УДК 004.43

Рудий Т.В., к.т.н., доцент, **Бичинюк І.В.**, викладач,
Довганик Б.С., викладач©
Львівський державний університет внутрішніх справ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ АПК

Розглядаються загальні принципи організації системи захисту інформації у інформаційних системах підприємств АПК. Обґрунтовано запровадження принципу поетапного здійснення захисту інформаційних систем з урахуванням динаміки зміни загроз.

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

Постановка проблеми. Широке впровадження у системи менеджменту підприємствами, системи підтримки управлінських рішень сучасних інформаційних систем (ІС) вимагає забезпечення надійного захисту оброблюваної у ІС інформації. Порушення безпеки функціонування ІС може істотно ускладнити виконання управлінських рішень і виробничих завдань, тому проблема створення ефективної системи захисту інформації (ЗІ) набуває дуже важливого значення. Автори вважають, що така система ЗІ повинна бути, у першу чергу, комплексною і адаптивною.

Аналіз останніх досліджень. Проблемам створення і функціонування систем ЗІ присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах. З доступних, для пересічного користувача, джерел хочемо відзначити праці таких вчених як В.Б. Дудикевич, М.П. Карпінський, В.М. Максимович, В.П. Захаров. Важливість наукового здобутку та внеску у теорію і практику інформаційної безпеки (ІБ) згаданих вчених важко переоцінити.

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування систем ЗІ є суттєві недоліки, які знижують ефективність їх функціонування. Необхідно обґрунтувати розробку організаційно-правових засад ЗІ, які визначать стратегію, тактику системи ЗІ, а також врахують динаміку змін загроз інформаційним активам ІС.

Мета даної публікації полягає у тому, щоб окреслити організаційно-правову структуру системи ЗІ у ІС підприємств АПК. Разом з тим відзначимо, що це є всього лише однин з аспектів стратегії системи управління інформаційними технологіями (ІТ) стосовно підприємств АПК.

Виклад основного матеріалу. Правову основу ЗІ у ІС підприємств АПК становлять: Конституція України; 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, згода на обов'язковість яких надана Верховною Радою України. Видано низку відомчих актів Держкомсекретів України – циркулярних листів, тлумачень, методик тощо, які є обов'язковими для усіх державних органів, підприємств, установ, організацій під час здійснення ними функцій щодо забезпечення захисту службової інформації, перш за все – державної таємниці.

Регулятивно-правову основу забезпечення ЗІ у ІС підприємств АПК України становлять: Конституція України; Концепція національної безпеки України; Закони України "Про інформацію", "Про науково-технічну інформацію", "Про державну таємницю", "Про національний архівний фонд та архівні установи", "Про зв'язок", "Про видавничу справу", "Про доступ до публічної інформації", "Про захист персональних даних".

Організаційно-правова структура системи ЗІ в ІС формується відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою [1,2,3,4].

У всіх аспектах забезпечення ЗІ основним елементом є аналіз можливих загроз щодо порушення роботи ІС, тобто загроз, які підвищують уразливість інформації, призводять до її витоку, випадкового або навмисного компрометування, знищення [5]. Розглядаючи загальні принципи ЗІ в ІС, доцільно відзначити, що комплексний ЗІ в ІС має у своїй основі використання організаційних та програмно-апаратних засобів ЗІ. Такі засоби повинні забезпечувати ідентифікацію та автентифікування користувачів, розподіл повноважень доступу до активів ІС, реєстрування та облік спроб НСД.

Система ЗІ реалізовується у кілька етапів: перший етап – визначення і аналіз загроз; другий – розробка системи ЗІ; третій етап – реалізація плану ЗІ; четвертий етап – контроль за функціонуванням та управлінням системою ЗІ.

На першому етапі здійснюється ґрунтовний аналіз об’єктів ЗІ, ситуативного плану, умов функціонування ІС, оцінювання ймовірності прояву загроз та збитки від їх реалізації, підготовка даних для побудови моделі загроз.

На другому етапі розробляється план, який містить організаційні, первинні технічні та основні технічні заходи ЗІ. Організаційні заходи регламентують порядок інформаційної діяльності (ІД) з урахуванням норм і вимог ЗІ. Мінімально необхідний рівень ЗІ забезпечується обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Третій етап реалізує організаційні, первинні технічні та основні технічні заходи ЗІ, встановлюються необхідні зони безпеки інформації, проводиться атестування технічних засобів забезпечення ІД [6], технічних засобів ЗІ на відповідність вимогам безпеки. Система ЗІ передбачає використання захищеного, ліцензійно чистого програмного забезпечення, технічних засобів ЗІ та контролю ефективності, які мають сертифікат відповідності вимогам нормативних документів або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу.

На четвертому етапі здійснюється контроль за функціонуванням системи 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 ЗІ включає планування та проведення перевірок стану ЗІ в ІС, проведення аналізу та надання настанов з удосконалення заходів ЗІ. Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

Під час комплексної перевірки вивчається та оцінюється стан ЗІ у ІС, щодо яких здійснюється ЗІ. Цільова (тематична) перевірка полягає у вивченні окремих напрямків ЗІ, перевіряється виконання рішень (розпоряджень, наказів, настанов) з питань ЗІ в ІС, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності у галузі ЗІ за відповідними дозволами та ліцензіями суб'єктами системи ТЗІ.

Під час контрольної перевірки перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки. Такі 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 з ЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ЗІ.

Керування системою ЗІ полягає у адаптуванні заходів до поточного завдання ЗІ. За фактами зміни умов здійснення або виявлення нових загроз заходи ЗІ реалізовуються у найкоротший термін.

Контроль організаційних заходів ЗІ в ІС включає перевірку: переліку відомостей, які підлягають ЗІ; окремої моделі загроз для ІС; плану контрольованої зони підприємства, щодо якого здійснюється ЗІ; переліку

виділених приміщень підприємства, щодо якого здійснюється ЗІ; проведення категоріювання інформаційних активів та об'єктів.

При категоріюванні інформаційних активів та об’єктів основною складністю є те, що важко визначити їх цінність. Фахівцям з інформаційної безпеки потрібно розробити ефективні методики і критерії категоріювання інформаційних активів. Відзначимо, що визначення цінності інформаційних активів дійсно дуже складний процес [7].

Сформульовані правила фіксуються у відповідних документах (документування процедур – одне з основних вимог стандарту ISO 27001). Наголосимо, що основним документом є політика інформаційної безпеки (ПІБ), у якій перераховані всі процедури, визначено ступінь відповідальності посадових осіб за забезпечення ІБ, а також позиція керівництва. Автори вважають, що ПІБ у ІС підприємства є багаторівневою системою документів, які визначають вимоги безпеки, систему заходів, відповідальність персоналу та механізми контролю задля забезпечення захисту інформації у ІС. ПІБ розповсюджується на всі аспекти діяльності ІС та застосовується до всіх інформаційних активів, які можуть мати матеріальний інтерес для кримінальних структур та конкурентів у разі несанкціонованого витоку.

Організаційно-технічні заходи ЗІ у ІС, роботи з атестування об’єктів інформаційної діяльності 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 [8].

Висновки. На підставі проведеного аналізу автори вважають, що ефективна система ЗІ повинна бути, у першу чергу, комплексною і адаптивною, а у другу чергу – задовольняти умови спостережливості та керованості.

Запропоновані організаційно-правові засади формування системи безпеки дають можливість визначати стратегію і тактику системи ЗІ з урахуванням динаміки зміни загроз інформаційним активам ІС підприємств АПК.

Література

1. Міжнародний стандарт ISO/IEC 27002 [Електронний ресурс]. – Режим доступу: http://www.wikitntu.org.ua.

2. Міжнародний стандарт ISO/IEC 27003-27004 [Електронний ресурс]. – Режим доступу: http://www.iso27001security.com.

3. Міжнародний стандарт ISO/IEC 27005 [Електронний ресурс]. – Режим доступу: http://www.riskmanagementinsight.com.

4. Міжнародний стандарт ISO/IEC 27006 [Електронний ресурс]. – Режим доступу: http://27000.org.

5. Рудік В.М. Аналіз злочинів, скоєних з використанням інформаційних технологій / В.М. Рудік, Т.В. Рудий, В.М. Фірман / Проблеми

застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 14 грудня 2012 р. – Львів: Львівський державний університет внутрішніх справ, 2012. – С. 96-99.

6. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах оперативних підрозділів МВС / Т.В. Рудий, Я.Ф. Кулешник, І.В. Бичинюк, Є.Г. Горпинченко / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 14 грудня 2012 р. – Львів: Львівський державний університет внутрішніх справ, 2012. – С. 18-21.

7. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник / 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: Львівський державний університет внутрішніх справ, 2010. – С. 90-97.

8. Руда О.І. Аутсорсинг у сфері інформаційних технологій / О.І. Руда, І.І. Руда. / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 24 грудня 2010 р. – Львів: Львівський державний університет внутрішніх справ, 2010. – С. 196-200.

Summary

Rudyy T., Bychynyuk I., Dovganyk B.
Lviv State University of Internal Affairs

ORGANIZATIONAL AND LEGAL PRINCIPLES OF PROTECTION INFORMATION SYSTEMS ENTERPRISES AIC

The general principles of information security in information systems enterprises AIC. Proved the principle of phased implementation of technical protection of information in view of changes threats.

Key words: *information technology, information systems, information security, information threats, technical measures.*

Рецензент – к.е.н., доцент Колос Б.О.