КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018
ISSN 2663 - 4023

УДК 316.776:004.58

Рой Яніна Володимирівна
кандидат технічних наук
доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
djanetta378@gmail.com
Мазур Наталія Петрівна
кандидат педагогічних наук, доцент доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0001-7671-8287
n.mazur@kubg.edu.ua
Складанний Павло Миколайович
старший викладач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ – ОСНОВА ЕФЕКТИВНОГО ЗАХИСТУ ПІДПРИЄМСТВА

Анотація. У статті розглядається поняття аудиту інформаційної безпеки в організації, наведено його види та основні етапи. У загальному випадку аудит безпеки, незалежно від форми його проведення, складається з чотирьох основних етапів, на кожному з яких виконується певне коло робіт. У статті окреслено основні етапи організації процесу проведення аудиту інформаційної безпеки в рамках аудиту бізнесу як сучасної концепції на аудит в цілому. Розкрито особливості кожного з позначених етапів, і дані рекомендації по їх здійсненню. Результатом запропонованого підходу до аудиту інформаційної безпеки є комплексна модель аудиторського циклу в рамках аудиту бізнесу, що дозволяє здійснювати дослідження зазначеної предметної області, що є основою підготовки інформації для прийняття оптимальних управлінських рішень. Зменшення ризику за рахунок додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення атаки або зменшити можливі збитки від неї. Викладена інформація дозволить оцінити поточну інформаційну безпеку свого підприємства і прийняти рішення про проведення аудиту.

Ключові слова: аудит, інформаційна система, інформаційна безпека.

1. ВСТУП

Сьогодні інформаційні системи (ІС) відіграють ключову роль в забезпеченні ефективності роботи комерційних і державних підприємств. Повсюдне використання ІС для зберігання, обробки і передачі інформації робить актуальними проблеми їх захисту, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що приводять до значних фінансових і матеріальних втрат. Для ефективного захисту від атак компаніям необхідна об’єктивна оцінка рівня безпеки ІС - саме для цих цілей і застосовується аудит безпеки.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

2.1. ЩО ТАКЕ АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Визначення аудиту безпеки ще не усталене, але в загальному випадку його можна описати як процес збору та аналізу інформації про ІВ для якісної або кількісної оцінки рівня її захищеності від атак зловмисників. Існує безліч випадків, коли доцільно проводити аудит безпеки. Це робиться, зокрема, при підготовці технічного завдання на проектування і розробку системи захисту інформації та після впровадження системи безпеки для оцінки рівня її ефективності.

Можливий аудит, спрямований на приведення діючої системи безпеки у відповідність вимогам українського або міжнародного законодавства. Аудит може також призначатися для систематизації та впорядкування існуючих заходів захисту інформації або для розслідування інциденту, що стався, пов'язаного з порушенням інформаційної безпеки [1].

Як правило, для проведення аудиту залучаються зовнішні компанії, які надають консалтингові послуги в області інформаційної безпеки. Ініціатором процедури аудиту може стати керівництво підприємства, служба автоматизації або служба інформаційної безпеки. У ряді випадків аудит також проводиться на вимогу страхових компаній або регулюючих органів. Аудит безпеки виконується групою експертів, чисельність і склад якої залежить від цілей і завдань обстеження, а також від складності об'єкта оцінки.

2.2.ВИДИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Можна виділити наступні основні види аудиту інформаційної безпеки:

- експертний аудит безпеки, в ході якого виявляються недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь в процедурі обстеження;
- оцінка відповідності рекомендаціям міжнародного стандарту ISO 17799, а також вимогам керівних документів;
- інструментальний аналіз захищеності ІС, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи;
- комплексний аудит, який включає в себе всі перераховані вище форми проведення обстеження.

Будь-який з перерахованих видів аудиту може проводитися окремо або в комплексі, в залежності від тих завдань, які вирішує підприємство. Як об'єкт аудиту може виступати як ІС компанії в цілому, так і її окремі сегменти, в яких обробляється інформація, що підлягає захисту [2].

2.3. ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У загальному випадку аудит безпеки, незалежно від форми його проведення, складається з чотирьох основних етапів, на кожному з яких виконується певне коло робіт.

На першому етапі спільно з замовником розробляється регламент, який встановлює склад і порядок проведення робіт. Основне завдання регламенту - визначити межі, в рамках яких буде проводитися обстеження. Регламент дозволяє уникнути взаємних претензій по завершенні аудиту, оскільки чітко визначає обов'язки сторін. Як правило, регламент містить наступну основну інформацію:

• склад робочих груп від виконавця і замовника для проведення аудиту;
• список і місце розташування об'єктів замовника, що підлягають аудиту;
• перелік інформації, яка буде надана виконавцю;
• перелік ресурсів, які розглядаються в якості об'єктів захисту (інформаційні, програмні, фізичні ресурси і т. д.);
• модель загроз інформаційній безпеці, на основі якої проводиться аудит;
• категорії користувачів, які розглядаються в якості потенційних порушників;
• порядок і час проведення інструментального обстеження ІС замовника.

На другому етапі, відповідно до узгодженого регламенту, збирається вихідна інформація. Методи збору інформації включають інтерв'ювання співробітників замовника, заповнення опитувальних листів, аналіз наданої організаційно-розпорядчої та технічної документації, використання спеціалізованих інструментальних засобів.

Третій етап робіт передбачає аналіз зібраної інформації з метою оцінки поточного рівня захищеності ІС підприємства. За результатами проведеного аналізу на четвертому етапі розробляються рекомендації з підвищення рівня захищеності ІС від загроз інформаційної безпеки.

Нижче докладніше розглянуто етапи аудиту, пов'язані зі збором інформації, її аналізом і розробкою рекомендацій щодо підвищення рівня захисту ІС.

Збір вихідних даних

Якість аудиту безпеки багато в чому залежить від повноти і точності інформації, отриманої в процесі збору вихідних даних. Тому в неї необхідно включити наступне: організаційно-розпорядчу документацію, яка стосується питань інформаційної безпеки, відомості про програмно-апаратне забезпечення ІС, інформацію про засоби захисту, встановлених в ІС і т.д. Більш детальний перелік вихідних даних представлений в табл. 1.

Таблиця 1

Перелік вихідних даних, необхідних для аудиту безпеки

Тип інформації	Склад вихідних даних
Організаційно-розпорядча документація з питань інформаційної безпеки	• політика інформаційної безпеки ІС; • керівні документи (накази, розпорядження, інструкції) з питань зберігання, порядку доступу і передачі інформації; • регламенти роботи користувачів з інформаційними ресурсами ІС
Інформація про апаратне забезпечення хостів	• перелік серверів, робочих станцій і комунікаційного устаткування, встановленого в ІС; • апаратні конфігурації серверів і робочих станцій; • відомості по периферійному обладнанні
Інформація про загальносистемне ПЗ	• відомості про ОС, встановлену на робочих станціях і серверах; • відомості про СУБД, встановлену в ІС
Інформація про прикладне ПЗ	• перелік прикладного ПЗ загального і спеціального призначення, встановленого в ІС; • опис функціональних завдань, що вирішуються за допомогою прикладного ПЗ
Інформація про засоби захисту, що встановлені в ІС	• виробник засобів захисту; • конфігураційні налаштування засобів захисту;

ISSN 2663 - 4023

	• схема встановлення засобів захисту
Інформація про топологію ІС	• карта локальної обчислювальної мережі, включаючи схему розподілу серверів і робочих станцій за сегментами мережі; • типи каналів зв'язку, що використовуються в ІС; • використовувані в ІС мережеві протоколи; • схема інформаційних потоків ІС

Як вже зазначалося вище, для збору вихідних даних застосовуються такі методи.

Інтерв'ювання співробітників замовника, що володіють необхідною інформацією. Інтерв'ю зазвичай проводяться як з технічними фахівцями, так і з представниками керівної ланки компанії. Перелік питань, які планується обговорити в процесі інтерв'ю, узгоджується заздалегідь.

Надання опитувальних листів з певної тематики, які співробітники замовника заповнюють самостійно. У тих випадках, коли представлені матеріали не повністю відповідають на необхідні питання, проводиться додаткове інтерв'ювання.

Аналіз організаційно-технічної документації, що використовується замовником.

Використання спеціалізованого ПЗ, яке дозволяє отримати необхідну інформацію про склад і настройках програмно-апаратного забезпечення ІС підприємства. Наприклад, за допомогою систем аналізу захищеності (security scanners) можна провести інвентаризацію мережевих ресурсів і виявити уразливості в них. Як приклади таких систем можна назвати Internet Scanner компанії ISS і XSpider компанії Positive Technologies.

Оцінка рівня безпеки ІС

Після збору необхідної інформації проводиться її аналіз з метою оцінки поточного рівня захищеності системи. У процесі такого аналізу визначаються ризики інформаційної безпеки, яким схильна компанія. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти інформаційним атакам [3].

Зазвичай виділяють дві основні групи методів розрахунку ризиків безпеки. Перша група дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності певним набором вимог до інформаційної безпеки. Як джерела таких вимог можуть виступати:

• нормативно-правові документи підприємства, що стосуються питань інформаційної безпеки (політика безпеки, регламенти, накази, розпорядження);

• вимоги чинного українського законодавства;

• рекомендації міжнародних стандартів – ISO 17799, OCTAVE, CoBIT, BS 7799-2 і т. д .;

• рекомендації компаній-виробників програмного і апаратного забезпечення - Microsoft, Oracle, Cisco і т. д.

Друга група методів оцінки ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. Значення ризику обчислюється окремо для кожної атаки і в загальному випадку є як добуток імовірності проведення атаки а на величину можливого збитку від цієї атаки - Ризик (а) = Р (а). Збиток (а). Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту. Імовірність в даному випадку розглядається як міра того, що в результаті проведення атаки порушники досягли своїх цілей і завдали шкоди компанії [4].

Методи обох груп можуть використовувати кількісні або якісні шкали для визначення величини ризику інформаційної безпеки. У першому випадку для ризику і

всіх його параметрів беруться чисельні вираження. Наприклад, при використанні кількісних шкал ймовірність проведення атаки P (a) може виражатися числом в інтервалі [0,1], а збиток від атаки - задаватися у вигляді грошового еквівалента матеріальних втрат, які може понести організація в разі успішної атаки. При використанні якісних шкал числові значення замінюються на еквівалентні їм понятійні рівні. Кожному понятійному рівню в цьому випадку буде відповідати певний інтервал кількісної шкали оцінки.

Кількість рівнів може варіюватися в залежності від застосовуваних методик оцінки ризиків. У табл. 2 і 3 наведені приклади якісних шкал оцінки ризиків інформаційної безпеки, в яких для оцінки рівнів збитків та ймовірності атаки використовується п’ять понятійних рівнів.

Таблиця 2

Якісна шкала оцінки рівня збитку

№	Рівень збитку	Опис
1	Малий	Незначні втрати матеріальних активів, які швидко відновлюються, або незначні наслідки для репутації компанії
2	Помірний	Помітні втрати матеріальних активів або помірні наслідки для репутації компанії
3	Середньої тяжкості	Істотні втрати матеріальних активів або значної шкоди репутації компанії
4	Великий	Великі втрати матеріальних активів і великих втрат репутації компанії
5	Критичний	Критичні втрати матеріальних активів або повна втрата репутації компанії на ринку, що робить неможливим її подальшу діяльність

Таблиця 3

Якісна шкала оцінки ймовірності проведення атаки

№	Імовірність атаки	Опис
1	Дуже низька	Атака практично ніколи не буде проведена. Відповідає числовому інтервалу ймовірності [0, 0,25)
2	Низька	Вірогідність проведення атаки досить низька. Відповідає числовому інтервалу ймовірності [0,25, 0,5)
3	Середня	Вірогідність проведення атаки приблизно дорівнює 0,5
4	Висока	Атака швидше за все буде проведена. Відповідає числовому інтервалу ймовірності (0,5, 0,75]
5	Дуже висока	Атака напевно буде проведена. Відповідає числовому інтервалу ймовірності (0,75, 1]

Для обчислення рівня ризику за якісними шкалами застосовуються спеціальні таблиці, в яких в першому стовпці задаються понятійні рівні збитку, а в першому рядку – рівні ймовірності атаки. Осередки же таблиці, розташовані на перетині відповідних рядків і стовпців, містять рівень ризику безпеки (табл. 4). Розмірність таблиці залежить від кількості концептуальних рівнів ймовірності атаки і шкоди.

ISSN 2663 - 4023

Таблиця 4

Визначення рівня ризику інформаційної безпеки по якісної шкалою

	Вірогідність атаки				
Збиток	Дуже низька	Низька	Середня	Висока	Дуже висока
Малий	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
Помірний	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
Середньої тяжкості	Низький ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
Великий	Середній ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
Критичний	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

При розрахунку значень ймовірності атаки, а також рівня можливого збитку використовують статистичні методи, експертні оцінки або елементи теорії прийняття рішень. Статистичні методи передбачають аналіз вже накопичених даних про реально траплялися інциденти, пов'язані з порушенням інформаційної безпеки. На основі результатів такого аналізу будуються припущення про ймовірність проведення атак і рівнях збитку від них в інших ІС. Однак статистичні методи не завжди вдається застосувати через нестачу статистичних даних про раніше проведених атаках на ресурси ІС, аналогічної тій, яка виступає в якості об'єкта оцінки [5].

При використанні апарату експертних оцінок аналізуються результати роботи групи експертів, компетентних в області інформаційної безпеки, які на основі наявного у них досвіду визначають кількісні або якісні рівні ризику. Елементи теорії прийняття рішень дозволяють застосовувати для обчислення значення ризику безпеки більш складні алгоритми обробки результатів роботи групи експертів.

Існують спеціалізовані програмні комплекси, що дозволяють автоматизувати процес аналізу вихідних даних і розрахунку значень ризиків при аудиті безпеки.

Результати аудиту безпеки

На останньому етапі аудиту інформаційної безпеки розробляються рекомендації щодо вдосконалення організаційно-технічного забезпечення захисту на підприємстві. Такі рекомендації можуть включати в себе різні типи дій, спрямованих на мінімізацію виявлених ризиків.

Зменшення ризику за рахунок додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення атаки або зменшити можливі збитки від неї. Так, установка міжмережевих екранів в точці підключення ІС до Інтернету істотно знижує ймовірність проведення успішної атаки на загальнодоступні інформаційні ресурси ІС – такі, як веб-сервери, поштові сервери і т. д.

Ухилення від ризику шляхом зміни архітектури або схеми інформаційних потоків ІС, що дозволяє виключити проведення тієї чи іншої атаки. Наприклад, фізичне відключення від Інтернету сегмента ІС, в якому обробляється конфіденційна інформація, дозволяє уникнути зовнішніх атак на конфіденційну інформацію.

Зміна характеру ризику в результаті вживання заходів по страхуванню. Як приклади зміни характеру ризику можна привести страхування обладнання ІС від пожежі або страхування інформаційних ресурсів від можливого порушення їх конфіденційності, цілісності або доступності. В даний час ряд українських компаній вже пропонують послуги страхування інформаційних ризиків.

Прийняття ризику, якщо він зменшений до того рівня, на якому вже не представляє небезпеки для ІС.

Зазвичай рекомендації спрямовані не на повне усунення всіх виявлених ризиків, а лише на їх зменшення до прийнятного рівня. При виборі заходів для підвищення рівня захисту ІС враховується одне принципове обмеження - вартість реалізації цих заходів не повинна перевищувати вартості захищаються інформаційних ресурсів, а також збитків компанії від можливого порушення конфіденційності, цілісності або доступності інформації [6].

На завершення процедури аудиту його результати оформляються у вигляді звітного документа, який надається замовнику. У загальному випадку цей документ складається з наступних основних розділів:

- опис меж, в рамках яких проводився аудит безпеки;
- опис структури ІС замовника;
- методи і засоби, які використовувалися в процесі проведення аудиту;
- опис виявлених вразливостей і недоліків, включаючи рівень їх ризику;
- рекомендації щодо вдосконалення комплексної системи забезпечення інформаційної безпеки;
- пропозиції до плану реалізації першочергових заходів, спрямованих на мінімізацію виявлених ризиків.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Аудит інформаційної безпеки - один з найбільш ефективних сьогодні інструментів для отримання незалежної і об’єктивної оцінки поточного рівня захищеності підприємства від загроз інформаційної безпеки. Крім того, результати аудиту дають основу для формування стратегії розвитку системи забезпечення інформаційної безпеки організації. Однак необхідно розуміти, що аудит безпеки - не разовий процедура, він повинен проводитися на регулярній основі. Тільки в цьому випадку аудит буде приносити реальну віддачу і сприяти підвищенню рівня інформаційної безпеки компанії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Д. И. Кравчук, «Аудит безопасности корпоративных информационных систем», *Молодой ученый,* №10, сс. 697–700, 2015.
[2] В. И. Аверченков, *Аудит информационной безопасности*, 2-е изд., Москва, ФЛИНТА, 269 с., 2011.
[3] В. К. Новиков, *Организационное и правовое обеспечение информационной безопасности. Часть 2: Организационное обеспечение информационной безопасности: учеб. пособие*, Москва, МИЭТ, 172 с., 2013.
[4] А. П. Курило, *Аудит информационной безопасности*, БДЦ-пресс, 304 с., 2006.
[5] С. С. Ерохин и С. В. Голубев, «Основные этапы оценки защищенности объектов информационных систем. Электронные средства и системы управления», *5-я молодежной научно–практической конференции*, Томск, В–Спектр, сс. 51–53, 2009.
[6] С. С. Ерохин и С. В. Голубев, «Международные стандарты в области аудита информационной безопасности: история создания, текущее состояние и проблемы», *Научная сессия ТУСУР-2007: Всероссийская научно–технической конференции студентов, аспирантов и молодых ученных*, Томск, Ч. 2, сс. 117–119, май 2007.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (1), 2018
ISSN 2663 - 4023

UDC 316.776:004.58

Yanina Vl. Roy
PhD, Associate Professor of the Department of Information and cyber security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0001-7671-8287
djanetta378@gmail.com
Nataliia P. Mazur
PhD, Associate Professor the Department of Information and cyber security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0001-7671-8287
n.mazur@kubg.edu.ua
Pavlo M.Skladannyi
Senior Lecturer of the Department of Information and cyber security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

AUDIT OF INFORMATION SECURITY IS THE BASIS OF EFFECTIVE PROTECTION OF THE ENTERPRISE

Abstract. The article considers the concept of audit of information security in the organization, its types and main stages are given. In general, security audit, regardless of the form of its conduct, consists of four main stages, each of which carries out a certain range of work. The article outlines the main steps in the organization of the process of conducting information security audit within the framework of business audit as a modern concept for audit in general. The features of each of the indicated stages are disclosed, and recommendations for their implementation are given. The result of the proposed approach to the audit of information security is a comprehensive audit cycle model within the framework of business auditing, which allows carrying out studies of the specified subject area, which serves as the basis for preparing information for making optimal management decisions. Reducing the risk through additional organizational and technical means of protection, which reduce the likelihood of an attack or reduce the possible damage from it. The above information will allow you to assess the current information security of your company and make a decision to conduct an audit.

Keywords: audit; information system; information security.

REFERENCES

[1] D. I. Kravchuk, "Audit bezopasnosti korporativnykh informatsionnykh sistem [Audit of the security of corporate information systems]," *Molodoi uchenyi*, no. 10, pp. 697–700, 2015.
[2] V. I. Averchenkov, *Audit informatsionnoi bezopasnosti* [*Information security audit*], 2nd izd., Moskva, FLINTA, 269 p., 2011.
[3] V. K. Novikov, *Organizatsionnoe i pravovoe obespechenie informatsionnoi bezopasnosti. Chast' 2: Organizatsionnoe obespechenie informatsionnoi bezopasnosti: ucheb. posobie* [*Organizational and legal support of information security. Part 2: Organizational Information Security: A Training Manual*], Moskva, MIET, 172 p., 2013.
[4] A. P. Kurilo, *Audit informatsionnoi bezopasnosti* [*Information security audit*], BDTs-press, 304 p., 2006.
[5] S. S. Erokhin and S. V. Golubev, "Osnovnye etapy otsenki zashchishchennosti ob"ektov informatsionnykh sistem. Elektronnye sredstva i sistemy upravleniya [The main stages of assessing the security of information system objects. Electronic means and control systems]," *V Molodezhnoi nauchno–prakticheskoi konferentsii*, Tomsk, V–Spektr, pp. 51–53, 2009.
[6] S. S. Erokhin and S. V. Golubev, "Mezhdunarodnye standarty v oblasti audita informatsionnoi bezopasnosti: istoriya sozdaniya, tekushchee sostoyanie i problemy [International standards in the field of information security audit: history of creation, current state and problems]," *Nauchnaya sessiya TUSUR-2007: Vserossiiskaya nauchno–tekhnicheskoi konferentsii studentov, aspirantov i molodykh uchennykh*, Tomsk, vol. 2, pp. 117–119, May 2007.