УДК 004.056.53

ОСНОВНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Драб Ю., Ящук В.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто методи проведення атак на системи захисту інформації, проаналізовано дії реального порушника контурів захисту інформації, наведено етапи створення систем захисту інформації. Запропоновано підходи до побудови системи управління інформаційною безпекою відповідно до стандарту ISO 2700, що надає підприємству конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, та збільшує капіталізація компанії.

Ключові слова: *захист інформації, системи управління інформаційною безпекою, система захисту інформації, несанкціонований доступ.*

The methods of carrying out attacks on information protection systems are considered, the actions of the real violator of information protection circuits are analyzed, the stages of creation of information protection systems are given. Approaches to building an information security management system in accordance with the ISO 2700 standard are proposed, which gives the company a competitive advantage, demonstrating the ability to manage information risks and increase the company's capitalization.

Key words: *information protection, information security management systems, information protection system, unauthorized access.*

Розвиток інформаційно-комунікаційних систем відіграє важливу роль у життєвому циклі більшості підприємств. Проблеми захисту та оцінки даних інформаційних систем в умовах пандемії набувають особливої актуальності. У сучасному світі інформація є найціннішим ресурсом. Для забезпечення необхідного рівня безпеки інформації необхідно регулярно проводити аудит безпеки інформаційних систем.

Головна мета захисту інформації полягає у тому, щоб виключити можливість їх несанкціонованого використання або втрат у відповідному середовищі. Важливим напрямом протидії таким ситуаціям є проведення періодичних перевірок захищеності системи шляхом тестувань на проникнення. Такий метод ґрунтується на реалізації різних способів проникнення до інформаційно-комунікаційної мережі, що імітують дії реального порушника. Це дозволить отримувати фактичні результати з питань дослідження рівня та стану інформаційної безпеки.

Інвестиції в сферу забезпечення інформаційної безпеки підвищать конкурентоспроможність підприємства на ринку. Нездатність належним чином захистити свої ресурси може призвести до непоправних збитків, а в деяких випадках – до банкрутства. Аналіз сьогоднішнього ландшафту

кіберзагроз дає зрозуміти, що недостатньо інвестувати тільки в захист. Підприємства повинні покращувати загальну стратегію безпеки, а це означає, що інвестиції в захист, виявлення і реагування повинні бути узгоджені.

Сучасна практика з питань інформаційної та кібербезпеки розрізняє та виділяє декілька основних методів проведення атак на системи захисту інформації, серед яких вирізняються як суто технічні методи (апаратне та програмне забезпечення), так і методи, що пов'язані із використанням психологічних та соціологічних прийомів впливу на людей, маніпуляцією людським фактором.

Однією з прогалин у системі захисту інформації є відсутність уніфікованої моделі захисту інформації. Більша частина дослідників згодна між собою в загальній концепції щодо етапів формування системи захисту інформації, що була запропонована в стандарті НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційнотелекомунікаційній системі" [3]. Дана загальна концепція визначає наступні основні етапи створення систем захисту інформації в різних суб'єктах господарювання (рис. 1).

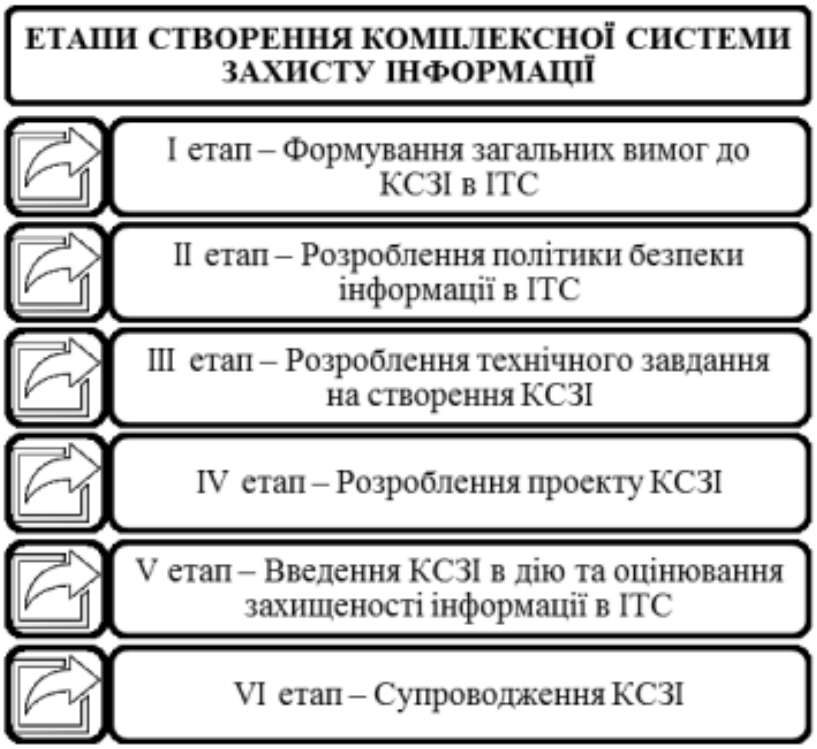

Рис.1. Етапи створення комплексної системи захисту інформації (розроблено авторами на основі [3])

Відсутність уніфікованої моделі захисту інформації актуалізує процес розроблення системи управління інформаційною безпекою (Information Security Management System, ISMS), як частини загальної системи управління, що базується на аналізі ризиків і призначена для проектування, ре-

алізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Побудова СУІБ дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування тощо. Одним із ключових чинників успішності системи управління інформаційною безпекою підприємства є побудова її на базі міжнародних стандартів ISO/IEC 27001. Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

СУІБ і сертифікація на відповідність стандарту ISO 27001 дає підприємству такі переваги, як управління інформаційною безпекою в межах єдиної корпоративної політики, управління ризиками та їх своєчасне виявлення, зниження ризиків від зовнішніх і внутрішніх загроз, систематизація процесів забезпечення ІБ, встановлення пріоритетів підприємства в області ІБ. У свою чергу це забезпечує підприємству конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, при цьому також збільшується капіталізація компанії.

Таким чином, в процесі проведеного дослідження визначено роль процесу захисту інформації в інформаційно-комунікаційних системах та мережах, класифіковано методи захисту, визначено порядок формування систем захисту інформації, їх використання, окреслено стандарти, що стосуються захисту інформації.

Література

1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p.

2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p.

3. Нормативні документи з питань захисту інформації ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]. – Режим доступу: http://surl.li/gnbi.

4. ISO 27001:2005 «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги».