the information security policy are developed.

Keywords: Information security, information system, information security, information technology, anti-virus protection, information security policy, information confidentiality, information integrity, cryptographic protection, unauthorized access, economic feasibility.

Постановка проблеми у загальному вигляді. Актуальність теми зумовлена тим, що науковий аналіз чинної науково-правової бази України і загалом у світі доводить, що поняття державної безпеки (в усьому його змісті) досі залишається невизначеним. Сучасні дослідження інформаційної безпеки мають широкий спектр напрямів у межах як технічних, так і соціально-гуманітарних, зокрема правових, наук. Це висуває особливі вимоги до формування методологічних основ досліджень, які повинні забезпечувати розвиток цілісної галузі знань про інформаційну безпеку, повноту та об'єктивність її наповнення, що сприятиме втіленню принципів науковості і професіоналізму у практичному складнику забезпечення інформаційної безпеки і наближатиме його до оптимальності.

Аналіз останніх досліджень і публікацій. Проблематика захисту інформаційних систем вивчається багатьма зарубіжними та вітчизняними вченими, серед яких: С. Бармен, В. Гафнер, В. Домарєв, Д. Керр, С. Маднік, Г. Ємєльянов, У. Мусаєва та ін. У роботах цих учених висвітлюються основні теоретичні і практичні аспекти щодо можливого вдосконалення та розвитку комплексного захисту інформації. Утім, навіть у цих роботах є деякі упущення, які потрібно заповнити та дослідити: основні аспекти застосування політики інформаційної безпеки, її економічна доцільність та ефективні засоби захисту інформаційної системи.

Формулювання цілей статті (постановка завдання). Мета статті – аналіз наявного стану справ із виявлення і протидії інформаційним загрозам нашої держави, визначення нагальних проблем та формування на цій основі пропозицій щодо створення системи інформаційної безпеки в Україні.

Виклад основного матеріалу дослідження. Захист інформації перетворюється нині на одне з найактуальніших завдань унаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набуває особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані користувачів лише у захищеному вигляді в інформаційних системах (ІС).

Не менш важливим завданням уважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, майбутнє введення електронних паспортів та медичних карт, студентських квитків та залікових книжок; зрештою, все більше державних установ та приватних підприємств переходять на електронний документообіг, який до того ж вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасної інформаційної системи:

• протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;

• порушення встановлених регламентів збору, обробки та передачі інформації;

• навмисні дії та ненавмисні помилки користувачів інформаційних систем;

• помилки в проектуванні інформаційних систем;

• відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо [6].

Нині фахівцями досліджується досить широкий перелік загроз безпеці інформаційних систем, які класифікують за низкою ознак (рис. 1) [6].

Захист інформації – галузь науки і техніки, яка динамічно розвивається, пропонує ринку широкий спектр засобів для захисту даних. Проте жоден із них окремо взятий не може гарантувати адекватну безпеку інформаційної системи. Необхідною умовою ефективного захисту є проведення комплексу взаємодоповнюючих заходів [5].

Із липня 2003 р. в Україні введена кримінальна відповідальність за незаконне втручання в роботу комп'ютерів і комп'ютерних мереж, а також за поширення комп'ютерних вірусів, що призвело до спотворення, зникнення, блокування інформації чи її носіїв [3].

Сучасна організація повинна вміти належно будувати політику інформаційної безпеки, тобто розробляти й ефективно впроваджувати комплекс превентивних заходів із захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Головними етапами побудови політики інформаційної безпеки є:

1) реєстрація усіх ресурсів, які мають бути захищені;

2) створення переліку можливих загроз для кожного ресурсу;

3) оцінка ймовірності появи кожної загрози;

4) вжиття заходів, які дають змогу економічно ефективно захистити інформаційну систему.

Більшість фахівців у галузі захисту інформації вважає, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості

навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію).

Можна виділити такі підсистеми ефективного захисту інформації:

1. Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.

2. Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.

3. Підсистема міжмережного екранування, яка дає змогу реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.

4. Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.

5. Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.

6. Підсистема захисту від несанкціонованих дій інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку під час управління доступом і реєстрації.

7. Підсистема захисту систем управління базами даних.

8. Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів із протидії атакам хакерів і поширенню спаму.

9. Підсистема захисту мобільних пристроїв.

10. Підсистема моніторингу трансакцій порушення інформаційної безпеки, яка дає змогу

Рис. 1. Класифікація загроз безпеці інформаційної системи

своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

Нині спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом під час вибору того чи іншого варіанту є дотримання принципу розумної достатності, суть якого полягає у тому, що визначальними під час проектування політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Для оцінки ефективності корпоративної системи захисту інформації рекомендується використовувати деякі показники ефективності, наприклад сукупної вартості володіння (ТСО), коефіцієнти повернення інвестицій на ІБ (ROI) та ін.

Суттєво, що нині методика ТСО може бути використана для доказу економічної ефективності наявних корпоративних систем захисту інформації. Вона дає змогу керівникам служб інформаційної безпеки обгрунтовувати бюджет на ІБ, а також доводити ефективність роботи співробітників служби.

Але зрозуміло, що вміле керування ТСО дає змогу більш раціонально та економно реалізовувати кошти бюджету на ІБ, досягаючи при цьому прийнятного рівня захищеності компанії, адекватного поточним цілям та завданням бізнесу.

У цілому визначення витрат компанії на ІБ передбачає вирішення трьох завдань:

1) оцінки поточного рівня ТСО корпоративної системи захисту інформації та КІС у цілому;

2) аудиту ІБ підприємства на основі порівняння рівня захищеності підприємства і рекомендованого рівня ТСО;

3) формування цільової моделі ТСО.

Разом із методикою ТСО можна використовувати різноманітні методи для розрахунку повернення інвестицій (ROI). Як правило, для оцінки доходної частини спочатку аналізують ті цілі, завдання і напрями бізнесу, які потрібно досягти за допомогою впровадження або реорганізації наявних проектів у сфері системної інтеграції, автоматизації та інформаційної безпеки. Далі використовують деякі вимірні показники ефективності бізнесу для оцінки ефекту окремо за кожним рішенням, наприклад для скорочення операційних витрат, забезпечення прийнятної конкурентної спроможності, поліпшення внутрішнього контролю і т. д. Указані показники не треба вигадувати, вони є в достатній кількості. Далі можна використовувати методики розрахунку коефіцієнтів повернення інвестицій в інфраструктуру підприємства (ROI), наприклад також Gartner Group.

Досить результативно використовувати таку комбінацію: ТСО як витратну частину і ROI як розрахункову. Крім того, є й інші різноманітні методи і технології розрахунку та вимірювання різних показників економічної ефективності [4].

Для виключення зайвих витрат щодо захисту вся інформація ділиться на категорії відповідно до необхідного ступеню захисту. Цей ступінь визначається виходячи з:

- можливих збитків для власника за несанкціонованого доступу до інформації, що підлягає захисту;
- економічної доцільності подолання захисту для зловмисників.

Природно, виробляти таку оцінку для кожного документа було б дуже трудомістким, тому склалася практика визначення категорій секретності документів, по яких документи розподіляються за формальними ознаками. Наприклад, у наших державних органах прийнято дві категорії обмеження доступу: «для службового користування» та «таємно».

Для спрощення вирішення питань захисту слід застосовувати аналогічну схему. Видається інструкція, яка визначає, за якими ознаками документ (інформація) належить до тієї чи іншої категорії та які співробітники до якої категорії мають доступ.

Водночас безпека інформаційної системи має розглядатися як важливий складник загальної безпеки. Причому необхідне розроблення концепції ІБ, в якій слід передбачити не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але й відповідні заходи адміністративного та технічного характеру.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи із цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають

ураховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами.

Висновки з цього дослідження. В умовах відсутності стандартного підходу до оцінки ефективності роботи підрозділів інформаційної безпеки та їхнього внеску в загальний рівень безпеки витрати на забезпечення безпеки можуть зростати майже не корельовано з рівнем безпеки. Використання на стадії обґрунтування доцільності інвестицій у проекти інформаційної безпеки сучасних методів оцінки вартості інформаційних активів та ефективності їхнього захисту дасть змогу визначити критично важливі для бізнесу інформаційні активи і довести керівництву організації, що у витратах на їхній захист частка витрат на підтримку їхнього функціонування у стандартному режимі повинна бути збільшена, щоб забезпечити основну мету ефективного функціонування бізнес-процесів підприємства.

ЛІТЕРАТУРА:

1. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.

2. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К. : Держстандарт України, 1997. – 11 с.

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 18.04.2006 // Урядовий кур'єр. – 2006. – № 73. – Ст. 74.

4. Галкін А.П. Оцінка необхідності захисту інформації підприємства / А.П. Галкін. – 2009. – № 1. – С. 55–58.

5. Глушков В.М. Кибернетика, вычислительная техника, информатика. Избранные тр. : в 3-х т. / В.М. Глушков. – К. : Наукова думка. – 1990. – Т. 1. – 264 с. ; Т. 2. – 267 с. ; Т. 3. – 222 с.

6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

7. Остапов С.Є. Технології захисту інформації / С.Є. Остапов, С.П. Євсеєв, О.Г. Король. – Харків : ХНЕУ, 2013. – 476 с.

8. Schneier B. Applied Cryptography. Protocols, algorithms, source texts in C / B. Schneier. – 2002. – 816 p.

9. Singh S. The book of ciphers / S. Singh. – M. : AST : Astrel, 2007. – 447 p.

10. Stolings V. Cryptography and network protection / V. Stolings. – M. : Williams, 2004. – 848 p.