УДК 004.56
DOI: 10.31673/2409-7292.2018.042229

**О.А. Курченко, М.В. Бржевський,
А.Б. Гребенніков, В.І. Корсун**

# ЗАГАЛЬНІ ПРИНЦИПИ ПРОВЕДЕННЯ ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті розглянуто технічні методи тестування інформаційної безпеки підприємства та розробка послідовності їх застосування. Також досліджено методи і механізми тестування інформаційної безпеки підприємства. Існуючі методи дослідження інформаційної безпеки підприємства умовно розділені на 3 категорії: методи дослідження, аналізу цілі та підтвердження наявності вразливостей. Керуючись принципами закладеними у цих методах зовнішній аудитор, за згодою замовника, може на власний розсуд формувати послідовність дій для тестування безпеки. Досі ці методики залишаються лише вказівниками для аудитора і він змушений, в значній мірі, покладатися на свій досвід і експертну думку.

***Ключові слова:*** інформаційна безпека підприємства, тестування, інформаційна безпека, безпека підприємства, методи тестування, механізми тестування, вразливість.

**Вступ.** В умовах економіки постіндустріального суспільства, інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки – усе більш складними і практично значущими. Інформаційна безпека є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства.

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою - комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

**Постановка проблеми**. Впевнитись у правильній роботі механізму забезпечення інформаційної безпеки підприємства можливо лише при наявності певного зворотного зв'язку цієї системи до керівника підприємства, або іншої уповноваженої особи. Механізмом такого зворотного зв’язку є аудит інформаційної безпеки. Питання тестування і аудиту широко розглянуті в міжнародних стандартах інформаційної безпеки, але лише в питаннях вимог до аудиторів, нормативних процесів та послідовності етапів тестування. Нерозглянутими залишаються конкретні прикладні питання аудиту, оскільки зазвичай вони повністю віддаються на розгляд до компаній аудиторів. Такий підхід є доцільним з огляду на швидкість зміни технологій та інструментів тестування. З іншого боку, відсутність навіть приблизних рекомендацій щодо методів тестування інформаційної безпеки підприємств залишає дрібний бізнес, що не може собі дозволити наймання сторонньої організації аудитора, без можливості створення ефективної системи менеджменту інформаційної безпеки. Тому доцільним є розробка алгоритму тестування інформаційної безпеки підприємства з вказанням конкретних методів і заходів.

**Аналіз останніх досліджень і публікацій**. Проблемі тестування інформаційної безпеки підприємства присвячена серія міжнародних стандартів, зокрема розділ 6 документу ISO 27001 висуває вимоги до внутрішнього аудиту СМІБ. Деякі міркування та рекомендації щодо реалізації тестування інформаційних систем надано у розділі 15.3 стандарту ISO 27002. Стандарт ISO 27006 встановлює вимоги та рекомендації до органів, що проводять аудит та сертифікацію СМІБ на додаток до ISO 27001, та в першу чергу призначений для підтримки акредитації органів, що сертифікують СМІБ. Стандарт ISO 19011 містить керівні вказівки по аудиту систем менеджменту і є доволі непоганим фундаментом для даної курсової роботи, але містять лише загальне коло питань і недостатню специфіку для цілей інформаційної безпеки. Стандарт CobiT for Assurance визначає цілі контролю інформаційної безпеки , які слід використовувати для забезпечення відповідності інформаційних технологій компанії

потребам бізнесу. У вітчизняній літературі означені питання розглядаються у НД ТЗІ 3.7-003-05, в рамках проведення робіт зі створення Комплексної системи захисту інформації. Цей документ визначає вимоги до обстеження інформаційного, фізичного та середовища користувачів ІТС і пояснює яких результатів необхідно досягти, але не пояснює як.

Досі невизначеним залишаються основні технічні аспекти оцінки інформаційної безпеки, дослідженню яких і присвячена ця робота.

**Основна частина.** Існують десятки технічних методів тестування безпеки які можуть бути використані для оцінки рівня інформаційної безпеки. Їх можна умовно згрупувати за такими категоріями [5]:

1. *Методи дослідження*. Це методи які використовуються для оцінки систем, додатків, мереж, політик і процедур для виявлення вразливих місць, і, як правило, проводяться вручну. Вони включають в себе дослідження документації, огляд конфігурації системи; сканування мережі.

2. *Методи аналізу цілі*. Ці методи тестування допомагають визначити відкриті порти, сервіси та потенційно вразливі місця, і можуть бути виконані вручну, але, як правило, здійснюється з використанням автоматизованих засобів. Вони включають в себе дослідження мережі, сканування служб і відкритих портів та сканування вразливостей.

3. *Методи підтвердження наявності вразливостей*. Ці методи тестування підтверджують наявність вразливостей, можуть бутив використані вручну або за допомогою автоматичних інструментів, в залежності від конкретної техніки і майстерності аудитора. Вони включають злом паролів, тестування на проникнення, соціальну інженерію і тестування безпеки додатків.

***Методи дослідження***

**Аналіз документації.** Аналіз документації допомагає визначити чи є комплексними та адекватними технічні аспекти політик і процедур обробки інформації в системі. Ці документи забезпечують основу системи безпеки організації, і мають бути всебічно досліджені в ході аудиту. Служба безпеки організації повинна надати аудиторам відповідну документацію для забезпечення комплексності тестування. Перелік цих документів включає в себе політику безпеки, загальна структурна схема архітектури системи, опис стандартних операційних процедур, політика авторизації, план реагування на інциденти інформаційної безпеки.

Дослідження документації може виявити прогалини і недоліки, які можуть призвести до неправильної реалізації заходів безпеки. Аудитор зазвичай перевірити, що документація організації відповідає стандартам і правилам, таким як ISO 27001, і шукають застарілі або нерелевантні політики. Наявність документації не гарантує, що контроль безпеки здійснюються належним чином а лише показує, що для підтримки інфраструктури безпеки існує загальний напрямок і вказівки. Результати аналізу документації можуть бути використані для виконання точного налаштування інших методів тестування і експертизи. Наприклад, якщо політика управління паролями має специфічні вимоги до мінімальної довжини і складності пароля, ця інформація може бути використана для налаштування параметрів злому паролів для більш ефективної роботи.

**Аналіз журналу подій.** Аналіз журналу подій визначає, чи є реєструєте підсистема безпеки належну інформацію, і чи дотримується організація власної політики управління журналами. Журнали аудиту можуть бути використані, щоб допомогти підтвердити, що система працює відповідно до встановлених правил.

Аналіз журналу подій також може виявити такі проблеми, як неправильно налаштовані служби і контролю безпеки, спроби несанкціонованого доступу, або злому. Наприклад, розміщення датчику система виявлення вторгнень (IDS) одразу за брандмауером, допоможе зібрати інформацію про мережеві запити, що проходять первинну фільтрацію і надходять у

внутрішню мережу підприємства. Якщо датчик реєструє дії, які повинні бути заблоковані, це означає, що брандмауер налаштований неправильно.

Приклади журнальованої інформації, що можуть бути корисною при проведенні аудиту інформаційної безпеки включають в себе [6]:

• Вдалі та невдалі спроби аутентифікації на сервері

• Перелік служб автозапуску та подій що відбуваються безпосередньо перед відключенням системи, встановлення програмного забезпечення, доступу до файлів, змін політики безпеки, змін ідентифікаційних даних (наприклад створення, видалення або зміна облікових записів, зміна привілегій облікових записів), політика привілегій.

• Журнали підозрілої активності, або нераціонального використання комп'ютерних ресурсів.

• Дані про вихідні з'єднання, які вказують на скомпрометованих внутрішні пристрої (наприклад, руткіти, ботів, троянських програм, шпигунського ПЗ).

• Дані про збої поновлення антивірусних баз та інші ознаки застарілих сигнатур і програмного забезпечення.

Ручна перевірка журналів може бути дуже тривалою і громіздкою. Саме тому існують автоматизовані інструменти аудиту журналів подій, що дозволяє істотно скоротити час їх аналізу і створення типових звітів, що підсумовують вміст журналу і відстежувати в них певний набір конкретних дій. Аудитори також можуть використовувати ці автоматизовані інструменти для полегшення аналізу журналу шляхом перетворення журналів різних форматів в єдиний стандартний формат для аналізу.

**Аналіз конфігурації системи.** Аналіз конфігурації системи являє собою процес виявлення слабких місць в органах управління системою безпеки. Цей тип тестування дозволяє виявити непотрібні служби і додатки, неправильні налаштування облікових записів користувачів і паролів, а також ненадійні засоби ведення журналу та параметри резервного копіювання. Тестуванню можуть бути піддані Параметри політики безпеки Windows, або файли конфігурацій безпеки UNIX у директорії /etc.

Використовуючи ручні методи тестування аудитори покладаються на керівництва з конфігурації безпеки або контрольні списки, щоб переконатися, що система налаштована оптимальним чином.

Автоматизовані методи тестування конфігурації системи швидше ніж ручні методи, але деякі налаштування все ще потрібно перевіряти вручну. Обидва методи вимагають привілеїв адміністратора або root-доступ для перегляду обраних параметрів безпеки. Як правило, краще використовувати автоматизовані перевірки замість ручних перевірок, коли це можливо.

**Сканування мережі.** Сканування мережі це пасивний метод що дозволяє слідкувати за активністю в мережі зв'язку, декодувати протоколи, а також аналізувати заголовки і корисне навантаження на хости в мережі. В якості методики тестування, сканування мережі може розглядатися також як метод аналізу цілі.

Цілі мережевого сканування:

• Захоплення і відтворення мережевого трафіку;

• Виконання пасивного дослідження мережі (наприклад, ідентифікації активних пристроїв в мережі);

• Визначення операційних систем, додатків, служб і протоколів мережі;

• Виявлення несанкціонованих і неадекватних дій, таких як незакодована передача конфіденційної інформації;

• Збір інформації, наприклад незашифрованих імен користувачів і хеші паролей.

Сніффер - інструмент, який використовується для проведення мережевого сканування - вимагає засіб для підключення до мережі, такий як концентратор, хаб, або маршрутизатор з ввімкненим режимом Spanning. Режим Spanning означає процес копіювання трафіку, що

передається на всіх інших портах до порта, де встановлений сніффер. Організації можуть розгортати сніффери пакетів в кількох місцях мережі підприємства.

Вони зазвичай включають наступні:

• По периметру, для оцінки вхідного і вихідного трафіку з мережі;

• За брандмауерами, щоб оцінити, точність фільтрації трафіку;

• Перед частиною критичної системи або додатку для оцінки адекватності його роботи;

• На певному сегменті мережі, для перевірки зашифрованих протоколів.

Єдиним обмеженням методу сканування мережі є шифрування трафіку. Якщо зловмисник буде використовувати зашифровані канали для приховання своєї діяльності, аудитори не зможуть відслідковувати його поведінку. Іншим обмеженням є те, що сніффер може прослуховувати трафік лише того локального сегмента, де він встановлений. Це вимагає від аудиторів розміщення відповідного ПЗ у різних частинах мережі та/або використання на маршрутизаторах режиму Spanning, що збільшує навантаження на мережу. Крім того, аналіз мережі є досить трудомісткою діяльністю, яка вимагає високого ступеня залученості людини у інтерпретацію даних.

**Методи аналізу цілі.** Ці методи тестування направлені на пошук та ідентифікацію активних сегментів мережі, пов'язаних з ними портів та сервісів, а також аналіз їх потенційних вразливостей.

Аудитор використовує цю інформацію, щоб підтвердити наявність вразливостей. Організації часто використовують нетехнічні методи тестування на додаток або замість технічних методів для виявлення активів, що підлягають аналізу. Наприклад, організації можуть мати переліки існуючих активів, що можуть піддатися цільовим атакам; або аудитору можуть виконати перевірку приміщень організації для виявлення активів, які не були знайдені за допомогою технічних прийомів, таких як хости, які були відключені від мережі, коли були використані технічні прийоми.

**Дослідження мережі.** Для дослідження мережі використовується ряд методів, щоб виявити активні хости в мережі, виявити слабкі місця, і дізнатися як працює мережа. Існують пасивні (експертиза) та активні (тестування) методи для виявлення пристроїв в мережі. Пасивні методи використовують мережевий аналізатор для моніторингу мережевого трафіку і запису IP-адрес активних хостів, і можуть надавати інформацію про порти що використовуються і операційні системи, що були виявлені в мережі. Пасивне дослідження може також визначити відносини між вузлами мережі, в тому числі, які хости спілкуються один з одним, як часто відбувається їх спілкування, а також типовий тип трафіку. Пасивне дослідження, як правило, здійснюється з хоста у внутрішній мережі. Пасивне сканування відбуваються без відправки жодного пробного пакету. Пасивне сканування займає більше часу ніж активне і хости що не були задіяні у комунікації за тестовий період можуть залишитись невиявленими, але при цьому воно може бути виконано непомітно для учасників мережі.

Активні методи сканування передають по мережі різні типи мережевих пакетів, наприклад ICMP та ping-запити. Одна з методик, відома як методика знімків операційної системи (OS fingerprinting), дозволяє аудитору визначити параметри операційної системи, відправляючи хосту суміш типового і нетипового мережевого трафіку, та досліджуючи його відповіді [7]. Інша методика включає в себе відправку пакетів на загальновідомі стандартні номера портів для перевірки їх активності. Спеціалізований інструмент аналізує відповіді на такі пакети, і порівнює їх з відомими типовими відповідями різних конкретних операційних систем і мережевих сервісів, що дозволяє йому ідентифікувати вузли, операційні системи, що на них працюють, їх порти, а також стан цих портів.

Ця інформація може бути використана для таких цілей:

• підготовки етапу тестування на проникнення;

• генерування топології мережі;

• визначення конфігурації брандмауера та IDS;

• виявлення вразливостей в системах і конфігурації мережі.

Існує декілька типів сканування за допомогою інструментів дослідження мережі. Системи виявлення вторгнень міжмережеві екрани корпоративного рівня можуть ідентифікувати безліч екземплярів сканування, особливо ті, які використовують підозрілі пакети (наприклад, SYN/FIN сканування, NULL- сканування) [7]. Для сканування мережі в обхід міжмережевих екранів та систем виявлення вторгнень, аудиторам слід обрати такий тип сканування, що приверне найменше уваги адміністраторів безпеки, та можливо застосовувати певні стелс-техніки, такі як більш повільне сканування, або сканування з великої кількості різних IP-адрес.

Аудитори також повинні бути обережними при виборі типу сканування для старих систем, особливо тих, про які відомо, що вони мають слабкий захист, оскільки деякі типи сканування можуть викликати збої такої системи. Як правило, чим ближче сканування до нормальної діяльності мережі, тим менша ймовірність того, що виникнуть проблеми проблеми в її роботі.

**Визначення мережевих портів та служб.** Цей метод передбачає використання сканера портів для виявлення мережевих протоколів і служб, що працюють на активних хостах, (наприклад FTP та HTTP), та конкретного програмного забезпечення цих протоколів та служб, такого як Microsoft Internet Information Server (IIS) або Apache для HTTP служби. Ця інформація може бути використана для визначення цілей для тестування на проникнення.

Всі основні сканери можуть визначити активні хости і відкриті порти, але деякі сканери також можуть надати додаткову інформацію про просканові хости. Інформація, зібрана під час відкритого сканування портів може допомогти у визначенні цільової операційної системи за допомогою процесу під назвою OS fingerprinting. Наприклад, якщо хост має відкриті TCP-порти 135, 139, та 445 – це, ймовірно, Windows-хост, або, можливо, Unix-хост на якому працює сервер Samba [7]. Підказку для ідентифікації операційної системи також можуть надати інші елементи мережевих запитів,наприклад спосіб нумерації TCP-сегментів, та формат відповідей на деякі специфічні запити. Однак метод OS fingerprinting не є надійним. Наприклад, брандмауери блокують певні порти і типи трафіку, і системні адміністратори можуть налаштувати свої системи, так, щоб вони нестандартно реагувати на специфічні запити, , щоб допоможе приховати справжню ОС.

Багато сканерів використовують спеціальний список, в якому перераховані загальні номери портів і типові супутні послуги, наприклад, ідентифікуючи відкритий 80-й TCP-порт сканер повідомляє, що на цьому порті працює веб-сервер, тому що це стандартний для нього порт, але для підтвердження цього, необхідні додаткові кроки [7].

Деякі сканери можуть ініціювати зв'язок зі знайденим портом і аналізувати його відповіді, щоб визначити, які послуги ним надаються, часто шляхом порівняння спостережуваної активності з інформацією про загальні службах і реалізації послуг. Ці методи також можуть бути використані для ідентифікації версії програмного забезпечення, що полегшить подальший пошук відомих вразливостей.

Сканери різних моделей підтримують різні методи сканування з сильними і слабкими сторонами, які зазвичай пояснюються в їх документації. Деякі сканери просто перевіряють порти на відкритість/закритість, в той час як інші пропонують додаткові деталі (наприклад, дані про фільтрованість порта мережевим фільтром), що можуть допомогти експерту визначити додаткові типи сканування для збору більшої кількості інформації.

**Сканування на вразливості.** Сканування вразливостей може допомогти визначити застарілі версії програмного забезпечення, і помилки в конфігурації системи, а також оцінити відповідність або відхилення функціонування програмного забезпечення від політики безпеки організації. Це робиться шляхом визначення операційних систем і

основних програмних додатків, що працюють на хостах і порівнянні їх з інформацією про відомі вразливості, що зберігаються в базах сканерів вразливостей.

Сканери вразливостей можуть:

• перевіряти дотримання політик безпеки програмними додатками на хостах;

• надавати інформацію про цілі для тесту на проникнення;

• надавати інформацію про те, як пом'якшити виявлених вразливостей.

Сканери вразливостей можуть працювати локально або з мережі. Деякі мережеві сканери можуть мати облікові дані адміністратора на окремих хостах і можуть добувати інформацію про вразливість хостів, використовуючи ці облікові дані. Якщо сканер не володіє такими обліковими даними, то пошук вразливостей буде в основному опиратися на сканування портів, визначення операційної системи та пошук відомих вразливостей по базі сканера.

Сканування мережі без відомих облікових записів хоста може бути виконано як ззовні так і всередині цільової системи. Незважаючи на те, що внутрішнє сканування зазвичай знаходить більше вразливостей, сканування ззовні також є дуже важливим, оскільки воно перевіряє адекватність роботи охоронного периметру системи, особливо пристроїв, що фільтрують, або блокують трафік.

**Методи підтвердження наявності вразливостей.** Мета застосування цих методів полягає в тому, щоб довести, що існує проблема вразливості системи, а також для демонстрації впливу на інформаційну безпеку, в разі експлуатації вразливості. Методи підтвердження наявності вразливостей включають найбільші ризики, оскільки ці методи мають більший потенціал впливу на цільову систему або мережу, ніж інші методи.

**Підбір паролів.** Коли користувач вводить пароль, генерується хеш введеного пароля і порівнюється зі збереженим хешем фактичного пароля користувача. Якщо хеші збігаються, то користувач проходить аутентифікацію. Підбір паролів це процес відновлення фактичних паролів з їх хеш-значень, що зберігаються в комп'ютерній системі або передаються по мережі. Це, як правило, виконується в ході аудиту для виявлення облікових записів зі слабкими паролями. Підбір паролів застосовується до хешів, що перехоплюються при передачі через мережу, або вилучаються із цільової системи, завдяки помилкам розподілу доступу. Після отримання хешів, застосовується спеціальне програмне забезпечення, що швидко генерує значення хешів на основі випадкових значень, поки не буде знайдено збіг з реальними даними хешів. Можлива також атака за словником, тобто використання для генерації не випадкових значень а типових значень слабких паролів.

Є безліч словників, доступних в Інтернеті, які охоплюють основні та другорядні мови, імена, популярні телевізійні шоу і т.д. Інший спосіб злому відомий як гібридна атака, ґрунтується на словниковому методі, додаючи числові і символічні знаки до слів зі словника. Залежно від програмного забезпечення, цей тип атаки може включати кілька варіантів замін, таких як використання загальних заміни символів і чисел для букв (наприклад, p@ssword і h4ckme). Деякі з них також будуть намагатися додавати символи і цифри на початку і в кінці слів зі словника (наприклад, password99, password$%) [8].

Ще один метод підбору паролів називається методом грубої сили. Він дозволяє отримати всі можливі паролі певної довжини і пов'язаних з ними хешів. Оскільки існує дуже багато можливостей, цей метод займає дуже багато часу, хоча, як правило, його застосування займає набагато менше часу, ніж середній час використання паролів відповідно до парольних політик. Отже, паролі, підібрані методом грубої сили також занадто слабкі. Теоретично, будь-який пароль може бути підібраний за допомогою атаки грубої сили, але лише при наявності достатньої кількість часу і обчислювальної потужності. Окрім того аудитори або зловмисники часто мають кілька машин, між якими вони розподіляють завдання підбору паролів, що значно скорочує час, що витрачається.

Підбір паролів може також бути виконаний за допомогою райдужних таблиць, це таблиці з попередньо обчисленими хешами паролів. Райдужні таблиці вимагають великої кількості дискового простору і часу для їх генерації. Крім того вони ефективні лише проти хешів що не включають сіль. Сіль – це випадкове значення, що генерується операційною системою і додається до значення паролю перед розрахунком хешу [8].

**Тест на проникнення.** Тест на проникнення це техніка, в якій аудитори безпеки імітують реальні атаки, щоб визначити методи для обходу функцій безпеки програми, системи або мережі. Вона часто включає в себе запуск реальних атак на реальні системи і дані, з використанням інструментів і методів, які зазвичай використовуються зловмисниками. Більшість тестів на проникнення включають експлуатацію вразливостей на одній або декількох системах, для отримання адміністраторських прав в системі. Тестування на проникнення також може бути корисним для визначення:

- Наскільки добре система реагує на моделі атак реального світу.
- Ймовірний рівень вмінь зловмисника для успішної компрометації системи.
- Додаткові заходи протидії, які могли б пом'якшити загрози проти системи.
- Здатність системи до виявлення атак і реагування відповідним чином.

Тестування на проникнення може бути безцінним, але це трудомісткий процес, що вимагає великого досвіду, для зведення до мінімуму ризику для цільових систем. Системи можуть бути пошкоджені або іншим чином виведені з ладу в процесі тестування на проникнення. Хоча досвідчені аудитори можуть зменшити цей ризик, він ніколи не може бути повністю усунений. Тестування на проникнення повинно виконуватися тільки після ретельного моделювання, підготовки та планування.

Тестування на проникнення часто включає в себе нетехнічні методи атаки. Наприклад, аудитор може порушити фізичні механізми контролю та процедури безпеки для підключення до мережі, вкрасти обладнання, захопити конфіденційну інформацію (можливо, шляхом установки кейлогерів), або порушити зв'язок. Слід дотримуватися обережності при виконанні тестування фізичної безпеки, охоронці повинні бути інформовані про те, як відрізнити аудитора від реального зловмисника, ці процедури повинні бути описані у відповідній документації, або контракті. Іншим нетехнічних засобом атаки є використання соціальної інженерії, наприклад дзвінок до користувача системи начебто від імені адміністратора з проханням повідомити пароль, або дзвінок від фіктивного користувача системи адміністратору з проханням змінити загублений пароль.

**Результати досліджень.** Тестування інформаційної безпеки підприємства складається з 4 фаз. Кожна фаза реалізується з застосуванням методів описаних вище і відбувається в такому порядку:

- Фаза планування.
- Фаза дослідження.
- Фаза атаки.
- Звіт.

На етапі планування, визначаються правила аудиту, документально встановлюється мета аудиту та підтвердження обізнаності керівництва про майбутнє тестування. Етап планування встановлює основу для успішного тесту на проникнення. Фактичного тестування в цій фазі не відбувається.

Фаза дослідження складається з двох частин. Перша частина є початком фактичного тестування, і охоплює збір інформації та сканування.

Друга частина фази виявлення є фактичним аналізом вразливостей, який включає визначення сервісів, додатків і операційних систем сканованих хостів пошук по базам вразливостей (процес, який відбувається автоматично для сканерів вразливостей) і ручне тестування експертом аудитором. Експерти можуть використовувати свої власні бази для виявлення вразливостей вручну.

Далі слідує фаза атаки. Вона складається з таких кроків:

• Отримання доступу до системи
• Підвищення власних привілеїв
• Дослідження системи всередині
• Встановлення додаткових утиліт для полегшення повторного доступу

Якщо атака пройшла успішно, вразливість документується і розробляються рекомендації для її усунення. У багатьох випадках, експлуатовані вразливості не надають максимальний рівень потенційного доступу для зловмисника. Замість цього вони можуть надати аудиторам додаткові інформацію про цільову мережу і її потенційних вразливості, або викликати зміна стану безпеки цілі. Деякі вразливості дозволяють аудиторам підвищувати свої привілеї в системі або мережі, та отримувати доступ до додаткових ресурсів. Якщо це стається, необхідно проведення додаткового аналізу і тестування, щоб визначити справжній рівень ризику для мережі, та типи інформації, що може бути скомпрометована. В рази виявлення неможливості експлуатації вразливості, аудитор повинен спробувати використати інші виявлені вразливості.

Фазу звітності відбувається одночасно з іншими трьома фазами випробувань на проникнення. У фазах дослідження та атаки, зазвичай записуються для подальшого зберігання журнали подій і формуються періодичні звіти для системних адміністраторів і менеджменту. По завершенні тестування, звіт, як правило, розробляється для опису виявлених вразливостей, оцінку ризику, а також подальшими рекомендаціями, щодо пом'якшення ризику.

**Висновки.** Питання аудиту інформаційної безпеки описані у значній кількості літератури, включаючи іноземну та вітчизняну, як в стандартах так і в прикладних практичних довідниках. Крім того методики оцінювання відрізняються в залежності від сфери їх застосування і конкретного виду діяльності підприємства. Однак досі не існує єдиного стандарту та методології для технічного аудиту інформаційної безпеки.

Існуючі методи дослідження інформаційної безпеки підприємства умовно розділені на 3 категорії: методи дослідження, аналізу цілі та підтвердження наявності вразливостей. Керуючись принципами закладеними у цих методах зовнішній аудитор, за згодою замовника, може на власний розсуд формувати послідовність дій для тестування безпеки. Досі ці методики залишаються лише вказівниками для аудитора і він змушений, в значній мірі, покладатися на свій досвід і експертну думку.

Проблема досі залишається невирішеною, оскільки механізми захисту у різних підприємствах мають гетерогенний характер та абсолютно різні цілі. Тому доцільним є подальше вивчення питань технічного аудиту інформаційної безпеки підприємств та розробка нових методів дослідження з урахуванням специфіки різних операційних систем, апаратного забезпечення та формальних моделей безпеки.

**Список використаних джерел**

1. Технічний захист інформації [Електронний ресурс] // Режим доступу: http://tzi.com.ua/audbezib.html

2. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення Комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

3. ISO/IEC 27001. Information technology -- Security techniques -- Information security management systems – Requirements // 2015.

4. ISO/IEC 27002. Information technology – Security techniques – Code of practice for information security management. // 2013.

5. В.И Аверченков Аудит информационной безопасности, учебное пособие // ФЛИНТА 2011.

6. Logging The Ultimate Guide [Електронний ресурс] // Режим доступу: https://www.loggly.com/ultimate-guide/linux-logging-basics/

7. Справочное руководство Nmap (Man Page) [Електронний ресурс] // Режим доступу: https://nmap.org/man/ru/

8. FreeBSD Handbook [Електронний ресурс] // Режим доступу: https://www.freebsd.org/doc/handbook/