ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

МЕТОДИ ПЛАНУВАННЯ ТА ПРОВЕДЕННЯ ВНУТРІШНЬОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Студент: КУЧМІСТЕНКО Олексій Олегович

Керівник: доктор філософії з кібербезпеки ЗАПОРОЖЧЕНКО Михайло Михайлович

Актуальність

Постійне зростання інтенсивності та складності цілеспрямованих кібератак

Розмиття мережевого периметра та критичність вразливостей нульового дня

Неефективність формального підходу та потреба у виявленні реальних вразливостей

Внутрішній аудит як третя лінія захисту та основа циклу вдосконалення PDCA

Впровадження ризик-орієнтованого підходу та інструментальних засобів аналізу

Мета роботи

підвищення рівня захищеності інформаційних ресурсів організації
шляхом удосконалення ризик-орієнтованого процесу внутрішнього аудиту інформаційної безпеки та оцінювання ефективності корегувальних заходів.

Об’єкт дослідження

Процеси організації, планування та проведення внутрішнього аудиту системи управління інформаційною безпекою організації.

Предмет дослідження

Методи ризик-орієнтованого планування, технічні інструменти збору аудиторських доказів, а також математичні моделі прогнозного оцінювання залишкових кіберризиків.

Методи дослідження

Для вирішення означеного вище науково-практичного завдання в роботі використані методи аналізу та синтезу, класифікації, емпіричні методи та метод ситуаційного моделювання, а також матричні методи теорії ризиків і системного підходу для оцінювання зрілості процесів СУІБ (за шкалою SSE-CMM).

Завдання

1. Проаналізувати теоретико-нормативні засади внутрішнього аудиту інформаційної безпеки та обґрунтувати перехід до ризик-орієнтованого планування перевірок.

2. Систематизувати методи збору аудиторських доказів із визначенням інструментальних засобів аналізу захищеності інфраструктури та методологію оцінювання невідповідностей.

3. Провести ситуаційне моделювання процесу аудиту на базі демонстраційного кейсу IT-інфраструктури з формуванням відповідних чек-листів, робочих документів та журналу спостережень.

4. Розробити математичну модель оцінювання та мінімізації ризиків інформаційної безпеки для розрахунку ефективності запропонованих корегувальних дій та аналізу динаміки рівнів зрілості СУІБ.

Взаємозв’язок та функціональний розподіл стандартів у процесі аудиту ІБ

Стандарт	Роль у процесі аудиту	Ключовий фокус дослідження
ISO/IEC 27001	Джерело критеріїв (Що перевіряти?)	Встановлює обов'язкові вимоги до наявності процесу внутрішнього аудиту та містить еталонний перелік засобів захисту, з якими порівнюється об'єкт.
ISO/IEC 19011	Джерело процесу (Як перевіряти?)	Визначає загальну методологію, етапи організації перевірки, принципи незалежності аудиторів та правила збору доказів.
ISO/IEC 27007	Джерело специфіки (Як перевіряти саме ІБ?)	Конкретизує вимоги ISO 19011 під специфіку кібербезпеки, деталізує методи оцінки ризиків, аналізу логів та технічних конфігурацій СУІБ.

Методи та інструментальні засоби збору аудиторських доказів

Документальний аналіз

Вивчення політик ІБ, регламентів, інструкцій, Декларації про застосовність. Перевірка відповідності вимогам ISO/IEC 27001 та актуальності документів. Кінцева форма фіксації — чек-ліст відповідності документів вимогам стандарту.

Nmap — мережевий аналіз

Інвентаризація мережевих активів, виявлення активних вузлів, відкритих портів, ідентифікація мережевих служб і версій ОС. Дозволяє виявити несанкціоновано підключене обладнання або активні критичні протоколи. Кінцева форма фіксації — звіт сканування мережі.

Інтерв'ювання та спостереження

Опитування персоналу за чек-листами для оцінки обізнаності з питань кібербезпеки. Візуальний контроль процесів: політика «чистого столу», фізичний доступ до серверних. Кінцева форма фіксації — протокол інтерв'ю, зафіксовані відповіді.

Nessus / OpenVAS — аналіз вразливостей

Сканування вузлів інфраструктури на наявність відомих технічних дефектів. Категоризація загроз за шкалою CVSS, виявлення застарілих версій ПЗ та відсутніх патчів безпеки. Кінцева форма фіксації — офіційний звіт сканера із градацією за CVSS.

Класифікація невідповідностей та модель зрілості СУІБ

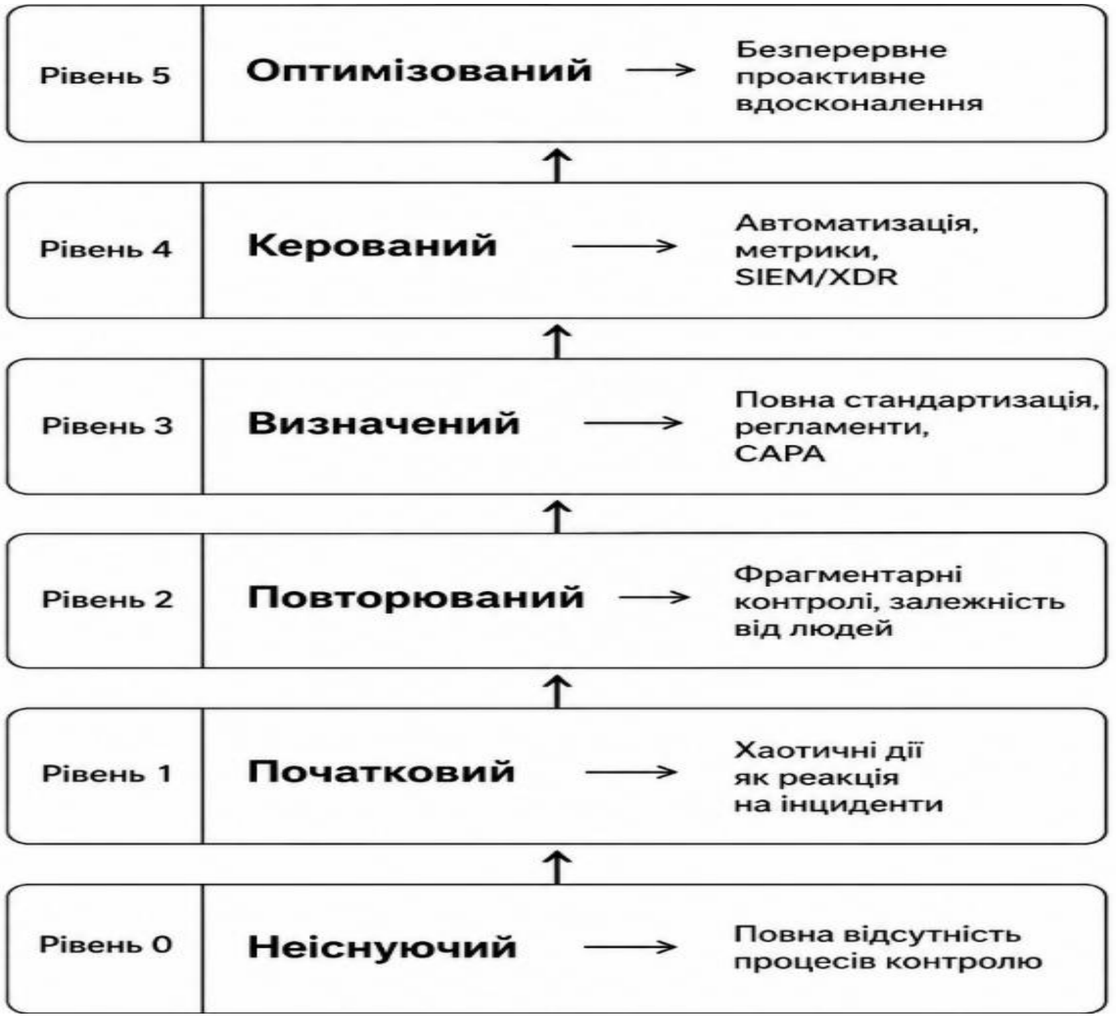
Рівні невідповідностей (ISO/IEC 19011)

Значна (Major)
Системне порушення, що безпосередньо впливає на конфіденційність, цілісність або доступність критичних даних.

Незначна (Minor)
Поодиноке відхилення без системного характеру, що не створює передумов для негайної компрометації активів.

OFI — Можливість для вдосконалення
Факт, що не є порушенням, але вказує на потенційне «вузьке місце», що може перерости в невідповідність.

Ієрархічна структура рівнів зрілості процесів СУІБ.



Демонстраційний кейс: Журнал аудиторських спостережень

Для верифікації розробленої методики сформовано демонстраційний кейс типової IT-інфраструктури: VPN-шлюз віддаленого доступу, сервер БД (192.168.1.10, Linux), платформа Jira, фізичний периметр та ЛОМ. Межі аудиту охоплюють механізми автентифікації, управління правами доступу, стан захищеності сервера СУБД та фізичну безпеку серверного обладнання.

№	Об'єкт	Виявлена невідповідність	Рівень
1	Сервер БД (192.168.1.10)	Вразливість RCE класу Log4Shell (CVE-2021-44228) у ПЗ логування	Критичний
2	Мережеве обладнання	Незахищений протокол Telnet (порт 23) для адміністрування	Високий
3	VPN-шлюз	Відсутність обов'язкової 2FA для віддалених підключень	Високий
4	Платформа Jira	5 активних облікових записів звільнених співробітників	Середній
5	Робочі станції	Слабкі паролі (на кшталт Password123) на 15% кінцевих точок ЛОМ	Середній
6	Серверне приміщення	Відсутність відеофіксації входу та журналу обліку відвідувачів	Низький

Комплекс корегувальних та запобіжних дій (CAPA)

Log4Shell (№1)

Усунення: Оновлення Apache Log4j до версії 2.17.1+.

Захист: Мікросегментація на фаєрволі, сигнатури IDS/IPS, щотижневе сканування Nessus.

Telnet (№2)

Усунення: Деактивація демона Telnet, закриття порту 23.

Захист: Перехід на SSHv2 з автентифікацією за ключами, регулярний контроль Nmap.

VPN без 2FA (№3)

Усунення: Тимчасове обмеження сесій віддаленого доступу.

Захист: Інтеграція VPN-шлюзу з MFA-сервером, евристичні політики блокування при аномальних входах.

Застарілі акаунти Jira (№4)

Усунення: Блокування 5 облікових записів колишніх співробітників.

Захист: Інтеграція Jira з Active Directory, автоматичне відкликання прав у день звільнення.

Слабкі паролі (№5)

Усунення: Примусове скидання паролів.

Захист: GPO: мін. 12 символів, різні регістри, цифри, спецсимволи; термін дії 90 діб; блокування після 5 невдалих спроб.

Фізичний захист (№6)

Усунення: Інвентаризація ключів, обмеження кола осіб із доступом.

Захист: IP-камера з детекцією руху, електромагнітний замок, інтеграція з СКУД на RFID-картках.

Прогнозна ефективність заходів

$$R_{total\_init} = R_{init1} + R_{init2} + R_{init3} = 25 + 16 + 16 = 57 \quad (3.9)$$

де R_{init} - вихідний стан після спостереження.

$$R_{total\_res} = R_{res1} + R_{res2} + R_{res3} = 5 + 4 + 4 = 13 \quad (3.10)$$

де R_{res} - прогнозий стан після спостереження.

$$\eta = \frac{R_{total\_init} + R_{total\_res}}{R_{total\_init}} \times 100\% \quad (3.8)$$

$$\eta = \frac{57-13}{57} \times 100\% \approx 77.2\ \% \quad (3.11)$$

де η - загального інтегральний показник ефективності мінімізації критичних ризиків

77.2%

Зниження критичних ризиків

Сумарний індекс ризику зменшився з 57 до 13 після реалізації плану CAPA для трьох найкритичніших невідповідностей

3.75

Рівень зрілості СУІБ

Підвищення за шкалою SSE-CMM / COBIT: з рівня 2.0 (Повторюваний) до 3.75 (Визначений з елементами кількісного керування)

6

Невідповідностей виявлено

1 критична, 2 високих, 2 середніх, 1 низька — для всіх розроблено адресні картки CAPA

Висновки

1. Обґрунтовано перехід від формального аудиту до ризик-орієнтованого підходу на основі стандартів ISO/IEC 27001, 19011 та 27007 для забезпечення безперервного вдосконалення СУІБ.
2. Поєднано організаційні методи перевірки з інструментальним скануванням, що гарантує об'єктивність та технічну незаперечність аудиторських доказів.
3. Проведено апробацію методики на демонстраційному кейсі IT-інфраструктури, що дозволило перевірити алгоритми аудиту без деструктивного впливу на реальні сервіси.
4. Сформовано журнал невідповідностей та розроблено адресний план корегувальних дій з чіткими інженерними рекомендаціями щодо їх усунення.
5. Доведено ефективність запропонованих рішень: розрахункове зниження критичних ризиків становить 77,2%, а прогнозний рівень зрілості процесів СУІБ зростає з показника 2.0 до 3.75 бала.

Застосування розробленої методології дозволяє трансформувати внутрішній аудит у проактивний інструмент менеджменту, забезпечуючи своєчасне виявлення векторів атак та оптимізацію витрат на кіберзахист підприємства.

Дякую за увагу!