Тарас В. Рудий, Леся М. Томаневич, Ольга І. Руда

ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВ*

У статті розглянуто загальні принципи організації системи захисту інформації в інформаційних системах підприємств. Обґрунтовано запровадження принципу поетапного здійснення технічного захисту інформації з урахуванням динаміки зміни загроз.

Ключові слова: *інформаційні технології; інформаційна система; захист інформації; інформаційні загрози; технічні заходи.*

Рис. 1. Літ. 21.

Тарас В. Рудый, Леся М. Томаневич, Ольга И. Руда

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ КОМПАНИЙ

В статье рассмотрены общие принципы организации системы защиты информации в информационных системах предприятий. Обосновано внедрение принципа поэтапной реализации технической защиты информации с учетом динамики изменения угроз.

Ключевые слова: *информационные технологии; информационная система; защита информации; информационные угрозы; технические мероприятия.*

Taras V. Rudyi[1], Lesya M. Tomanevych[2], Olga I. Ruda[3]

THE FUNDAMENTALS OF INFORMATION SECURITY IN ENTERPRISES' INFORMATION SYSTEMS

The general principles of information security organization in enterprises information systems are considered. The principle of stepwise implementation of information technical protection is reasoned subject to the changing dynamics of threats.

Keywords: *information technologies; information systems; information security; information threats; technical measures.*

Постановка проблеми. Інформація та інформаційні системи (ІС) підприємств, 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 підприємства, руху коштів, рентабельності, відповідності правовим нормам і стандартам. Водночас, унаслідок посилення залежності підприємств від інформаційних, комунікаційних систем і сервісів вони стають вразливішими до порушень режиму безпеки. Поширення інформаційних і комунікаційних систем надає все нові можливості несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи обмежує можливості фахівців централізовано контролювати ІС та мережеве оточення.

Порушення режиму безпеки ІС може істотно ускладнити реалізацію виробничих завдань, тому вирішення проблеми формування ефективної систе-

* статтю підготовлено на основі доповіді на XII-му міжнародному науковому семінарі «Сучасні проблеми інформатики в управлінні, економіці, освіті та екології» (1–5 липня 2013 р., оз. Світязь – Київ).

[1] Lviv State Interior University, Ukraine.
[2] Lviv State Interior University, Ukraine.
[3] Lviv State Interior University, Ukraine.

© Тарас В. Рудий, Леся М. Томаневич, Ольга І. Руда, 2014

ми захисту інформації (ЗІ) набуває дуже важливого значення. Це пояснюється тим, що у процесах розроблення й удосконалення систем ЗІ є чимало недостатньо вивчених і досліджених аспектів, які можуть негативно впливати на показники ефективності та надійності функціонування системи безпеки загалом.

Вимогою сьогодення є необхідність вирішення питань фізичної безпеки, управління інцидентами, виконання законодавчих актів, стандартів, настанов.

Аналіз останніх досліджень. Питанням розробки і функціонування систем ЗІ присвячено значну кількість праці В.Б. Дудикевича [7; 18], М.П. Карпінського [20], О.С. Петрова [15; 21], В.О. Хорошка [15].

Аналіз наукових публікацій дає підстави стверджувати, що у процесі проектування, створення й експлуатування систем ЗІ трапляються помилки та недоречності, які суттєво знижують ефективність їх функціонування. Вимагає окремого обґрунтування розроблення політики інформаційної безпеки, яка визначає стратегію і тактику системи ЗІ в ІС підприємств і враховує динаміку процесів зміни типів і рівня загроз інформації, що є одним з активних і значущих ресурсів сучасного бізнес-середовища [17].

Система ЗІ в ІС підприємств повинна будуватися на засадах комплексності й адаптивності. Доцільно розробляти організаційну структуру і впроваджувати систему ЗІ в ІС підприємств відповідно до рекомендацій міжнародних стандартів і чинного законодавства України. Такими стандартами є: ISO/IEC 27002 «Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою" [9]; ISO/IEC 27003 «Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації" [10]; ISO/IEC 27004 «Інформаційні технології. Методи захисту. Вимірювання" [11]; ISO/IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки" [12]; ISO/IEC 27006 «Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою" [13]; ISO/IEC 27011 «Інформаційні технології. Керівництво з управління інформаційною безпекою для телекомунікацій" [14].

Дотримання принципів стандартів серії ISO 27000 забезпечує керування і контроль за доступом, розробкою й обслуговуванням апаратно-програмних систем, керування безперервністю бізнес-процесів. Відповідність вимогам ISO 27000 і дотримання національних правових норм з інформаційної безпеки є необхідними для сталого розвитку бізнесу.

Метою дослідження є визначення методів і засобів ЗІ в ІС підприємств. Пропонується використовувати набір організаційно-технічних методів і засобів, які дозволяють формувати ефективні системи ЗІ. Відзначимо, що ці методи є лише одним з аспектів реалізації цілісної концепції управління інформаційною безпекою ІС підприємства [7].

У публікації не розглядаються методи ЗІ, які ґрунтуються на системному адмініструванні та спеціальних математичних методах і алгоритмах. Основна увага зосереджена на розробці й аналізі організаційно-технічних заходів, які будуть зрозумілими і для менеджменту середньої ланки, і для керівництва підприємства.

Основні результати дослідження. Законодавчі заходи щодо ЗІ 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 [17].

Правову основу у вирішенні проблем ЗІ в Україні формують Конституція України [1], Закони України, акти Президента України та 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 інформації, згода на обов'язковість яких надана Верховною Радою України. В Україні діє близько 60 нормативних актів, які безпосередньо або опосередковано стосуються регулювання відносин у інформаційній сфері. 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 (ІзОД), насамперед, це стосується державної таємниці.

Регулятивно-правову основу забезпечення ЗІ в ІС підприємств України різної форми власності становлять: Конституція України [1]; Концепція національної безпеки України [6]; Закони України: «Про державну таємницю» [2]; «Про доступ до публічної інформації» [3]; «Про інформацію» [4]; «Про науково-технічну інформацію» [5].

Впровадження та дотримання вимог стандартів з питань ЗІ не може трактуватися як одномоментна, разова акція. Це, фактично, є безперервним процесом розробки, впровадження, функціонування, моніторингу, перегляду, підтримки та вдосконалення цілісної системи інформаційної безпеки як складової частини ІС підприємств.

З метою протидії процесам неконтрольованого витоку, несанкціонованого доступу (НСД), модифікування службової інформації та зменшення збитків від реалізація цих загроз потрібно фахово формувати заходи і вибирати засоби забезпечення ЗІ. Необхідно також володіти знаннями основних правових положень у цій галузі, вміти ефективно реалізовувати організаційні, програмно-технічні та інші заходи із забезпечення безпеки інформації.

Актуальність вирішення даної проблеми пов'язана із суттєвим зростанням можливостей сучасних інформаційних технологій (ІТ). Розвиток програмно-апаратних засобів, методів і способів обробки інформації та широке застосування ІТ роблять інформацію більш уразливою.

Процедура проектування системи ЗІ та вибору засобів ЗІ в ІС є складним комплексним завданням, при вирішенні якого потрібно враховувати різні типи ймовірних загроз для безпечного функціонування ІС, вартість реалізації ЗІ і наявність численних зацікавлених сторін.

При забезпеченні ЗІ основним елементом є процедура аналізу можливих загроз функціонуванню ІС, тобто загроз, що підвищують уразливість інфор-

мації, яка обробляється ІС, призводять до її неконтрольованого витоку, випадкового або цілеспрямованого модифікування, знищення.

Засоби системи ЗІ не варто проектувати, закуповувати або встановлювати доти, поки не буде виконаний аналіз ризиків та імовірних загроз [9]. Тільки ґрунтовний аналіз ризиків і загроз дає об'єктивну оцінку наслідків реалізації загроз, збитків від комерційних втрат, зниження коефіцієнта готовності системи ЗІ, правових проблем, інформацію для визначення найпридатніших методів і засобів забезпечення належного рівня безпеки ІС підприємств.

Розглядаючи загальні засади ЗІ в ІС, доцільно відзначити, що комплексний ЗІ в ІС передбачає використання спеціальних правових, фізичних, організаційних і програмно-апаратних засобів ЗІ, які повинні забезпечувати ідентифікацію й аутентифікацію користувачів, розподіл повноважень доступу до технічних, інформаційних ресурсів і сервісів ІС, реєстрування та облік спроб НСД.

Організаційні заходи ЗІ в ІС, як правило, спрямовані на чіткий розподіл відповідальності персоналу в процесах опрацювання інформації, створення декількох рубежів контролю, запобігання зовнішнім та інсайдерським загрозам, навмисному або випадковому знищенню й модифікуванню інформації.

Об'єктом технічного захисту, відповідно до чинного законодавства, є інформація, яка становить державну або іншу, передбачену чинним законодавством України, таємницю, службова інформація, яка є державною власністю або передана державі у володіння, користування, розпорядження.

Технічний захист інформації (ТЗІ) здійснюється у кілька етапів: перший етап – визначення і аналіз загроз; другий етап – розробка системи ЗІ; третій етап – реалізація плану ЗІ; четвертий етап – контроль за функціонуванням і керуванням системою ЗІ.

На першому етапі здійснюється ґрунтовний аналіз об'єктів ТЗІ, ситуаційного плану, умов функціонування ІС, оцінювання ймовірності прояву загроз та очікувані збитки від їх реалізація, підготовка даних для побудови моделі загроз.

Загрози можуть здійснюватися:

- технічними каналами, які включають канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи ЗІ або порушення цілісності інформації;
- НСД шляхом під'єднання до апаратури та ліній зв'язку, маскуванням під зареєстрованого користувача, подоланням заходів захисту Web-ресурсів, застосуванням закладних пристроїв, програм і вкоріненням комп'ютерних вірусів.

На другому етапі ТЗІ розробляється план, який містить організаційні, первинні технічні й основні технічні заходи захисту ІзОД, визначаються зони безпеки інформації. Організаційні заходи регламентують порядок інформаційної діяльності (ІД) з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ІД.

Первинні технічні заходи передбачають ЗІ блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають ЗІ з використанням засобів ТЗІ.

Заходи захисту інформації повинні:

- бути адекватними до загроз;
- бути розробленими з урахуванням можливих збитків від реалізація загроз і вартості захисних заходів та обмежень, які вносяться ними;
- забезпечувати задану ефективність ЗІ на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Мінімально необхідний рівень ЗІ забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

На третьому етапі ТЗІ слід реалізувати організаційні, первинні технічні й основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестування технічних засобів забезпечення інформаційної діяльності (ІД) підприємств, технічних засобів ЗІ, робочих місць (приміщень) на відповідність вимогам безпеки інформації [8].

ТЗІ передбачає застосування захищених програм і технічних засобів забезпечення ІД, програмних і технічних засобів ЗІ та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем.

На четвертому етапі здійснюється контроль за функціонуванням та управлінням системою ТЗІ на об'єктах ІД з метою визначення й удосконалення стану ЗІ в ІС, виявлення та запобігання порушенням системи ЗІ. Контроль стану ЗІ в ІС організовується відповідно до планів, затверджених керівниками підприємств, шляхом проведення перевірок.

Контрольно-інспекційна робота з питань ЗІ включає планування та проведення перевірок стану ЗІ в ІС, щодо яких здійснюється ТЗІ, проведення аналізу та надання настанов з удосконалення заходів щодо ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

Під час комплексної перевірки вивчається й оцінюється стан ЗІ в ІС, щодо яких здійснюється ТЗІ.

Під час цільової (тематичної) перевірки вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ЗІ в ІС, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності у галузі ТЗІ за відповідними дозволами та ліцензіями суб'єктами системи ЗІ.

Під час контрольної перевірки перевіряється усунення недоліків, які були виявлені попередньою комплексною або цільовою перевіркою. Відзначені перевірки можуть бути планові та позапланові, з попередженням та раптові.

Позапланова перевірка здійснюється за вказівкою вищого менеджменту підприємства у разі виникнення потреби визначення повноти та достатності заходів щодо ТЗІ за наявності відомостей про порушення виконання вимог нормативно-правових актів з питань ЗІ.

Перевірки здійснюються комісіями, на які покладено виконання завдань здійснення контролю за функціонуванням системи ЗІ. При проведенні перевірки стану ЗІ контролю підлягають організаційні, організаційно-технічні, тех-

нічні заходи ЗІ у виділених приміщеннях, ІС і периметру корпоративної мережі (КМ), повнота та достатність робіт з атестування виділених приміщень.

Контроль за організаційними заходами ЗІ в ІС включає перевірку:

- переліку відомостей, які підлягають захисту;
- окремої моделі загроз для ІС та периметру КМ;
- плану контрольованої зони, стосовно якої здійснюється ТЗІ;
- переліку виділених приміщень, щодо яких здійснюється ТЗІ, ІС та КМ;
- проведення категоріювання виділених приміщень та інформаційних активів підприємства.

Система менеджменту інформаційної безпеки (СМІБ) полягає в адаптації заходів ТЗІ до поточного завдання ЗІ. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізовуються якнайшвидше.

Варто зауважити, що СМІБ застосовують до обраного підприємством набору процесів функціонування, який є важливим для основного процесу функціонування підприємства, тобто визначається як сфера діяльності (СД) СМІБ. У СД повинні відзначатися критичні для функціонування підприємства процеси, від коректної роботи яких залежить присутність підприємства на ринку, його дохід тощо. Виконання цієї умови надає практичного сенсу впровадженню СМІБ – така система гарантуватиме безпечний процес функціонування підприємства.

За своєю суттю СМІБ є вибором і управлінням відповідними заходами захисту інформаційних активів ІС підприємства від визначених загроз відповідно до їх критичності функціонування [18].

Ще одним аспектом запровадження СМІБ є зменшення й оптимізація вартості підтримки системи безпеки. Фінансуватимуться тільки ті напрямки безпеки, які ліквідовують найнебезпечніші ризики. Об'єктивне оцінювання зв'язку «збиток-імовірність» дасть змогу постійно ефективно фінансувати систему ЗІ підприємства (рис. 1).

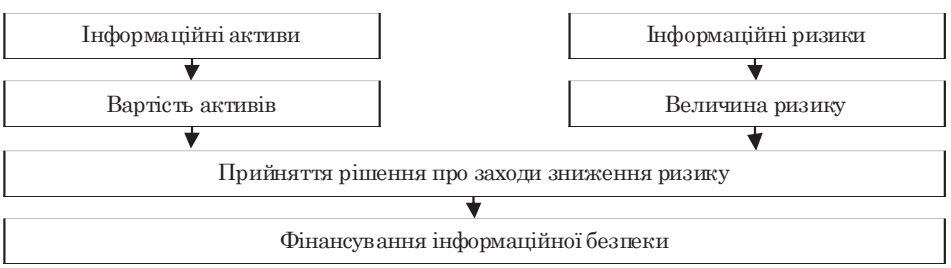

Рис. 1. **Схема прийняття рішення про фінансування інформаційної безпеки** [18]

Висновки. Вищевикладене дає підстави стверджувати, що система ЗІ в ІС підприємств повинна будуватися на засадах комплексності й адаптивності.

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

Організаційно-технічні заходи ТЗІ у виділених приміщеннях, ІС та периметру КМ, роботи з атестування виділених приміщень виконуються власними силами або передаються на аутсорсинг суб'єктам підприємницької діяльності у галузі ЗІ, які мають дозвіл і ліцензію від уповноваженого Кабінетом Міністрів України органу.

Керівник підприємства зобов'язаний вжити невідкладних заходів з усунення недоліків і реалізації пропозицій комісії відповідно до вимог нормативно-правових актів з питань ЗІ.

1. Конституція України // zakon.rada.gov.ua.
2. Про державну таємницю: Закон України від 21.01.1994 №3855-XII // zakon.rada.gov.ua.
3. Про доступ до публічної інформації: Закон України від 13.01.2011 №2939-VI // zakon.rada.gov.ua.
4. Про інформацію: Закон України від 02.10.1992 №2657-XII // zakon.rada.gov.ua.
5. Про науково-технічну інформацію: Закон України від 25.06.1993 №3322-XII // zakon.rada.gov.ua.
6. Про Концепцію національної безпеки України: Постанова Верховної Ради України від 16.01.1997 №3/97-ВР // zakon.rada.gov.ua.
7. *Гарасимчук О.І., Дудикевич В.Б., Ромака В.А.* Комплексні системи санкціонованого доступу: Навч. посібник. – Львів: Львівська політехніка, 2010. – 212 с.
8. *Когут В.В., Рудий Т.В., Кулешник Я.Ф.* Порядок атестування систем технічного захисту інформації // Проблеми діяльності кримінальної міліції в умовах розбудови правової держави: Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ (12 березня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 90–97.
9. Міжнародний стандарт ISO/IEC 27002 // www.iso27000security.com.
10. Міжнародний стандарт ISO/IEC 27003 // www.iso27000security.com.
11. Міжнародний стандарт ISO/IEC 27004 // www.iso27000security.com.
12. Міжнародний стандарт ISO/IEC 27005 // www.iso27000security.com.
13. Міжнародний стандарт ISO/IEC 27006 // www.iso27000security.com.
14. Міжнародний стандарт ISO/IEC 27011 // www.iso27000security.com.
15. Нормативне забезпечення інформаційної безпеки: Підручник / 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.
16. *Северинов А.В., Черныш В.И.* Анализ угроз и рисков безопасности информации в беспроводных сетях // Системи управління, навігації та зв'язку. – Вип. 1. – К.: ЦНДІ НіУ, 2011. – С. 229–232.
17. *Сєвєрінов О.В., Черниш В.І., Молчанова М.Є.* Управління інформаційною безпекою згідно міжнародних стандартів // Системи управління, навігації та зв'язку. – Вип. 4. – К.: ЦНДІ НіУ, 2011. – С. 250–253.
18. Системи менеджменту інформаційної безпеки: Навч. посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк. – Львів: Львівська політехніка, 2012. – 232 с.
19. *Шорошев В.В.* Основи формування політики безпеки комп'ютерних систем: Наук. видання. – К.: Бизнес и безопасность, 2006. – 141 с.
20. *Karpinski, M.* (2012). Information Security. Warsaw: Measurements, Automation and Monitoring. 280 p.
21. *Lahno, V.A., Petrov, A.S.* (2012). The information protection in automated systems on transport: Monograph. Krakow (Poland): Knowledge Press. 169 p.

Стаття надійшла до редакції 30.08.2013.