КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4(20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.4561
УДК 657.6, УДК 004.056

**Якименко Юрій Михайлович**
кандидат військових наук, доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-6848-852X
*yakum14@ukr.net*

**Рабчун Дмитро Ігорович**
кандидат технічних наук, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

**Мужанова Тетяна Михайлівна**
кандидат державного управління, доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-7435-0287
*muzanovat@gmail.com*

**Запорожченко Михайло Михайлович**
асистент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

**Щавінський Юрій Віталійович**
кандидат технічних наук, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-2319-8983
*yushchavinsky@ukr.net*

# ТЕХНІЧНИЙ АУДИТ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО - ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ

**Анотація.** Розглянуто зміст аудиту і тестування вразливості інформаційно - телекомунікаційної системи (ІТС) будь-якого підприємства. На основі результатів аудиту інформаційної безпеки оцінюється в цілому захищеність ІТС підприємства. Оцінку захищеності ІТС пропонується проводить, використовуючи тестування на проникнення за наступними напрямками: тестування на проникнення ззовні і зсередини інформаційної інфраструктури, тестування соціальною інженерією персоналу підприємства і тестування на стійкість до DDoS атакам; оцінка захищеності мобільного додатку, веб-ресурсу і бездротових мереж. Запропонований загальний алгоритм проведення тестування на проникнення ІТ-інфраструктури (аналіз вразливостей та захищеності інформаційних ресурсів) у вигляді етапів: ініціалізації, пасивної і активної розвідки, експлуатації і пост-експлуатації, систематизація і презентація результатів оцінки безпеки, оцінки ризиків та вразливостей, рекомендацій щодо їх усунення. На етапах всі операції проводяться без нанесення реальної шкоди ІТС.

Показано призначення технічного аудиту, який охоплює складові ІТС і можна розглядати як незалежну експертизу або процедуру по їх досліджуванню, щоб оцінити стан та виявити резерви. Технічний аудит в результаті перевірки програмної та технічної частини ресурсу надає можливість сформувати перелік ключових проблем і отримати вичерпні рекомендації

щодо їх усунення. Зазначено, що відповідно до вимог сучасності технічний аудит може використовуватись як аудит у вигляді дистанційної технічної підтримки, а аудит інформаційної безпеки розглядатись як варіант технічного аудиту. Проведення аудиту інформаційної безпеки включає: аналіз ризиків, пов'язаних з можливістю здійснення інформаційних загроз безпеки щодо ресурсів; оцінку поточного рівня захищеності ІТС; локалізацію "вузьких місць" в системі захисту ІТС; оцінку відповідності ІТС існуючим стандартам в області безпеки; надання рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІТС. Розкрито зміст деталізованого звіту технічного аудиту захищеності ІТС підприємства.

**Ключові слова:** інформаційна безпека, інфраструктура, підприємство, інформаційно – телекомунікаційна система, тестування, вразливість

## ВСТУП

Забезпеченню захищеності інформаційно - телекомунікаційної системи (ІТС) будь-якого підприємства (маленької компанії або великої корпорації), в яких знаходиться і циркулює корпоративна інформація, наділяється значна увага в умовах зростання сучасних внутрішніх та зовнішних інформаційних загроз і масової цифровізації процесів в інформаційних активах.

Оцінку захищеності ІТС підприємства можна привести завдяки якісному проведенню аудиту інформаційної безпеки (ІБ). Аудит ІБ - це системний процес отримання об'єктивних якісних і кількісних оцінок поточного стану підприємства відповідно до визначених критеріїв його безпеки, що включає обстеження різних середовищ функціонування ІТС, тестування її на вразливості, аналіз і оцінку захищеності інформації, формування звіту та розробку відповідних рекомендацій по підвищенню ефективності захищеності самого підприємства. Аудит завжди сприймається як незалежна, комплексна або спрямована на окремі системи і процеси підприємства перевірка[20,21] .

На основі результатів аудиту оцінюється в цілому захищеність ІТС підприємства та готуються вихідні дані для формування нових вимог до комплексної системи захисту інформації (КСЗІ) в ІТС. Але високі інформаційні технології динамічно розвиваються, і разом із ними удосконалюються засоби скоєння злочинів у сфері ІБ. Саме КСЗІ дозволить нейтралізувати використання зловмисниками виявлених вразливостей і забезпечить оптимальний по ефективності захист інформації в ІТС підприємства.

Як правило більшість робочіх місць працівників підприємств оснащені персональними комп'ютерами та відповідним до них програмно-апаратним забезпеченням. Всі комп'ютери, як правило, автономно працюючі і пов'язані між собою або приєднані до інформаційно-обчислювальної мережі в складі ІТС. Поява нових загроз в сучасних умовах накладає обмеження на нормальне функціонування комп'ютерних систем. Тому досвід проведення аудиту на підприємстві залишається бути актуальним, особливо в пошуку новітних підходів в організаційних і технічних заходах його проведення. Як показує практика, проведення даних заходів дозволяє якісно підняти рівень захищеності ІТС.

**Постановка проблеми.**

Переважна більшість підприємств мають у своїх інформаційних системах вразливості з високими та критичними рівнями ризику. Наприклад, в ситуації, коли унаслідок некоректної конфігурації захищеного та оновленого сервісу, вдалося обійти авторизацію та користуватися сервісами підприємства за рахунок інших клієнтів, може стати причиною значних репутаційних і фінансових втрат. Для того, щоб успішно контролювати та покращувати рівень захищеності інфраструктури, перш за все, потрібно

спробувати подивитися на інфраструктуру підприємства очима порушника. Працівники підприємства мають знати, яким чином зловмисник буде намагатися вплинути безпосередньо на процеси в ІТС і що в таких випадках слід робити. Лише тоді, коли вдасться подивитися на інформаційні ресурси з позиції зловмисника, можна вибудувати захисну стратегію, яка буде стійкою перед можливими атаками. Тому значна увага повинна наділятися оцінці захищеності ІТС за допомогою симуляції дій реального порушника. Цього можна досягти, використовуючи тестування завдяки якому відтворюються алгоритми дій порушників. При тестуванні всі операції проводяться в рамках дозволеного договором, без нанесення реальної шкоди підприємству, проте всі інструменти, що використовуються, є справжніми, а результати оцінювання будуть відображати існуючі в системі вразливості, які можуть використовуватись зловмисником.

Тест на проникнення запобігає економічним та репутаційним втратам шляхом перевірки або побудови ефективного інформаційного захисту підприємства. У ході тестування виконується виявлення та перевірка вразливостей у системі, які могли виникнути через програмні та технічні помилки, неправильні налаштування, операційні недоліки тощо, які можуть бути використані реальним порушником. Також тестування дозволяє наочно продемонструвати значимість можливого потенційного збитку для підприємства. Керівнику потрібно завжди бути впевненим, що його підприємство готове до виникнення непередбачених ситуацій, а співробітники мають знання та навички щодо оперативного реагування на дії порушників.

Таким чином, на підприємстві треба визначати організаційні і технічні напрями діяльності, які спрямовані на закриття виявлених вразливостей і недопущення їх в майбутньому. Цього можна досягти тільки після виявлення вразливостей шляхом тестування на проникнення в рамках проходження аудиту захищеності ІТС.

**Аналіз останніх досліджень і публікацій.** Щоб гарантувати ефективний захист від інформаційних атак зловмисників, підприємствам необхідно мати об'єктивну оцінку поточного рівня його ІБ. Саме для цього і застосовується перевірка стану безпеки підприємства шляхом проведення аудиту. Багатьма авторами публікацій з питань контролю та аудиту в умовах застосування інформаційних технологій у сфері безпеки - С.А. Бурланом, , М.М Матюха, А.С. Немченко, В.М.Назаркіна, В.М. Чернуха, Я.В. Рой. [4,5,8] розглядається безліч випадків, коли доцільно проводити аудит безпеки. В даний час можна виділити такі основні види аудиту інформаційної безпеки: експертний аудит безпеки, в процесі якого виявляються недоліки в системі захисту інформації на основі наявного досвіду експертів, що беруть участь у процедурі обстеження; оцінка відповідності рекомендаціям міжнародних стандартів; інструментальний аналіз захищеності інформаційної системи, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи; комплексний аудит, що включає всі вище перелічені форми проведення обстеження. Кожен із перелічених вище видів аудиту може проводитися окремо чи комплексно залежно від тих завдань, які потрібно вирішити підприємству. Як об'єкт аудиту може виступати інформаційна система підприємства в цілому, так і її окремі сегменти, в яких проводиться обробка інформації, що підлягає захисту [3,6-9,12] У публікаціях зазначається, що якість аудиту безпеки багато в чому залежить від повноти і точності інформації, яка повинна бути отримана в процесі збору вихідних даних. Тому інформація повинна включати: існуючу організаційно-розпорядчу документацію, що стосується питань ІБ, відомості про програмно-апаратне забезпечення інформаційної системи; дані про засоби захисту інформації, які встановлені в системі і т.д. Рекомендується завжди готувати спочатку перелік вихідних даних, необхідних для проведення аудиту безпеки. У той же час

залишається переважно закритим питання тестування процесів в інформаційній системі. Однак роз'єднаність у поглядах щодо проведення аудиту та відсутність єдиних універсальних методичних інструментів щодо виконання тестування призводить до необхідності проведення додаткових досліджень та пошуку прийнятних варіантів на практиці.

У той же час деякі компанії, що працюють за аутсорсом, пропонують свої послуги підприємствам у проведенні аудиту безпеки [20,21]. Так, компанія **SI BIS**, яка входить до п'ятірки провідних системних інтеграторів України і неодноразово визнана кращим технологічним партнером світових лідерів в IT-галузі, розглядає і виконує як превентивні заходи для зниження ризиків, пов'язаних з ІБ, за рахунок виявлення та аналізу вразливостей в мережевій інфраструктурі при проведенні аудиту існуючих інформаційних систем і технологій (оцінка поточного стану і визначення відповідності або невідповідності системи заданим критеріям) [10,14]. Інша компанія IT Specialist, яка акредитована в Україні зі статусом QSA (Qualified Security Assessor), QPA (Qualified PIN Assessor), 3DS Security and ASV (Approve Scanning Vendor), надає послуги аудиту на відповідність вимогам стандарту PCI DSS, PIN Security, 3DS Security, SWIFT і отримання сертифіката відповідності [15].

**Мета статті.** Аналізування використання сучасних підходів щодо методики проведення технічного аудиту безпеки підприємства з метою оцінки стану захищеності і тестування на вразливості його інформаційно - телекомунікаційної системи.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У загальному випадку аудит інформаційних систем включає в себе комплексне обстеження різних середовищ їх функціонування, тестування на вразливості, аналіз та систематизацію отриманих результатів, оцінку рівня захищеності, формування звіту та розробку відповідних рекомендацій [1,2,4,5]. Ретельна та всебічна робота з дослідження інформаційно - телекомунікаційної системи (ІТС) будь-якого підприємства може проводиться завдяки тестуванню захищеності, як основного методичного інструменту для проникнення до її ресурсів , після чого відкриваються можливості до формування нових вимог до КСЗІ підприємства. Протягом тестування спеціалісти завжди використовують інструменти та інші методології, що дозволяють якомога точніше відтворити алгоритми дій справжніх порушників. Це означає, що всі операції проводяться без нанесення реальної шкоди ІТС, проте всі інструменти, що використовуються в процесі, є справжніми, а результати оцінювання будуть відображати існуючі в системі вразливості, які може використати порушник. Загальний принцип сценаріїв проникнення, що реалізуються реальними зломщиками – простота: чим простіше, примітивніше і, разом з тим, елегантніше сценарій проникнення, тим більш передбачуваним результатом такий сценарій буде реалізований. Багато сценаріїв проникнення (особливо на основі соціальної інженерії та фізики соціальних процесів), які використовуються реальними зломщиками, залишаються незмінними вже протягом багатьох років. Таким чином, тестування на проникнення – це дії, які націлені на спробу злому ресурсу, для виявлення слабків місць ІТС з метою подальшої реалізації її безпеки та захисту. Тому тестування захищеності ІТС можна запропонувати для виконання - за наступними напрямками (рис.1):

1. Тестування на проникнення ззовні (об'єкт – **зовнішній периметр інформаційної інфраструктури** підприємства);
2. Тестування на проникнення зсередини (об'єкт – **інформаційна інфраструктура** підприємства);

3. Оцінка захищеності мобільного додатку (об'єкт – **мобільний додаток**);
4. Оцінка захищеності веб-ресурсу (об'єкт – **WEB-додаток**);
5. Оцінка захищеності бездротових мереж (об'єкт – **Wi-Fi мережі** підприємства);
6. Тестування соціальною інженерією (об'єкт – **персонал** підприємства);
7. Тестування на стійкість до DDoS атакам [2,5,16-18].

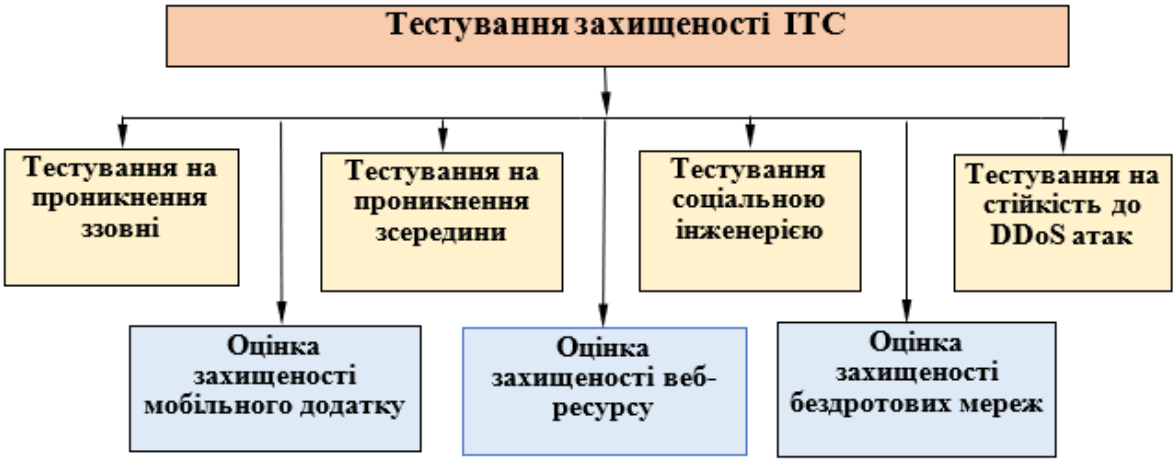


*Рис.1. Напрямки тестування захищеності ІТС*

В свою чергу, кожний з вище наведених видів тестування захищеності ІТС може надаватися за різними сценаріями:

- Білий ящик (White box testing). Виконавець має повну інформацію щодо інфраструктури, що підлягає тестуванню. Під час такого тестування часто виконується аналіз вихідного коду додатків або сканування операційних систем зсередини. Цей тип тестування надає більш повний результат, однак відходить від симуляції дій порушника, наближаючись до формату аудиту;
- Сірий ящик (Grey box testing). Виконавець має загальну, часткову або приблизну інформацію про інфраструктуру, що підлягає тестуванню. Дана опція є найбільш гнучкою та збалансованою, надаючи можливість симулювати дії більш підготовлених зловмисників;
- Чорний ящик (Black box testing). Виконавець має лише ту інформацію, що необхідна для ідентифікації області дії (наприклад, область дії - центральний офіс, все підприємство або перелік його IP-адрес). Дана опція дозволяє отримати найбільш реалістичні результати в контексті симуляції дій стороннього порушника.

**Тестування на проникнення ззовні та зсередини**

Інформаційна інфраструктура підприємства найчастіше складається зі значної кількості серверів, задачею яких є обробка інформації, що поступає з багатьох джерел. Така ситуація створює ризик порушення нормального режиму функціонування інфраструктури та компрометації даних. Слід згадати, що такі сумно відомі інциденти безпеки, як поширення вірусів NotPetya, WannaCry були б неможливими у разі проведення належних заходів перевірки інформаційних систем заздалегідь. Тестування на проникнення мережевих периметрів є способом визначити існуючі в IT-інфраструктурі проблеми безпеки.

Загальний алгоритм проведення тестування IT-інфраструктури (аналіз вразливостей та захищенності інформаційних ресурсів) можна представити у вигляді етапів (рис.2).

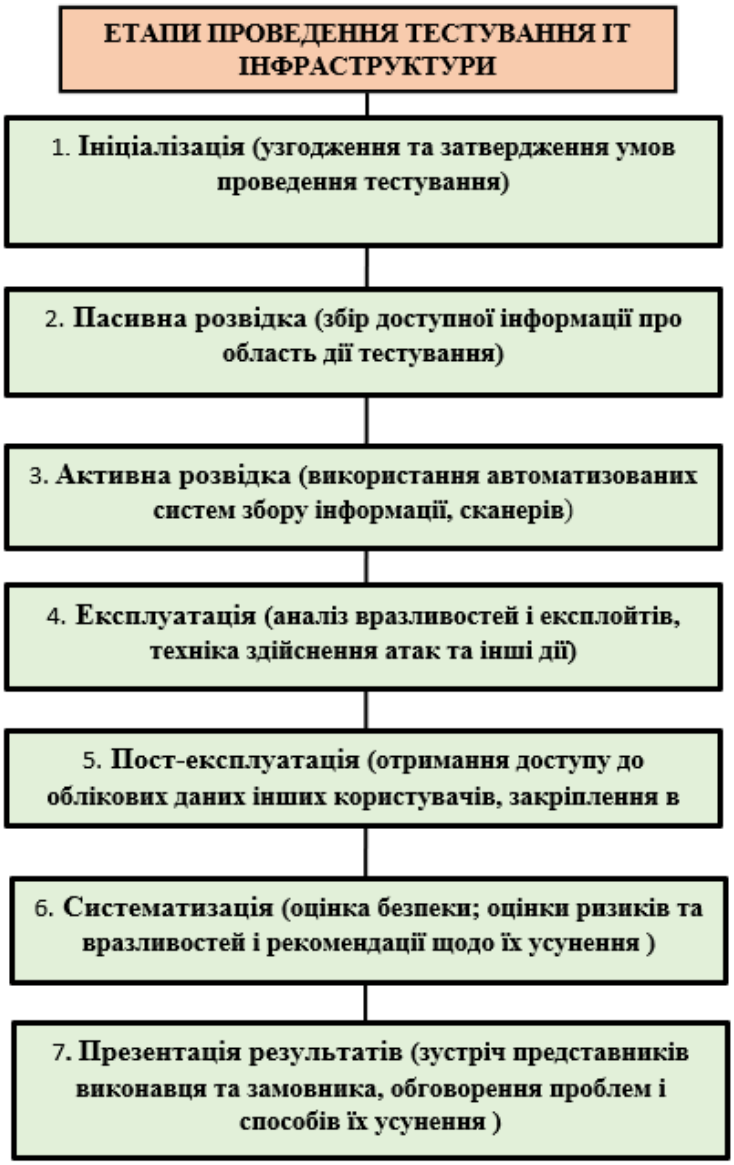


*Рис.2. Перелік етапів проведення тестування IT інфраструктури*

На етапі ініціалізації відбувається узгодження та затвердження умов проведення тестування: область дії, обмеження, тощо. Надаються необхідні дозволи, узгоджуються відповідальні представники з обох сторін, узгоджуються канали комунікації.

На етапі пасивної розвідки відбувається збір усієї доступної інформації про область дії тестування без використання інвазивних методів, тобто таких, що вимагають контакту з об’єктом тестування. Широко використовуються методи OSINT (Open Source Intelligence).

Етап активної розвідки включає в себе використання автоматизованих систем збору інформації, сканерів, інвазивних методів розвідки. Під час сканування діяльність виконавців може бути зафіксована IT- системами підприємства.

На основі інформації, отриманої на двох попередніх етапах, виконується аналіз та підготовка третього етапу – експлуатації. Під час виконання цього етапу використовуються інструменти експлуатації вразливостей (експлойти), техніки здійснення атак та інші дії, що імітують діяльність порушника.

У випадку отримання в результаті експлуатації достатнього рівня доступу виконується пост-експлуатація. Метою даного етапу є підвищення привілеїв, виявлення можливості розширення поверхні атаки, отримання доступу до облікових даних інших користувачів, закріплення в системі тощо.

У ході розробки звіту інформація про всі виявлені на попередніх етапах вразливості систематизується та оцінюється, після чого на її основі формується звіт, що містить безпосередню оцінку безпеки, оцінки ризиків та вразливостей, рекомендації щодо їх усунення.

Останнім етапом є презентація результатів, в ході якої передається звіт та проводиться фінальна зустріч представників виконавця та підприємства для обговорення всіх питань щодо процесу тестування, виявлених проблем та способів їх усунення.

**Тестування захищеності мобільного додатку**

Широке розповсюдження та спрощення механізмів створення мобільних додатків значно збільшує ризики виникнення в них вразливостей. Кожна така проблема може мати катастрофічні наслідки, оскільки один і той самий вразливий додаток використовується на всіх користувацьких пристроях. Відомі інциденти із виявленням критичних RCE-вразливостей в додатках WhatsApp та Outlook доводять, що навіть провідні розробники не можуть уникнути ризиків, пов’язаних із використанням мобільних додатків.

Тестування безпеки мобільних додатків являє собою детальний аудит функціональності та вихідного коду додатку, що включає в себе методи статичного та динамічного аналізу. У ході тестування визначаються та перевіряються вразливості в додатку, які могли виникнути через програмні помилки, операційні недоліки, тощо.

Проведення тестування включає в себе активну перевірку вразливостей мобільного додатку та його взаємодію з серверами замовника, яка виконується після узгодження часу проведення й обсягу таких дій із замовником.

Процедура тестування веб-додатків передбачає наступні частини:

- Reverse Engineering та аналіз байт-коду;
- проведення атак, пов'язаних із модифікацією коду;
- пошук застарілих бібліотек сторонніх організацій та ідентифікація SDK;
- експлуатація вразливостей автентифікації й авторизації;
- аналіз недоліків логіки роботи додатку;
- перевірка механізмів виявлення ROOT-прав;
- аналіз безпеки даних, що зберігаються на пристрої.

**Тестування захищеності ВЕБ-додатків**

Веб-додатки – невід’ємний атрибут функціонування сучасного бізнесу в кіберпросторі, а їх вразливості – одні з найпоширеніших у сфері ІБ. Інциденти Drupalgedon та безліч випадків «дефейсу» сайтів українських державних структур доводять, що проблеми безпеки веб-додатків – це не те, що можна ігнорувати.

Тестування веб-додатків на проникнення дозволяє виявити реальні можливості компрометації ВЕБ-ресурсів, які можуть призвести до отримання несанкціонованого

доступу до конфіденційних даних, відмов в обслуговуванні, репутаційних збитків чи навіть захоплення системи порушником.

Процес тестування веб-додатків складається з наступних кроків:

- аналіз призначення веб-додатку;
- пошук вразливостей із використанням автоматичних сканерів вразливостей;
- аналіз загроз для виявлення можливих атак (наприклад, неавторизована маніпуляція зовнішніми даними);
- ручний пошук вразливостей;
- перевірка виявлених вразливостей (наприклад, SQL injection, XML injection, XSS тощо);
- перевірка систем розмежування та контролю доступу;
- пошук помилок логіки роботи додатку.

**Тестування захищеності бездротових мереж**

Використання бездротових мереж в корпоративному сегменті – це в однаковій мірі зручно та небезпечно, адже сама специфіка концепції безпровідного зв'язку передбачає відсутність передачі сигналу точно до адресату – перехоплення такого сигналу можливе будь-ким і лише належні налаштування обладнання можуть гарантувати цілісність та конфіденційність даних.

Тестування на проникнення бездротових мереж проводиться з метою виявлення вразливостей у поточній архітектурі бездротового сегмента інформаційної системи й окремих компонентах цієї архітектури. Воно дозволяє виявити вразливості, доступні для використання в бездротових мережах, системах, хостах і мережевих пристроях, перш ніж зловмисники зможуть їх виявити та використовувати.

Процес тестування захищеності бездротових мереж включає:

- розвідку бездротових мереж замовника;
- детальне вивчення характеристик і особливостей виявлених мереж;
- проведення атак на аутентифікацію й авторизацію в мережах;
- проведення атак на апаратне забезпечення мереж;
- проведення атак на клієнтів мереж.

Проведення тестування захищеності бездротової мережі дозволяє:

- зрозуміти рівень ризиків, який створюють бездротові мережі для організації та шляхи їх зменшення;
- забезпечити більшу гнучкість для користувачів при збереженні конфіденційності та цілісності даних;
- впевнитись, що конфігурації бездротових мереж відповідають сучасним вимогам до захисту даних, таких як PCI DSS.

**Тестування соціальною інженерією**

Персонал – найменш захищена ланка в будь-якій інформаційній системі, а людський фактор – причина виникнення більшості проблем безпеки. Таким чином, атаки, що спрямовані на персонал компанії мають надзвичайно високий ризик реалізації та можливий вплив. Практика показує, що, зокрема, переважна більшість епідемій шифрувальників розповсюджується через соціальних канал (наприклад електронною поштою), а відомі APT-групи окрім авторських інструментів та експлойтів зазвичай використовують методи шахрайства.

Тестування на проникнення по соціальному каналу призначене для імітації нападів, які шахраї використовують, щоб нашкодити компанії за допомогою психологічного впливу на персонал із використанням мережевого або телефонного засобів зв'язку та без нього, у безпосередньому контакті.

Тестування каналами соціальної інженерії включає наступні напрямки:

- перевірка підготовленості персоналу при шахрайських атаках по телефону;
- перевірка підготовленості персоналу при шахрайських атаках по електронній пошті;
- перевірка підготовленості персоналу у випадках спам-атак.

Проведення тестування на проникнення по соціальному каналу передбачає повний звіт, що включає в себе висновки та рекомендації зі зменшення ризиків для керівництва та команди з питань безпеки. За результатами тестування компанія отримує рекомендації з навчання персоналу для виправлення існуючих проблем та підготовки до майбутніх нападів.

**Тестування на стійкість до DDoS атак**

DoS – «відмова в обслуговувані» – це тип атак на інформаційну інфраструктуру з метою виведення її з нормального режиму функціонування та переривання доступності. DDoS-атака — це DoS атака, що виконується з багатьох мережевих вузлів одночасно. DDoS (Distributed Denial of Service) атаки виконуються зловмисниками з використанням значної кількості атакуючих машин для створення надмірного об'єму трафіку, що перевантажує обчислювальні можливості цільової системи.

**Тестування зовнішнього периметра мережі на стійкість до DDoS атак** має особливості – проводиться з використанням інших сценаріїв, наприклад: TCP-SYN flood, ICMP Storm, Ping flood, TCP malformed flood.

1. TCP-SYN flood

SYN flood це форма атаки «відмова в обслуговуванні» в якій зловмисник надсилає послідовно TCP SYN-запити до системи цілі, намагаючись вичерпати достатньо ресурсів сервера, виділених на підтримку з`єднань, щоб система не відповідала звичайному трафіку.

2. ICMP Storm

ICMP Storm це надсилання надмірної кількості різних ICMP-повідомлень (типів та кодів), спрямованих на те, щоб зробити систему недоступною через перевантаження стека TCP-IP на системному рівні або через спричинення інших негативних ефектів доступності на мережевому рівні.

3. Ping flood - це проста атака виду «відмови в обслуговуванні». Коли зловмисник надсилає жертві занадто багато пакетів ICMP "ехо-запит" (пінг). Пакети надсилаються з максимально можливою швидкістю і створюють необхідність для цільового серверу надавати на них відповіді.

4. TCP malformed flood

TCP malformed flood використовується для відправлення десятків неконвенційних пакетів TCP до цілі з метою збільшення часу на обробку таких пакетів, перевантаження файерволів, тощо. Використовуються будь-які типи нестандартних пакетів TCP - SYN-FIN, SYN-RST, SYN з даними, bad TCP checksum та будь-які інші.

**Які види оцінки захищеності можуть бути здійснені при тестуванні ІТС підприємства?** Оцінка захищеності мобільного додатку, веб-ресурсу, бездротових мереж здійснюється з метою перевірки здатності ІТС підприємства. протидіяти атакам, спрямованим на порушення доступності до інформації. В рамках тестування, розгортається у різних частинах світу мережа з віртуальних серверів (Botnet). За допомогою технологій C&C здійснюється синхронізоване керування даною мережею та запуск симуляції атаки на цільову інформаційну систему. Таким чином досягається максимальне наближення дій з симуляції зловмисної активності до реальної кібератаки, однак завдяки максимальній контрольованості ботнету та проведенню всіх операцій виключно в узгоджені часові проміжки в умовах комунікації з командою захисту, реальної шкоди інформаційній системі не задається.

Результати аналізу захищеності ІТС допомагає оцінити її рівень, створити звіт та розробити відповідні рекомендації, що дозволяє протистояти зовнішнім і внутрішнім загрозам безпеки, які постійно змінюються та адаптуються.

В останні часи значна увага стала наділятися проведенню **технічного аудиту**, який охоплює в тому числі і складові ІТС [5,7,10]. При технічному аудиту здійснюється більш детально перевірка структури та діяльності підприємства, відповідності впроваджених заходів нормативним вимогам, достатності технічних та програмних засобів для збереження інформації, практичних навичок співробітників та відповідального за інформаційну безпеку, якості технічної документації та алгоритмів контролю і оцінки процесів забезпечення захисту інформації.

**Технічний аудит можна розглядати також як незалежну експертизу**, процедуру, яка дозволяє досліджувати ІТ- системи, щоб оцінити їх стан та виявити резерви для покращення ефективності діяльності. Технічний аудит в результаті перевірки програмної та технічної частини ресурсу надає можливість сформувати перелік ключових проблем і отримати вичерпні рекомендації щодо їх усунення.

Так, аудит апаратно-програмного комплексу включає:

• аудит існуючих ІТС (оцінка поточного стану, процесів, визначення відповідності або невідповідності системи заданим критеріям);

• аналіз налаштувань комплексу за наданими пілпрємством даними;

• проведення аналізу готовності апаратно-програмного комплексу;

• рекомендації щодо покращення технічних характеристик різних компонентів існуючої ІТС та вироблення плану з оптимізації існуючого апаратно-програмного комплексу;

• виконання повної або часткової переконфігурації обладнання та комплексу в цілому (при необхідності);

• консультації спеціалістів підприємства в ході виконання робіт, а також по телефону / електронній пошті [7].

Відповідно до вимог сучасності технічний аудит може використовуватись як аудит у вигляді Дистанційної технічної підтримки.

**Дистанційна технічна підтримка** має на увазі підключення фахівця-аудитора до комп'ютера (комп'ютерної системи) за допомогою мережі Інтернет, що є важливим для бізнесу, тому що відсутні його простої.

Дистанційна технічна підтримка включає в себе повний супровід ІТС та всіх компонентів інфраструктури, а саме:

• підтримку систем зберігання даних (СЗД): налаштування та віддалене обслуговування СЗД, супровід систем резервного копіювання, супровід географічно рознесених кластерів;

• підтримку серверного обладнання: конфігурація налаштувань серверів, моніторинг і регулярне системне адміністрування;

• підтримку середовища віртуалізації: MS Hyper-V, VMware, Citrix, віртуалізація робочих Стіл VMware, Citrix, Microsoft;

• підтримку мереж передачі даних: локальних (LAN), бездротових (Wi-Fi), розподілених (WAN); IP-телефонії; систем колективної роботи (Collaboration); контакт-центрів; систем відеоконференцзв'язку (ВКЗ);

• управління загальними файловими ресурсами: розподіл прав доступу до файлового сервера і окремих папок, моніторинг використання дискового простору і його квотування;

• обслуговування і адміністрування робочих станцій;

• підтримку і супровід поштових систем MS Exchange, IBM Lotus Domino і ін.;

• адміністрування, моніторинг СУБД, резервне копіювання даних, настройка сценаріїв реплікації і продуктивності, виконання розподілених запитів і транзакцій і т.д. [11].

Частіше сам аудит ІБ розглядається теж як варіант технічного аудиту і є важливим з точки зору його стратегічного розвитку, який включає:

- аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки, особливо щодо інформаційних ресурсів;
- оцінку поточного рівня захищеності ІТС;
- локалізацію "вузьких місць" в системі захисту ІТС;
- оцінку відповідності ІТС існуючим стандартам в області ІБ;
- надання рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІТС [7,9].

Як показує практика від компаній Legal IT Group і ProNET, в межах технічного аудиту може здійснюватися перевірка:

- Обладнання.
- Шифрування.
- Умов зберігання та обробки інформації.
- Програмнних засобів захисту.
- Політики інформаційної безпеки.
- Ступені досвідченості та обізнаності команди в галузі ІБ.
- Алгоритми протидії зовнішнім та внутрішнім загрозам.
- Політики у сфері аутсорс ресурсів.
- Періодів та мету зберігання.
- Засобів виявлення нестачі або непередбаченої зміни конфіденційної інформації.
- Резервування даних [2].

Кінцевим результатом виконання технічного аудиту захищеності ІТС підприємства є деталізований звіт**,** який включає серед інших наступні елементи (рис.3):

- перелік виявлених вразливостей об'єкту з експертною оцінкою ризику від експлуатації;
- опис дій і процесів, необхідних для підтвердження наявності вразливості в системі, аудиторські докази – в першу чергу графічні ілюстрації наявності вразливостей;
- експертні оцінка та рекомендації щодо усунення проблем безпеки, технічні деталі та необхідні для цього кроки.

Загальні висновки щодо комплексної оцінки захищеності ІТС дозволять керівництву підприємства отримати розуміння стану безпеки протестованих об'єктів.


*Рис.3 Основні елементи деталізованого звіту з технічного аудиту захищеності ІТС*

Що являє собою результат оцінки безпеки інформаційної інфраструктури?

За результатами проведення оцінки безпеки інформаційної інфраструктури підприємству надається інший звіт, як комплексний звіт. Даний документ містить також перелік усіх знайдених під час тестування вразливостей, їх детальні описи, оцінки ризиків, описи дій, за допомогою яких було виявлено наявність дійсної вразливості, рекомендації щодо усунення цих вразливостей, а також перелік виявлених сервісів та узагальнені рекомендації щодо покращення рівня ІБ в рамках нетехнічної частини звіту.

Зміст звіту:

- резюме для керівництва. Стисле викладення результатів тестування;
- мета тестування. Опис цілей проведення тестування;
- область дії. Визначення області дії тестування;
- опис методики. Загальний опис проведених тестів, перелік перевірених ділянок, методики та інструментів, що були використані в ході тестування та його окремих етапів;
- результати тестування. Результати тестування та рекомендації виконавця у форматі «карток вразливостей» - виявлені недоліки або вразливі ділянки з докладним описом методу, за допомогою якого їх було виявлено, та варіанти усунення даних слабких місць.

Відомі методології**,** що використовуються під час оцінки безпеки інформаційної інфраструктури та найкращі практики щодо проведення технічного аудиту захищеності ІТС:

**ISECOM OSSTMM3** (Open Source Security Testing Methodology Manual) - високорівнева методологія тестування систем безпеки, яка розроблена та підтримується консорціумом «Institute for Security and Open Methodologies». Використовується як основа для планування і координації робіт, а також для складання звітів про результати проєкту [16].

**PTES** (Penetration Testing Execution Standard) - методологія, яка розробляється групою фахівців із тестування на проникнення, аудиту безпеки та соціальної інженерії. Методологія доповнює OSSTMM у ході планування та координації проекту, а також використовується на етапі неавтоматизованого пошуку й аналізу вразливостей IT-систем в області дії тесту [17].

**NIST SP800-115** (Technical Guide to Information Security Testing and Assessment) - методологія інструментального тестування безпеки IT-систем, обов'язкова до застосування у федеральних агентствах США. Ця методологія використовується на етапі автоматизованого пошуку й аналізу вразливостей IT-систем в області дії тестування, а також у ході можливої імітації атак із використанням виявлених вразливостей [18].

**OWASP** (OWASP Testing Guide) – індустріальний стандарт тестування на проникнення веб-додатків і пов'язаних із ними технологій. Методологія використовується при тестуванні веб-додатків [13,10].

**OWASP MSTG** (Mobile Security Testing) – індустріальний стандарт тестування на проникнення мобільних додатків та пов’язаних із ними технологій. Методологія використовується при тестуванні мобільних додатків.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження дозволяє зробити висновки:

1. Для гарантування ефективного захисту від інформаційних атак зловмисників, підприємствам необхідно мати об'єктивну оцінку поточного рівня його інформаційної безпеки. Перевірка стану безпеки підприємства досягається шляхом проведення аудиту.

2. У загальному випадку аудит інформаційних систем включає в себе комплексне обстеження різних середовищ їх функціонування, тестування на вразливості, аналіз та систематизацію отриманих результатів, оцінку рівня захищеності, формування звіту та розробку відповідних рекомендацій

3. Тестування захищеності інформаційно - телекомунікаційної системи розглядається як основний методичний інструмент для проникнення до її ресурсів, після чого відкриваються можливості до формування нових вимог до комплексної системи захисту інформації підприємства. Тестування захищеності можна запропонувати за наступними напрямками: проникнення ззовні і зсередини, перевіркою соціальною інженерією і на стійкість до DDoS атакам; оцінка захищеності мобільного додатку, веб-ресурсу і бездротових мереж.

4. В останні часи значна увага стала наділятися проведенню технічного аудиту, який охоплює в тому числі і складові інформаційно - телекомунікаційної системи. При технічному аудиту здійснюється перевірка структури та діяльності підприємства, відповідності впроваджених заходів нормативним вимогам, достатності технічних та програмних засобів для збереження інформації, практичних навичок співробітників та відповідального за інформаційну безпеку, якості технічної документації та алгоритмів контролю і оцінки процесів забезпечення захисту інформації.

5. Частіше сам аудит інформаційної безпеки підприємства розглядається теж як варіант технічного аудиту і є важливим з точки зору його стратегічного розвитку, який включає: аналіз ризиків щодо інформаційних ресурсів, оцінку поточного рівня захищеності інформаційної системи і локалізацію “вузьких місць” в її системі захисту, оцінку відповідності інформаційної системи існуючим стандартам в області інформаційної безпеки і надання рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки.

6. Пропонується перелік методологій**,** що використовуються під час оцінки безпеки інформаційної інфраструктури та найкращі практики щодо проведення технічного аудиту захищеності інформаційно - телекомунікаційної системи.

У перспективі подальших досліджень передбачається проаналізувати методичні підходи і досвід використання технічного аудиту в дослідженні систем управління інформаційною безпекою на підприємстві

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Немченко, А., Назаркіна, В., Губський, С., Чернуха, В., Корж, Ю. Сапсай Р (2012). *Аудит. Навчальний посібник для студентів вищих навчальних закладів.* http://dspace.nuph.edu.ua/handle/123456789/8693.

2 *Аудит інформаційної безпеки*. ProNET. https://www.pronet.ua/audit-informaczijnoi-bezpeki/.

3 Корченко, О. Гнатюк, С., Казмірчук, С., Панченко, В. Мельник С. (2014). *Аудит та управління інцидентами інформаційної безпеки*. Центр навчально-наукових та науково-практичних видань Національної академії СБ України.

4 Roy, Y. V., Mazur, N. P., Skladannyi, P. M. (2018). Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1*(1), 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693.

5 Бурлан, С., Руденко, Н. (2017). *Організація і методика аудиту*. Миколаїв: Вид-во ЧНУ ім. Петра Могили.

6 7 вагомих причин проведення технологічного аудиту підприємства https://aimarketing.info/uk/blog/technichal-audit/7-vagomyh-prychyn-provedennya-tehnologichnogo-audytu-pidpryemstva

*7* Зачек О., Сеник В. Магеровська, Т.(2022). *Інформаційні технології. Навчальний посібник. Львів: Львівський державний університет внутрішніх справ. http://dspace.lvduvs.edu.ua/handle/1234567890/4778*.

8 Матюха, М. (2018). *Комп'ютерний аудит*. ДП «Видавничий дім «Персонал». https://maup.com.ua/assets/files/lib/book/komputer_audit.pdf.
9 Системи забезпечення інформаційної безпеки. Огляд. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review .
10 *Технічний аудит обладнання - SI BIS.* SI BIS. https://www.sibis.com.ua/services/technical-support-and-maintanance/technical-audit-of-equipment/
11 *Дистанційна технічна підтримка - SI BIS.* SI BIS. https://www.sibis.com.ua/services/outsourcing/distantsijna-tehnichna-pidtrimka/
12 Якименко, Ю., Савченко, В., Легомінова, С. (2022). *Системний аналіз інформаційної безпеки: сучасні методи управління.* Державний університет телекомунікацій. https://www.dut.edu.ua/uploads/l_2230_88161692.pdf .
13 Drahuntsov, R., Rabchun, D., Brzhevska, Z. (2020). Architecture security principles of the android applications-based information system. *Cybersecurity: Education, Science, Technique*, 49–60. https://doi.org/10.28925/2663-4023.2020.8.4960.
14 Drahuntsov, R., Rabchun, D. (2021). Potential disguising attack vectors on security operation centers and siem systems. *Cybersecurity: Education, Science, Technique*, 2(14), 6–14. https://doi.org/10.28925/2663-4023.2021.14.614.
15 *Pentest* | IT Specialist. https://my-itspecialist.com/products/pentest.
16 *RESEARCH.* (b. d.). ISECOM. https://www.isecom.org/research.html
17 *The Penetration Testing Execution Standard.* The Penetration Testing Execution Standard. http://www.pentest-standard.org/index.php/Main_Page.
18 *SP 800-115, Technical Guide to Information Security Testing and Assessment* | CSRC. (b. d.). NIST Computer Security Resource Center | CSRC. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.
19 *OWASP Foundation, the Open Source Foundation for Application Security* | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://www.owasp.org.
20 Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості». (2019). *Інформаційні технології. Методи захисту* (ДСТУ ISO/IEC 27007:2018). http://online.budstandart.com/ua/catalog/doc-page?id_doc=80303.
21 ISO/TMBG Technical Management Board - groups. (2018). *Керівні вказівки щодо аудиту систем менеджменту* (ISO 19011:2018). https://cdn.standards.iteh.ai/samples/70017/559078f9a2634aca84ff0a6aac1498f6/ISO-19011-2018.pdf.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

**Yakymenko Yuriy Mykhailovych**
Cand. of military sciences (Ph.D), Associate Professor, Associate Professor
of Information Security and Cyber Security Department,
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-6848-852X
*yakum14@ukr.net*

**Dmytro I. Rabchun**
Cand. of Technical Sciences (Ph.D), Associate Professor
of Information Security and Cyber Security Department,
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

**Muzhanova Tetyana Mykhailivna**
Cand. of public administration (Ph.D), Associate Professor, Associate Professor
of Information Security and Cyber Security Department,
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

**Mykhailo M. Zaporozhchenko**
Assistant of Information Security
and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0003-0182-9497
*zaporozhchenkomm@gmail.com*

**Yurii V. Shchavinskyi**
Cand. of Technical Sciences (Ph.D), Associate Professor
of Information Security and Cyber Security Department,
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-2319-8983
*yushchavinsky@ukr.net*

# TECHNICAL AUDIT OF SECURITY OF INFORMATION - TELECOMMUNICATION SYSTEMS OF ENTERPRISES

**Abstract.** The content of the audit and vulnerability testing of the information and telecommunication system (ITS) of any enterprise is considered. Based on the results of the information security audit, the overall security of the company's ITS is assessed. It is proposed to assess the security of IT using penetration testing in the following areas: penetration testing from outside and inside the information infrastructure, social engineering testing of the company's personnel and testing for resistance to DDoS attacks; assessment of the security of the mobile application, web resource and wireless networks. The proposed general algorithm for IT infrastructure penetration testing (analysis of vulnerabilities and security of information resources) in the form of stages: initialization, passive and active intelligence, operation and post-exploitation, systematization and presentation of the results of security assessment, risk and vulnerability assessment, recommendations regarding them elimination. In stages
all operations are carried out without causing real damage to the ITS.
The purpose of a technical audit is shown, which covers the components of the ITS and can be considered as an independent examination or a procedure for their investigation in order to assess the condition and identify reserves. Technical audit as a result of checking the software and technical part of the resource provides an opportunity to form a list of key problems and get comprehensive recommendations for their elimination. It is noted that in accordance with modern requirements, technical audit can be used as an audit in the form of remote technical support, and information security audit can be considered as a variant of technical audit. Conducting an information security audit includes: analysis of risks associated with the possibility of information security threats to

resources; assessment of the current level of ITS security; localization of "bottlenecks" in the ITS protection system; assessment of ITS compliance with existing standards in the field of security; providing recommendations on the implementation of new and improving the effectiveness of existing ITS security mechanisms. The content of the detailed report of the technical audit of the enterprise's ITS security has been revealed.

**Keywords:** information security, infrastructure, enterprise, information and telecommunication system, testing, vulnerability

## REFERENCES

1 Nemchenko, A., Nazarkina, V., Gubsky, S., Chernukha, V., Korzh, Yu. Sapsai, R. (2012). *Audit Study guide for students of higher educational institutions.* 10.13140/RG.2.1.1857.4561.
2 *Information security audi*t. ProNET. https://www.pronet.ua/audit-informaczijnoi-bezpeki/
3 Korchenko, O. Hnatyuk, S., Kazmirchuk, S., Panchenko, V. Melnyk, S. (2014). *Audit and management of information security incidents*. Center of educational and scientific and scientific and practical publications of the National Academy of the Security of Ukraine. (The original was published in 2014).
4 Roy, Y. V., Mazur, N. P., Skladannyi, P. M. (2018). Information security audit is the basis of effective enterprise protection. *Electronic specialized scientific publication "Cybersecurity: education, science, technology"*, *1*(1), 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693 .
5 Burlan, S., Rudenko, N. (2017). Audit organization and methodology. Mykolaiv: Publishing House of the ChNU named after Peter's Tomb.
6 7 good reasons for conducting a technological audit of the enterprise. https://aimarketing.info/uk/blog/technichal-audit/7-vagomyh-prychyn-provedennya-tehnologichnogo-audytu-pidpryemstva.
7 Zachek O., Senyk V., Magerovska, T. (2022). Information Technology. Tutorial. Lviv: Lviv State University of Internal Affairs. http://dspace.lvduvs.edu.ua/handle/1234567890/4778
8 Matyukha, M. (2018). Computer audit. SE "Personal Publishing House". https://maup.com.ua/assets/files/lib/book/komputer_audit.pdf.
9 Information security systems. Review. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.
10 *Technical audit of equipment - SI BIS.* SI BIS https://www.sibis.com.ua/services/technical-support-and-maintanance/technical-audit-of-equipment/
11 Remote technical support - SI BIS. SI BIS. https://www.sibis.com.ua/services/outsourcing/distantsijna-tehnichna-pidtrimka/
12 Yakymenko, Yu., Savchenko, V., Legominova, S. (2022). *System analysis of information security: modern management methods*. State University of Telecommunications.
13 Drahuntsov, R., Rabchun, D., & Brzhevska, Z. (2020). Architecture security principles of the android applications-based information system. *Cybersecurity: Education, Science, Technique*, 49–60. https://doi.org/10.28925/2663-4023.2020.8.4960.
14 Drahuntsov, R., Rabchun, D. (2021). Potential disguising attack vectors on security operation centers and siem systems. *Cybersecurity: Education, Science, Technique*, 2(14), 6–14. https://doi.org/10.28925/2663-4023.2021.14.614.
15 Pentest | IT Specialist. (b. d.). https://my-itspecialist.com/products/pentest
16 *RESEARCH*. ISECOM. https://www.isecom.org/research.html.
17 *The Penetration Testing Execution Standard*. (b. d.). The Penetration Testing Execution Standard. http://www.pentest-standard.org/index.php/Main_Page
18 SP 800-115, *Technical Guide to Information Security Testing and Assessment* | CSRC. (b. d.). NIST Computer Security Resource Center | CSRC. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.
19 *OWASP Foundation, the Open Source Foundation for Application Security* | OWASP Foundation. (b. d.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://www.owasp.org
20 State enterprise "Ukrainian research and training center for problems of standardization, certification and quality" (2019). *Information Technology. Protection methods* (DSTU ISO/IEC 27007:2018). http://online.budstandart.com/ua/catalog/doc-page?id_doc=80303 .

21 ISO/TMBG Technical Management Board - groups. (2018). *Guidelines for auditing management systems* (ISO 19011:2018). https://cdn.standards.iteh.ai/samples/70017/559078f9a2634aca84ff0a6aac1498f6/ISO-19011-2018.pdf