УДК 004.056

РИЗИКИ ІНСАЙДЕРСЬКИХ ЗАГРОЗ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВ

Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
vladkorchin@ukr.net

РИСКИ ИНСАЙДЕРСЬКИХ УГРОЗ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЙ

Корчинский В.В., Аль-Файюми Халед, Копытин Ю.В., Копытина М.В.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
vladkorchin@ukr.net

THE RISKS OF ISIDER THREATS IN INFORMATION SECURITY SYSTEMS OF ENTERPRISE

Korchynskyi V.V., K. Alfaion, Kopytin Y.V., Kopytina M.V.

O.S. Popov Odessa National Academy of Telecommunications,
1 Kuznechna St., 65029, Ukraine, Odessa.
vladkorchin@ukr.net

Анотація. Розвиток інформаційних технологій обумовлює необхідність розробки методів і засобів, що забезпечують стійкість систем захисту інформації підприємства. Інсайдерська загроза являє собою одну з найбільш серйозних і наростаючих проблем для систем інформаційної безпеки підприємства в будь-якій області діяльності людства, що вимагає прийняття відповідних заходів по її запобіганню. Ефективне реагування на інсайдерську загрозу є необхідною умовою для успішної реалізації будь-якої системи безпеки. Оптимальний спосіб боротьби з цією проблемою полягає в прийнятті низки ефективних і послідовних нормативних заходів мінімізації інсайдерських загроз. Поряд з існуючими методами і засобами управління ризиками інформаційної безпеки дана проблема не вирішена повною мірою, про що свідчать статистичні звіти крупних зарубіжних компаній про внутрішні інциденти та загрози. За даними різних досліджень загрози інформаційної безпеки з боку інсайдерів становить до 80%, тобто можуть породжуватися всередині самої організації. Актуальність теми дослідження обґрунтовується рішенням найважливішої наукової задачі - розробка методів і засобів мінімізації ризиків інсайдерських загроз у системах захисту інформації підприємства. Метою дослідження є аналіз та мінімізація ризиків інсайдерських загроз в системах захисту інформації підприємства. У статті розглянуто ризики інсайдерських загроз та наведена класифікація дій працівників підприємства, що приводить до інсайдерства. Запропоновано алгоритм оцінки роботи в системах захисту інформації для завдання аналізу ризиків інсайдерских загроз та вживання заходів щодо їх зниження.

Ключові слова: інсайдери, загрози, атаки, ризики, інциденти, система захисту інформації.

Аннотация. Развитие информационных технологий обуславливает необходимость разработки методов и средств, обеспечивающих устойчивость систем защиты информации предприятия. Инсайдерская угроза представляет собой одну из наиболее серьезных и нарастающих проблем для систем информационной безопасности организации в любой области деятельности человечества, требует принятия соответствующих мер по ее предотвращению. Эффективное реагирование на инсайдерскую угрозу является необходимым условием для успешной реализации любой системы безопасности. Оптимальный способ борьбы с этой проблемой заключается в принятии ряда эффективных и последовательных нормативных мер минимизации инсайдерских угроз. Наряду с существующими методами и средствами управления рисками информационной безопасности данная проблема не решена в полной мере, о чем свидетельствуют статистические

отчеты крупных зарубежных компаний о внутренних инцидентах и угрозах. По данным различных исследований угрозы информационной безопасности со стороны инсайдеров составляют до 80%, то есть могут порождаться внутри самой организации. Актуальность темы исследования обосновывается решением важнейшей научной задачи - разработка методов и средств минимизации рисков инсайдерских угроз в системах защиты информации предприятия. Целью исследования является анализ и минимизация рисков инсайдерских угроз в системах защиты информации предприятия. В статье рассмотрены риски инсайдерских угроз и представлена классификация действий работников предприятия, которые приводят к инсайдерству. Предложен алгоритм оценки работы в системах защиты информации для задачи анализа рисков инсайдерских угроз и принятия мер по их снижению.

Ключевые слова: инсайдеры, угрозы, атаки, риски, инциденты, система защиты информации.

Abstract. The development of information technology determines necessity the development of methods and tools to ensure the sustainability of information security systems. The insider threat is one of the most serious and growing problems for information security systems of the organization in any area of human activity and requires the adoption of appropriate measures to prevent it. The effective response to the insider threat is the necessary condition for the successful implementation of any security system. The optimal way to deal with this problem is to accept the number of effective and consistent regulatory measures to minimize insider threats. Along with the existing methods and means of information security risk management, this problem has not been fully solved, as evidenced by the statistical reports of large foreign companies about internal incidents and threats. According to various researches, the threats of information security by insiders is up to 80%, that is, they can arise from within the organization itself. The relevance topic of the research is justified by solving the most important scientific problem - the development methods and means of minimizing risks of insider threats in information security systems of enterprise. The aim of the research is to analyze and minimize the risks insider threats in information security systems of enterprise. In the article considers the risks of insider threats and presents the classification of the actions of enterprise employees that lead to insider trading. The algorithm is proposed for evaluating the work in information security systems for the task of analyzing the risks insider threats and taking measures to reduce them.

Key words: insiders, threats, attacks, risks, incidents, information security system.

Розвиток національного законодавства у сфері інформаційної безпеки розпочався після прийняття в 1994 році Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [1]. При цьому важливим завданням є адаптація національного законодавства до вимог Європейського Союзу, що обумовлюється інтенсивним розвитком інформаційного законодавства, зокрема про інформаційну безпеку. Прийняті закони України «Про захист персональних даних» [2], «Про електронний цифровий підпис» [3], «Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації» [4].

Розвиток інформаційних технологій обумовлює необхідність розробки методів і засобів, які забезпечують стійкість систем захисту інформації (СЗІ). Особливо це важливо, коли мова йде про протидію внутрішнім загрозам, джерелами яких є свідомі або несвідомі дії співробітників підприємства, що зумовлює їх як потенційних інсайдерів.

Інсайдерська загроза являє собою одну з найбільш серйозних і наростаючих проблем для систем інформаційної безпеки організації в будь-якій області діяльності людства, що вимагає прийняття відповідних заходів по її запобіганню. Ефективне реагування на інсайдерську загрозу є необхідною умовою для успішної реалізації будь-якої системи безпеки. Оптимальний спосіб боротьби з цією проблемою полягає в прийнятті ряду ефективних і послідовних нормативних заходів мінімізації інсайдерських загроз, тому тема дослідження є актуальною. **Метою роботи** є аналіз та мінімізація ризиків інсайдерських загроз в СЗІ підприємства.

Розглянемо основні фактори, які необхідно взяти до уваги для вирішення поставленої задачі. На рис. 1 показана класифікація дій працівників підприємства, що приводить їх до інсайдерства. Практично всі працівники підприємства є потенційними інсайдерами. Проте з урахуванням дій працівників інсайдерство може бути навмисним або ненавмисним. Ненавмисне інсайдерство означає неумисні дії працівника, які призводять до

розголошення конфіденційної інформації. Таким чином, несвідомі дії співробітників, які призводять до інцидентів і ризиків порушення СЗІ, переводить їх у категорію інсайдерів. Слід відзначити, що причиною цього є недбалість працівників або втрати ними інформації в результаті попадання під вплив сторонніх осіб, тобто маніпуляції.

Рисунок 1 – Класифікація дій працівників підприємства, що призводить до інсайдерства

Однак більш проблематичною є категорія навмисних інсайдерів, які свідомо і цілеспрямовано здійснюють дії з метою порушення цілісності СЗІ, наприклад, це може бути саботаж, зрада, шпигунство. Як правило, це більш підготовлена категорія співробітників, що володіє всіма необхідними навичками для організації витоку конфіденційної інформації підприємства. Вочевидь, що кожен вид інсайдерства несе внутрішні загрози і призводить до збитків підприємства, величина яких залежить від ступеня важливості втраченої інформації. З урахуванням неправомірних дій інсайдерів можна виділити наступні загрози: розголошення і крадіжка конфіденційної інформації; порушення авторських прав на інформацію; нецільове використання ресурсів компанії та інше. Для мінімізації ризиків інсайдерських загроз пропонується проводити оцінку готовності СЗІ підприємства протидіяти внутрішнім атакам з урахуванням рекомендованих вимог [4].

На рис. 2 показані алгоритм оцінки роботи СЗІ для завдання аналізу й ухвалення рішення щодо зменшення ризиків інсайдерських загроз. При цьому, для порівняльного аналізу пропонується порівнювати роботу двох СЗІ підприємства. У першому випадку підприємство при побудові СЗІ буде використовувати повний набір вимог і рекомендації для забезпечення максимальної захищеності від інсайдерських загроз. В іншому випадку, підприємство, з метою зменшення витрат S_2 на СЗІ, обмежиться мінімальним набором

засобів захисту інформації від інсайдерства. З цієї причини величина витрат S_1 першої СЗІ буде більше, ніж S_2.

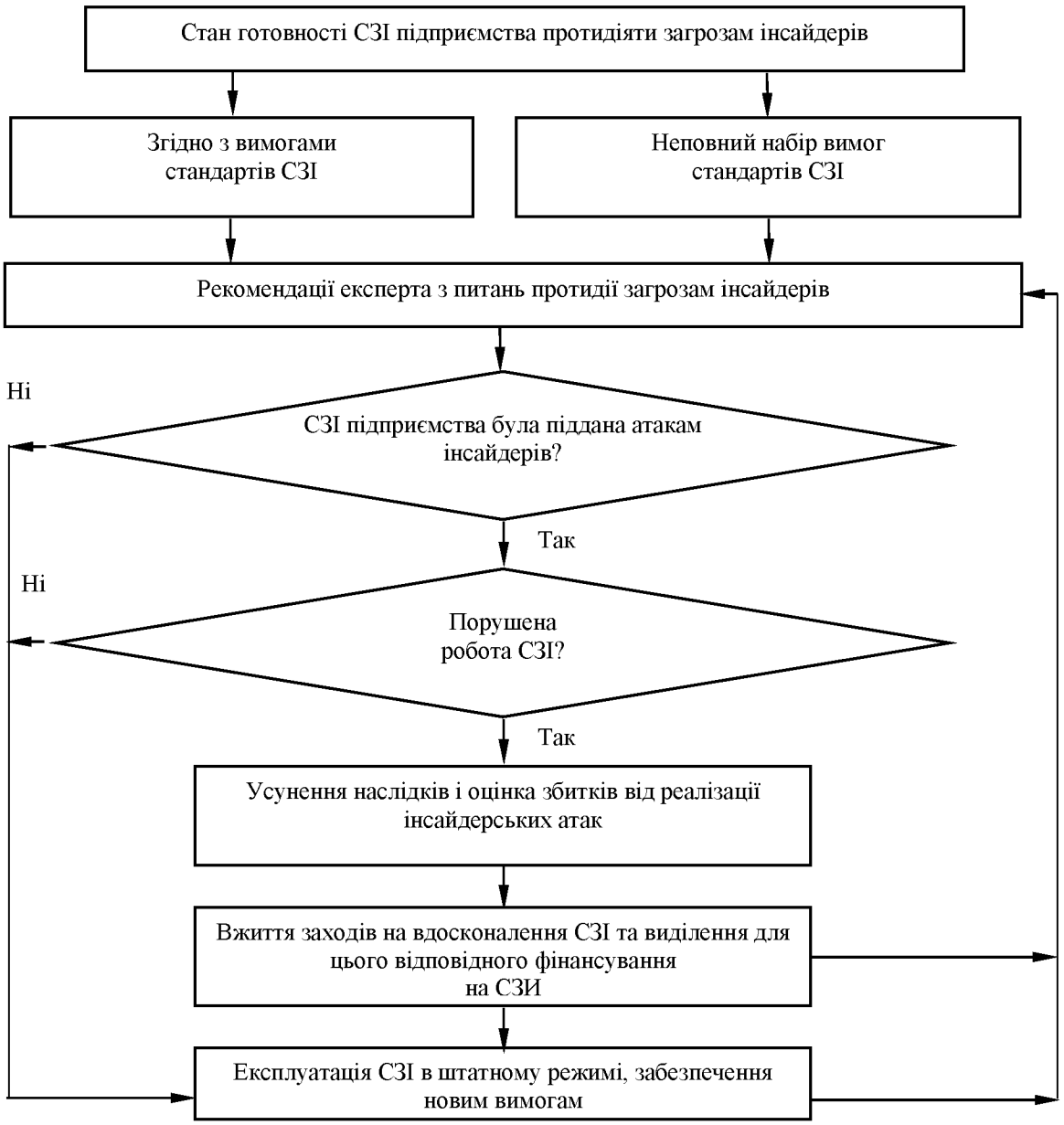

Рисунок 2 – Алгоритм оцінки роботи СЗІ для завдання аналізу та прийняття рішення по зменшенню ризиків інсайдерських загроз

Загальну величину внутрішнього ризику пропонується розраховувати за такою формулою:

$$R_{\text{заг}} = \sum_{i}^{N} p_i \times c_i \,, \tag{1}$$

де p_i - ймовірність *i*-го ризику; c_i - величина збитку від реалізації *i*-ї загрози.

Вочевидь, що величина *i*-го ризику

$$R_i = p_i \times c_i \qquad (2)$$

залежить від p_i та c_i. Тому, для оцінки загального ризику $R_{\text{заг}}$ потрібно виконати диференціацію величин збитків c_i та ймовірностей p_i для обох варіантів СЗІ, що можливо зробити на основі експертної оцінки із залученням спеціалістів відповідної кваліфікації та застосування імітаційного моделювання. Порівняльний аналіз значень загальних ризиків $R_{\text{заг}1}$ та $R_{\text{заг}2}$, витрат на СЗІ S_1 та S_2, суму втрат від реалізації загроз C_1 та C_2 відповідно для першого та другого варіантів дасть можливість визначити доцільність застосування певного набору заходів та методів з метою мінімізації ризиків від інсайдерських загроз.

Висновок. У статті розглянуто ризики інсайдерських загроз та надана класифікація дій працівників підприємства, що приводить до інсайдерства. Запропоновано алгоритм оцінки роботи СЗІ для завдання аналізу ризиків інсайдерских загроз та вжиття заходів для їх зниження. Пропонується оцінювати ефективність СЗІ шляхом порівняльного аналізу та оцінки показників витрат C_1 та C_2 на створення СЗІ, значень загальних ризиків $R_{\text{заг}1}$ та $R_{\text{заг}2}$, втрат від реалізації загроз C_1 та C_2.

ЛІТЕРАТУРА:

1. Конституція України. Закон України про захист інформації. Розділ V. Стаття 17.
2. Про захист персональних даних: Закон України від 07.07.2010р. // Офіційний вісник України. –№ 49. – 2010. – С. 199.
3. Про електронний цифровий підпис: Закон України від 04.07.2003 р. // Офіційний вісник України. – № 25. – 2003. – С. 111.
4. Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації: Закон України від 22.04.2011 р. № 3306-VI // Відомості Верховної Ради України. – 2011. – № 44. – С. 471.

REFERENCES:

1. The Constitution of Ukraine. Information Protection Law of Ukraine. Section V. Article 17.
2. On protection of personal data: Law of Ukraine of 07.07.2010. // Official Bulletin of Ukraine. № 49. 2010. P. 199.
3. On electronic digital signature: Law of Ukraine of 04.07.2003 // Official Bulletin of Ukraine. № 25. 2003. P. 111.
4. On Amendments to Some Legislative Acts of Ukraine on Insider Information: Law of Ukraine of April 22, 2011 No. 3306-VI // Bulletin of the Verkhovna Rada of Ukraine. 2011. № 44. P. 471.

DOI: 10.33243/2518-7139-2019-1-2-112-116