МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему

«Методика аудиту інформаційної безпеки на стійкість до атак соціальної інженерії»

Завідувач

випускаючої кафедри **Любчак В.О.**

Керівник роботи **Лаврик Т.В.**

Студентки групи КБ-81 **Тімченко А.В**

СУМИ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____

Зав. кафедрою Любчак В.О.

“_____” _____2022 р.

ЗАВДАННЯ

до бакалаврської роботи

Студентки четвертого курсу, групи КБ-81 спеціальності “Кібербезпека” денної форми навчання Тімченко Аліни Віталіївни.

Тема: “Методика аудиту інформаційної безпеки на стійкість до атак соціальної інженерії”

Затверджена наказом СумДУ

№_____ від _____2022 р.

Зміст пояснювальної записки: 1) аналіз предметної області дослідження; 2) характеристика методів і засобів аудиту інформаційної безпеки; 3) розробка методики аудиту інформаційної безпеки на стійкість до атак соціальної інженерії.

Дата видачі завдання “_____”_____2022 р.

Керівник бакалаврської роботи _____ Лаврик Т. В.

Завдання прийняв до виконання _____ Тімченко А.В.

РЕФЕРАТ

Записка: 67 стор., 24 рис., 2 табл., 52 джерела.

Мета роботи — розроблення методики аудиту інформаційної безпеки на стійкість до атак соціальної інженерії.

Об'єкт дослідження — основні техніки соціальної інженерії у розрізі інформаційної безпеки організації.

Предмет дослідження — методи і прийоми проведення аудиту інформаційної безпеки на схильність до атак соціальної інженерії.

Результати — розроблено методику і загальні принципи аудиту інформаційної системи підприємств на стійкість до атак методами соціальної інженерії, створений послідовний опис етапів проведення аудиту інформаційної безпеки.

ІНФОРМАЦІЙНА СИСТЕМА, ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ, СОЦІАЛЬНИЙ ІНЖЕНЕР, АТАКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, ЗОВНІШНІЙ АУДИТ, ВНУТРІШНІЙ АУДИТ, АУДИТОРСЬКА ДІЯЛЬНІСТЬ, АНАЛІЗ РИЗИКІВ, МЕТОДИКА АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, МЕТОД

ЗМІСТ

ВСТУП

У наш час значної комп’ютеризації в кожної людини «під рукою» майже завжди є потужний смартфон, а вдома, у більшості людей розвиненого світу, є стаціонарний персональний комп’ютер (ПК) або ноутбук. З кожним днем усе більше й більше підвищується попит на послуги, що пов’язані з обробкою інформації. Її роль у житті людини стає значною, але разом із цим виникає величезна частка потенційних загроз.

Порівняно велика кількість людей і організацій зацікавлені в тому, щоби придбати, викрасти, обміняти на будь-що персональні дані. Задля довгострокового зберігання інформації сьогодні використовують різні оптичні носії. У цей час величезною проблемою постають загрози втрат, викрадення, неправомірного доступу та використання інформації. Тому, як наслідок, надзвичайно актуальним постає питання захисту інформації. Більшість інформаційного суспільства приєднується до світової павутини, але навіть на цьому етапі від рівня безпеки зберігання, обробки й подальшого використання даних залежить не тільки добробут, але й більш важливе — життя людини. Фірмам, організаціям, вкрай необхідно уміти виявляти такі загрози на ранніх етапах, а ще краще — попереджувати їх. Для цього впроваджуються найрізноманітніші заходи захисту, які ефективно й незалежно від видів бізнесу чи форми власності, позитивно впливають на функціонування інформаційних систем даних організацій. Для успішної роботи мало впроваджувати лише такі заходи, треба бути впевненими в тому, що все працює належним чином, а захист відбувається на високому рівні. Для цього необхідно постійно спостерігати й досліджувати стан інформаційної системи (ІС), діставати незалежні, але об’єктивні, якісні й кількісні оцінки її роботи, а також актуальні рекомендації щодо виявлених інформаційних ризиків. Задля забезпечення даного етапу треба проводити системний процес аудиту безпеки ІС.

На сьогодні аудит інформаційної безпеки доцільно використовувати в будь-яких сферах, починаючи від впровадження самостійної системи безпеки й закінчуючи його проведення після завершення всієї загальної процедури. Аудит безпеки ІС вирішує широкий спектр запитань беручи свій початок від того, що може показати рівень системи безпеки, і до того, як привести раніше створену систему у відповідність до оновлених вимог, упорядкувати і систематизувати сучасні заходи, спрямовані на забезпечення захисту. За допомогою нього ми можемо збирати, аналізувати інформацію щодо системи, яку перевіряємо, що проводиться за допомогою кількісної та якісної оцінки рівня захищеності від ймовірних атак.

Незалежно від засобів захисту у випадку кібератаки людський фактор може виявитися вирішальним. Соціальна інженерія включає безліч технічних і психологічних прийомів, що дають змогу виманити в людини конфіденційні дані. І, далеко не завжди, жертві вчасно вдається розпізнати подібну атаку.

Перевірити обізнаність персоналу дозволяє аудит методами соціальної інженерії. Комплексна оцінка захищеності компанії допомагає оцінювати дії співробітників, дізнаватися, чи дотримуються вони відповідних інструкцій і рекомендацій, рівень стійкості методами соціальної інженерії.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальна характеристика існуючих загроз для підприємств малого і середнього бізнесу

Стрімке зростання попиту щодо інформаційних технологій упродовж останніх десятиріч призвів до кардинальних змін у суспільстві. Основною цінністю для людства взагалі й певної людини зокрема стає інформація, яка стає новим чинником виробництва [1, с.170].

З плином часу організація соціуму трансформується у вигляді перерозподілу традиційної влади до управління інформаційно-комунікаційними потоками, постійно зростає впливовість засобів масової інформації (ЗМІ). Тотальна автоматизація та комп’ютерні алгоритми докорінно змінюють світ.

На сьогодні проблеми національної безпеки виходять на перший план у контексті загального розвитку країни та безпеки інформаційного середовища, які є одними із найвпливовіших чинників у сфері державної безпеки України.

Інформаційну безпеку доцільно розглядати як самостійний складник національної безпеки. Проявлення її двостороннього характеру зумовлено:

– бажанням кожної держави захистити власні інтереси, які ставлять собі за мету сформування та накопичення інформаційного потенціалу завдяки розширенню інформаційних процесів у світі;

– необхідністю розвитку й захисту національного інформаційного потенціалу від сучасних інформаційних загроз та потенційних негативних наслідків ІТ-технологій;

– інформаційний тиск на свідомість і (або) підсвідомість реальних індивідів, суспільство й державу в цілому, що загрожує національній безпеці [2, с.1-2].

Національна безпека є невід'ємною складовою інформаційної безпеки. З бурхливим розвитком технічного прогресу її залежність стрімко зростає з кожним днем. На сьогодні існує велика кількість різноманітних визначень відносно інформаційної безпеки, проте єдиної думки щодо поняття в науковців немає.

Інформаційна безпека як складник національної безпеки забезпечується на належному рівні, проте проблема стану захисту інформації є й донині, оскільки немає єдиних правил у нормативно-правових документах і в науково-дослідницькій літературі про те, що, як і від чого ми маємо захищати. Методологічні підходи та логічні способи суттєво відрізняються один від одного, так як сама категорія інформаційної безпеки досить неоднозначна і вивчається залежно від конкретної області застосування. Наприклад, філософи розкривають її як тенденції розвитку й умови життєдіяльності соціуму, що визначаються політичними і правовими настановами, за яких забезпечується збереження їх якісної визначеності та вільне функціонування [3, с.42]; психологи – як необхідність у захисті суттєво необхідних і важливих потреб людини; юристи – як деяку систему встановлених законом гарантій прав і свобод.

Дослідимо різні погляди відносно визначення поняття "інформаційної безпеки" та проблем захищеності національного інформаційного простору.

На початку розвитку і становлення наукового розуміння спостерігалось ототожнення двох понять "інформаційної безпеки" і "безпеки інформації".

А.А Тер-Акопов розумів під інформаційною безпекою стан захищеності інформації, що забезпечує життєво важливі інтереси людини [4]. Але так зване ототожнення спостерігалося не лише в працях вітчизняних науковців, а й у зарубіжних. Яскравим прикладом цього стало визначення Л.Дж. Хоффмана: "Інформаційна безпека – це особливий стан інформації, у якому забезпечується

збереження безпеки властивостей інформації попередньо визначених політикою безпеки” [5].

Проте переважна більшість частина науковців чітко розмежовує між собою ці два фактори, спираючись на те, що під час визначення безпеки інформації об’єктом є інформація, відносно інформаційної безпеки – складова цілого.

Інформаційна безпека в уяві В.М. Фурашева постає у вигляді “стану захищеності життєво важливих інтересів людини, суспільства й держави загалом і в цілому ...” [6, с.163].

Позиція О.П. Дзьобаня і В.Г. Пилипчука є досить близькою до думки Фурашева В.М. У своїй праці вони дотримуються такого розуміння поняття: “Інформаційна безпека — це стан захищеності життєво важливих інтересів людини, суспільства й держави в інформаційній сфері від зовнішніх та внутрішніх викликів і загроз, що забезпечує їх сталий розвиток” [7, с.150].

У свою чергу, О.А. Баранов надає більш деталізовані виклики й загрози під час визначення інформаційної безпеки, при якому зводиться до мінімуму завдання шкоди через несвоєчасне надання недостовірної й неповної інформації під час її несанкціонованого поширення [8].

Науковець О.Д. Довгань розглядає сучасні інформаційні структури як компоненти інформаційної безпеки [9, с.111-112] і результат управління зовнішніми та внутрішніми викликами й загрозами з використанням правових методів відносно захищеності інтересів як окремої людини, так і держави в цілому.

Ю.А. Фісун характеризує інформаційну безпеку як своєрідний стан захищеності інформаційного середовища, який відповідає встановленим інтересам держави, завдяки якому забезпечується формування розвитку незалежно від впливу інформаційних загроз [10, с.11].

Зробивши детальний аналіз позицій науковців щодо тлумачення феномену, можна дійти до висновку, що поняття інформаційної безпеки можна розглядати на основі декількох аспектів. Інформаційна безпека являє собою:

– стан захищеності інформаційного середовища, що відповідає інтересам держави, за якого забезпечується формування, використання й можливості розвитку незалежно від дії внутрішніх і зовнішніх інформаційних загроз;

– стан інформаційного середовища й політичної еліти суспільства, який забезпечує формування й розвиток і інтересах керівництва країни й суспільства [4].

Демонстрування різноманітності підходів стосовно категорії “інформаційної безпеки” в XXI столітті вказує на те, що вона є однією із найважливіших концепцій у сфері науки.

Проблема повсякчасного збільшення рівня інформаційної безпеки сучасного підприємства в повній і значній мірі залежить від ступеня захищеності інформаційної сфери, яка безперервно має свій вплив на розвиток і впровадження особливих наукових інновацій у залежні від нього процеси виробництва [11, с.1].

З бурхливим розвитком наукового-технічного процесу активно зростає важливість дослідження питання інформаційної безпеки особистості, суспільства й держави.

Незалежно від сфери функціонування підприємства, організація працює в мовах повсякчасного впливу конструктивних і деструктивних чинників зовнішнього і внутрішнього середовища. На відміну зовнішнього середовища внутрішнє може контролюватися менеджментом організації, проте несвоєчасне реагування на виклики безпеки призводить до виникнення негативних факторів впливу. За величиною можливих наслідків виділяють такі види дестабілізуючих чинників: попередження, ризик і загроза [12, с.113].

Попередження — це комплекс обставин життєдіяльності, не в обов'язковому випадку небезпечного характеру, який потребує швидких протидій. За відсутності реагування організації на даний фактор попередження може перетворитися на ризик.

Ризик — це свідоме сприймання можливості небезпеки чи втрат у будь-якій справі. Ризик не завжди становить небезпеку, а лише передує потенційну умову для чогось; виникає лише в тих випадках, коли є декілька сценаріїв розвитку подій і відповідних можливих результатів.

Загроза — це реальна можливість або невідхильного виникнення небезпеки під впливом навмисного чи ненавмисного характеру проведення дій; те, що може спричинити відхилення від тактики.

Попередній аналіз ключових визначень щодо питання деструктивних чинників впливу дає зрозуміти те, що лише загрози завдають найбільшої шкоди активам підприємства [12, с.113].

Під час виконання організації своєї діяльності підприємець в обов'язковому порядку повинен бути обізнаним щодо обробки, зберігання й ліквідації непотрібних даних. Якщо деяка інформація є все ж таки цінною для підприємства, необхідно належним чином охороняти її від потенційних зловмисників. Цінність активів мусить виражатися через низку необхідних параметрів: актуальність, корисність і достовірність. Задля забезпечення безпечних умов зберігання даних слід запобігти перехопленню усіх каналів можливого витоку конфіденційної інформації [11, с.2].

Розглянемо чинники загроз зовнішнього характеру [11, с.2]:

– викрадення чи копіювання цінних документів, флеш-носіїв;
– пошкодження матеріальних об'єктів зберігання інформації;
– крадіжка особистих даних за допомогою інсайдерів;
– залучення персоналу до праці й інші підприємства.

Одними з найпоширеніших небезпек внутрішнього характеру є крадіжка, розповсюдження вірусів, псування файлів співробітниками організації.

Основні фактори внутрішніх загроз організації — причини внутрішнього характеру взаємодії співробітників компанії між собою й керівництвом, невдоволення рівнем заробітної плати [11, с.2].

Отже, питання захищеності інформаційних ресурсів в організації є одним із ключових аспектів задля відповідного функціонування підприємства.

1.2 Характеристика методів проведення атак із використанням інструментів соціальної інженерії

Інформаційні системи (ІС) сьогодення на даному етапі розвитку не можливо відокремлювати від суспільства, які надають величезні можливості практично у всіх сферах життя людини — навчанні, роботі та дозвіллі.

Одна із серйозних вимог щодо ІС — забезпечення інформаційної безпеки (ІБ) інформації, яка є конфіденційною. Застосування інформаційних технологій мають великий вплив на людську свідомість, надають низку переваг тим, хто вміє їх застосовувати. Останній ключовий чинник призводить до зростання важливості ролі людського чиннику в питаннях щодо інформаційного захисту системи [13, с.1].

Людина завжди була і є однією із найважливіших складових ризиків будь-якого підприємства, оскільки більша частина інцидентів виникала через провину співробітників в організації [14], які піддавалася атаці й не могли миттєво розпізнавати потенційну загрозу і зловмисника. Наслідками даних подій зазвичай було порушення конфіденційності й цілісності інформації фірм і установ.

Останнім часом під час створення комплексних систем захисту інформації на людський фактор дедалі менше звертають уваги через стрімкий розвиток інформаційних технологій [13-14]. Під час розроблення відповідних систем захисту інформації в першу чергу увагу приділяють питанню неавторизованого доступу. Проте не завжди є обов’язковим факт знешкодження системи захисту, достатньо використання іншого, більш простого способу — людські якості працівника організації.

На жаль, в Україні не існує єдиного ухваленого документу щодо регулювання норм політик ІБ проти впливу на ІС потенційного зловмисника, який володіє необхідними знаннями у сфері соціальної інженерії.

1.2.1 Методика досліджень соціальної інженерії

Соціальна інженерія у сфері ІБ — спосіб самовільного доступу до захищених інформаційних систем, який бере за свою основу способи впливу на людську свідомість [13]. Заданий метод поєднує в собі не тільки неабиякі глибокі знання щодо ІТ, а й навички й уміння із соціальної психології людини.

Людський чинник являє собою систему основних соціологічних властивостей людини, який базується виключно на психологічних характеристиках людини [14].

Соціальний інженер — спеціаліст широкого профілю, який володіє всіма необхідними навичками гнучкого мислення в області ІТ, комп'ютерних систем і мереж; використовує усі можливі способи задля примушення людини робити ті дії, які за звичайних умов вона б не здійснила у жодному разі на прохання незнайомої людини.

У понятті ІБ соціальний інженер виступає як порушник ІБ, що вміє завдяки навичкам соціальної інженерії, обману й шахрайству психологічно впливати на людину, тим самим підштовхуючи її до певних несанкціонованих дій з інформацією.

Основні загрози соціальної інженерії [13, с.1-2]:

– безконтрольний вихід конфіденційний відомостей за межі ІС;

– обхід програмних комплексів захисту інформації від витоку інформації;

– порушення авторського права;

– шахрайство в інформаційних мережах;

– пошкодження сучасних інформаційних технологій і засобів організації;

– модифікація чи знищення відкритої інформації користувачами.

Зазвичай спеціаліст зі сфери соціальної інженерії точно й безумовно розуміє, як можна скористатись особливими якостями людської натури потенційної жертви. Детально розглянемо основні прийоми природи людини й дослідимо, які використовуються процеси маніпулювання соціальними інженерами найбільш часто [13, с.2, 15, с.123-124]:

1. Відчуття авторитетності.

Індивідам властиве бажання задовольняти запит людини з більшим авторитетом. Головна мета способу полягає в тому, щоби запевнити особу у владі запитувача ставити питання й будь-що просити. Таким чином, злочинець видає себе за авторитетну особу з відділу IT і дізнається усю необхідну інформацію.

2. Відчуття спорідненості.

Частіше за все, люди мають звичку вірити й покладатися виключно на ту особу, яка має схожі з нею думки, погляди та інтереси. Заданий спосіб переконує людину у схожості її зі злодієм за будь-яких вагомих чинників задля виклику до себе довіри потенційної жертви.

3. Взаємодопомога.

Підсвідомо людина може відповісти на поставлене питання в разі отримання нею щось натомість. У вигляді “подарунку” можуть бути не тільки матеріальні речі, а й духовні цінності. Коли людина щось робить щодо відношення до нас, ми демонструємо прояв бажання віддячити їй будь-яким способом. Спосіб переконує особу в тому, що їй прагнуть допомогти або виконати замість неї послугу.

4. Відчуття відповідальності.

Людям притаманна стереотипна поведінка щодо виконання обіцянок і зобов’язань, які роблять будь-що задля здійснення дотримання слова і виконання обіцяного незважаючи на перепони.

5. Соціальна належність до групи.

Заданий спосіб полягає в запевнені людини в належності до конкретної команди і спричиняти відчуття того, що особа є складовою частиною чогось.

6. Відчуття терміновості.

У стані стресу й поспіху люди дуже часто губляться і стають не уважними по відношенню до своїх дій. Коли часу обмаль на виконання конкретно поставлених задач, особа “вибивається” зі своєї притаманної і звичної зони комфорту.

1.2.2 Методологія атак соціального інженера

Дослідимо основні техніки соціальної інженерії в розрізі інформаційної безпеки організації [16, 17, с.184-185]:

– фішинг атаки — одна із найпопулярніших атак у соціальній інженерії, який бере за свою основу отримання незаконного доступу конфіденційних даних користувачів (логін, пароль, номер банківського рахунку, платіжних карт, PIN-кодів, адресних книг тощо). Спосіб проведення: зазвичай злочинець використовує фальшиві e-mail адреси для розсилки через соціальні мережі листів, які схожі на офіційні. Особливо небезпечним різновидом фішингу є “таргінг”, під час якого обирають конкретну людину у вигляді об’єкта, що володіє необхідними службовими обов’язками і працює з повідомленнями від зовнішніх відправників;

– бейтинг атаки — застосовують у свої діяльності злоякісні програми, що починають своє виконання лише після того, як потенційна жертва відреагує на запит зловмисника. Соціальний інженер має можливість збирати, аналізувати й модифікувати отриману ним інформацію та ресурси користувача задля власних цілей;

– претекстинг — це атака, яка відтворюється завдяки підготовленому сценарію, під час якої зловмисник видає себе за іншу людину та викрадає конфіденційні дані жертви;

– зворотна соціальна інженерія — це прийом соціальної інженерії, під час якого ціль атаки самостійно звертається по допомогу до зловмисника. Задля досягнення поставленої мети використовуються різноманітні техніки, наприклад диверсія чи реклама;

– “дорожнє яблуко” — метод атаки, що базується на підкиданні заражених фізичних носіїв інформації.

Отже, знання прийомів і схем атак соціальної інженерії є важливим чинником, проте не менш необхідним обізнаність щодо захисту від них. Перш за все необхідно пропрацювати над своїми якостями, які частіше за все експлуатуються зловмисниками: довіра, милосердя, співчуття тощо. Головна ціль соціальних інженерів — отримання матеріальної вигоди або IT-ресурсів компанії-жертви. Основним способом захисту від соціальної інженерії є обізнаність у цій сфері. Усі працівники повинні в повному обсязі мають знати щодо небезпеки розкриття конфіденційних даних і способах її застереження, мати чіткі інструкції щодо того, як і які теми можна обговорювати зі співрозмовником.

1.3 Постановка задачі

На сьогодні день послуга аудиту безпеки ІС набуває широкого розповсюдження на ринку інформаційної безпеки, проте все частіше замовники і виконавці заданої перевірки сприймають її зовсім по-різному.

Недостатній розвиток аудиторської діяльності в Україні постає основною проблемою удосконалення аудиторської перевірки висококваліфікованими спеціалістами, яка потребує загального аналізу й невідкладного розроблення особливої методики вдосконалення аудиту безпеки.

Методикою аудиту передбачається визначення сукупності методів і прийомів, необхідних інструментів і засобів для дослідження стану та поведінки досліджувальних об’єктів відповідно поставленій меті й цілі.

Будь-яка аудиторська група фахівців з особливою увагою ставиться до питання розроблення методики аудиту безпеки ІС, враховуючи при цьому ряд кількох важливих чинників, наприклад, об’єкт дослідження, галузь діяльності фірми, враховуючи обізнаність аудиторів тощо. Під час одержання кількісних і якісних оцінок про актуальний стан безпеки ІС компанії, аудитори використовують власноруч розроблені ними методики, які весь час змінюються й доповнюються в залежності від того, яка головна мета аудиту, поставлені завдання, щодо якого підприємства здійснюється комплекс аналітичних робіт.

На жаль, актуальної єдиної й безкоштовної методики аудиту безпеки ІС не існує, тим паче яка б включала в себе розгляд питань відносно стійкості до атак соціальної інженерії. Через необізнаність малих і середніх підприємств із питання проведення аудиту ІБ виникає велика кількість кібератак, які пов’язані з людською поведінкою та чинниками, які на неї мають безпосередній вплив.

Отже, актуальність теми кваліфікаційної роботи бакалавра зумовлена необхідністю розроблення загальних принципів аудиту ІС підприємств на стійкість до атак методами соціальної інженерії.

2 ХАРАКТЕРИСТИКА МЕТОДІВ І ЗАСОБІВ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Особливості аудиту інформаційної безпеки для підприємств малого бізнесу

Однією із ключових ролей в забезпеченні діяльності роботи державних комерційних підприємств відіграють ІС. Поширене застосування ІС в інформаційних процесах робить актуальним проблеми їхньої захищеності, особливо безперервно зростаючого числа атак на ІС, які спричиняють не лише суттєві фінансові та матеріальні збитки, але призводять до більш серйозних і значних негативних наслідків. Задля дієвого захисту компаній від інформаційний атак потрібна об’єктивна оцінка рівня інформаційної безпеки, яка обумовлена аудитом безпеки.

Сталого визначення поняття “аудиту безпеки” не існує, проте у загальному випадку його можна представити як послідовну зміну станів збору та аналізу інформації щодо інтелектуальної власності для забезпечення двох факторів — кількісної і якісної оцінки рівня захищеності системи від кібер-зловмисників. Доцільність використання аудиту безпеки ІС полягає у здійсненні підготовки необхідного технічного завдання для комплексної системи захисту інформації та застосування доцільної системи безпеки для оцінювання рівня ефективності [18, с.87].

Аудит безпеки вживають для систематизування та упорядкування ІС та існуючих заходів з організації захисту інформації або для дослідження несприятливих подій, які сталися під час порушення інформаційної безпеки системи [19, с.697].

Задля виконання аудиту системи ІБ зовнішні компанії представляють власні послуг різного характеру, у тому числі й в області інформаційної

безпеки. Ініціатором проведення даної послуги може стати головне управління підприємства або служба ІБ [18, с.87]. Системний процес отримання об’єктивних і кількісних оцінок про поточний стан ІС досягається відповідною групою експертів ІБ, які залежать від конкретних цілей і завдань проведення обстеження, а також складності досліджувального об’єкта оцінки.

2.1.1 Основні напрямки діяльності в області аудиту безпеки інформації

За формою і метою здійснення розрізняють внутрішній і зовнішній аудит інформаційної безпеки. На сьогодні в нашій державі лише невелика частина деяких підприємств використовує внутрішній аудит, на відміну від вітчизняних підприємств, серед яких більш поширеним є застосування зовнішнього аудиту.

Є велика кількість різноманітних підходів щодо визначення понять “внутрішнього” й “зовнішнього” аудиту інформаційної безпеки та виявлення відмінностей щодо них. Дослідженню цього питання присвятили свої науково-дослідницькі праці вчені та практики, зокрема: Бутинець Ф.Ф., Кулаковська Л.П., Потопальська Г.Г., Назарова К.О., Савченко В.Я. та інші [20, с.78].

Підхід Бутинця Ф.Ф. полягає в тому, що науковець визначає аудит інформаційної безпеки як своєрідну експертизу. Сутність експертного дослідження базується на підтвердженні будь-яких фактів, проте поняття аудиту інформаційної безпеки є більш ширшим поняттям [21].

Кулаковська Л.П. розглядає зовнішній аудит як змогу зовнішніх груп спостерігати та контролювати діяльність конкретної організації й керівництва завдяки аудиторським фірмам, а внутрішній аудит — як складник загальної системи управління. Функції системи контролю, обробки й оцінювання якості інформації залежать від мети й завдань, які поставлені перед керівництвом у вигляді аудиту підприємства [22, с.14].

У свою чергу, Назарова К.О. визначає внутрішній аудит як один із способів з надання відповідних рекомендацій задля удосконалення діяльності організації та досягнення головних цілей із застосуванням визначених підходів до оцінки та управління ризиками [23, с.96].

Бачення поняття “внутрішнього аудиту” Потопальською Г.Г. полягає у діяльності аудиторської групи, яку можна розглядати як окремий вид аудиторських послуг, які визначаються і надаються в особливому порядку незалежним аудитором підприємству. Натомість зовнішній аудит дослідниця розглядає як самостійний елемент інфраструктури ринку, який з’єднує між собою користувачів інформації та її елементів, встановлює між ними довіру і прозорість, сприяє розширенню ділових відносин. Отже, внутрішній аудит працює на “внутрішньому полі” компанії, а зовнішній — на “зовнішньому” [24, с.94].

Савченко В.Я. визначає службу внутрішнього аудиту як складову частини системи внутрішнього контролю підприємства, на яку покладаються окремі функції перевірки і оцінювання ефективності механізмів систем і внутрішнього контролю [25, с.204, 246].

Зробивши теоретичне дослідження позицій науковців щодо тлумачення двох феноменів (рис.2.1), можна дійти до висновку, що:

– зовнішній аудит інформаційної безпеки проводиться із залученням сторонньої організації, за ініціативою керівництва компанії або акціонерів, коли підприємству необхідно підтвердити те, що вона відповідає встановленим галузевим стандартам і державним нормам;

– внутрішній аудит інформаційної безпеки здійснюється відповідно до плану підприємством, під час якого використовуються ресурси і відділ внутрішнього аудиту, який затверджується керівництвом компанії. Відбувається в тому випадку, коли організація хоче перевірити власний бізнес на відповідність політикам і процедурам.

У процесі здійснення детального аналізу та порівняння ознак зовнішнього і внутрішнього аудиту стає зрозумілим те, що за багатьма критеріями вони схожі та взаємодоповнюють один одного: обидва з них використовують однакову нормативну базу та особливі методи під час виконання конкретних завдань. Відмінність полягає в меті, завданні, призначенні, організації служби, користувачах інформацією тощо. Розглянемо більш детально кожну з ознак зовнішнього і внутрішнього аудиту інформаційної безпеки на табл. 2.1 [22, 26, с.346-348, 27, с.43-44].

Таблиця 2.1 – Порівняльна характеристика зовнішнього і внутрішнього аудиту

Ознака	Зовнішній аудит	Внутрішній аудит
1	2	3
Мета і завдання аудита	Підтвердження ведення обліку належним чином, вчасне складання звітів та оцінка відповідності внутрішнього аудиту меті і відповідній політиці діяльності суб'єкта [28, с.14].	Полягає в забезпеченні збереження власності та економно використанні матеріальних і трудових ресурсів, виконанні конкретних завдань і дотримання відповідних нормативів [28, с.15].
Вид діяльності	Підприємницька діяльність	Виконавська діяльність
Кваліфікація	Чітко визначений законодавством	Визначається за допомогою головних управляючих структур
Відповідальність	Відповідальні перед клієнтами і третіми особами	Підзвітні та відповідальні лише перед керівництвом підприємства

Продовження таблиці 2.1

1	2	3
Суб’єкт здійснення	Сертифіковані (незалежні) професіонали та експерти, які виконують функцію підтвердження на основі складання договорів	Здійснюється спеціалістами з обліку, контролю і аналізу, які є частиною штату підприємства
Об’єкт здійснення	Визначається статутом підприємства у вигляді стану обліку і звітності, перевірки ефективності використання ресурсів і рівня внутрішнього контролю	Визначається керівництвом підприємства у вигляді стану обліку і перевірки внутрішнього контролю, операцій і використання ресурсів
Взаємозв’язок	Залежно від якості проведення внутрішнього аудиту визначається обсяг, зміст і характер	Залежно від діяльності й ефективності проведення зовнішнього аудиту визначається обсяг, зміст і характер
Орієнтація в роботі	Аудит орієнтований на звітність та джерела доходів, за основу яких приймають необхідні групування за видами ресурсів і проведених операцій	Робота аудиту орієнтується залежно від наявних потреб управління в системі

Продовження таблиці 2.1

1	2	3
Організація роботи	Визначається аудитором самостійно на основі загальноприйнятих норм і правил аудиторської перевірки	Виконання конкретних завдань керівництва
Взаємовідносини	Рівноправ'я і незалежність, партнерство	Підпорядкованість керівництву підприємства, залежність від нього
Масштаб перевірки	Проведення визначається видом аудиту та законодавчими актами, що регулюють його проведення	Виступає у ролі взаємозалежних функцій з системою управління
Звітність	Зовнішній аудитор звітує аудиторським висновком (звітом) у письмовому вигляді перед замовником	Внутрішній аудитор звітує виключно перед своїм керівництвом
Періодичність здійснення	Є періодичним і визначається виключно керівництвом підприємства	Є частиною внутрішнього контролю, який має бути постійним і безперервним
Відношення до збереження активів	Пов'язаний із розкриттям фактів шахрайства і викривлення звітності	Пов'язаний із забезпеченням безпеки активів у повному обсязі, виявленням і усуненням заборгованості з нестач, розкрадань

Рисунок 2.1 – Схема взаємозв'язку зовнішнього та внутрішнього аудиту [29]

Виділимо основні цілі, які реалізуються в процесі проведення аудиту інформаційної безпеки підприємства [30, с.1416]:

– аналіз ризиків, пов'язаних із можливістю здійснення загроз безпеки щодо ресурсів ІС;

– оцінювання поточного рівня захищеності функціонування мережі зв'язку та корпоративної інформаційної системи;

– оцінювання відповідності ІС нинішнім стандартам в сфері інформаційної безпеки і кібербезпеки;

– вироблення технічно коректних і економічно обґрунтованих рекомендацій щодо впровадження нових та підвищення ефективності наявних механізмів безпеки ІС і інформаційних активів компанії.

2.1.2 Проблеми та перспективи аудиту безпеки ІС в Україні

Розвиток сучасного стану економіки України має глобалізаційний напрям та відображає у собі складні процеси. Останнім часом наріжним каменем суперечок стали активні спроби України інтегруватися у світову спільноту економічного середовища. Виникнення світової фінансової кризи 2007–2009 роках в Україні істотно вплинуло на ряд економічних показників і національну економіку в цілому. Внаслідок цього, у багатьох юридичних осіб зросла ймовірність настання кризових явищ і ситуацій. Реальна загроза припинення виробництва зумовлює потребу пошуку нових шляхів удосконалення фінансової діяльності підприємства [31, с.324, 32, с.7].

Найважливішим інструментом задля покращення фінансового стану підприємства і подолання кризи є аудит безпеки, проте проведення даної форми фінансового контролю в умовах загального стану економіки України і війни — дуже складно під час значних цінових коливань валютного курсу і постійних зривів постачання товарів і послуг.

Незалежний початок розвитку аудиту інформаційної безпеки в Україні розпочався після проголошення незалежності України 24 серпня 1991 року. 22 квітня у 1993 році відбулося офіційне визнання обов’язкового аудиту у зв’язку з прийняттям Закону України “Про аудиторську діяльність”, який визначає правові засади відносно здійснення аудиторської діяльності в Україні і спрямований на створення незалежної системи фінансового контролю задля захисту інтересів власних користувачів фінансової та економічної інформації.

Окрім Закону України “Про аудиторську діяльність”, аудит безпеки регулюють Міжнародні стандарти контролю якості аудиту, огляду, іншого надання впевненості і окремих супутніх послуг, які діють в Україні від 18.04.2003 року [31, с.325]. Згідно створеного Закону України “Про аудиторську діяльність”, була створена аудиторська палата України (АПУ), яка

є незалежним самоврядним органом для забезпечення регулювання і вдосконалення аудиторської діяльності в Україні [33].

Однак, на жаль, аудит безпеки в Україні ще не набув належного поширення і широкого розмаху. Задля успішного розвитку аудиторської діяльності в Україні насамперед необхідно вирішити низку проблемних аспектів і недоліків з надання аудиторських послуг.

Основні проблеми розвитку аудиту в Україні [34, с.338]:

– недосконалість теоретичних і методичних основ контролю аудиторських послуг;

– недостатня кількість кваліфікованих спеціалістів;

– нестача необхідного досвіду для здійснення аудиторської діяльності;

– порушення аудиторами якості аудиторських послуг, які надаються суб’єктом аудиторської діяльності;

– відсутність цінової політики і механізму з надання аудиторських послуг;

– відсутність штрафів і покарань за недостовірну інформацію у звітах аудиторів;

– низький рівень довіри до аудитора;

– відсутність методичних вказівок щодо прикладних комп’ютерних програм з аудиту.

Одна із найголовніших проблем в аудиторській діяльності — недостатній контроль за якістю надання аудиторських послуг [31, с.326]. Відсутність релевантних умінь і навичок, знань і досвіду аудиторів, необхідних ресурсів, призводять до того, що аудиторські фірми не можуть у повній мірі якісно виконати завдання відповідно вимогам, встановленим Законом про аудит. Зневажливе ставлення аудиторів щодо підвищення обізнаності й удосконалення знань аудиторської діяльності породжує іншу проблему — стан ринку

аудиторських послуг в Україні підпорядковується головними суб'єктам, які виступають у ролі іноземних компаній. У список Великої четвірки аудиторських компаній, які надають консалтингові послуги, входять: Deloitte Touche Tohmatsu Limited (Deloitte, Лондон, Велика Британія), PricewaterhouseCoopers (PwC, Лондон, Англія), Ernst & Young Global Limited (EY, Лондон, Сполучене Королівство) і Klynveld Peat Marwick Goerdeler (KPMG, Амстелвен, Нідерланди). Найбільші аудиторські фірми світу використовують сучасні інноваційні методи та технології у своїй діяльності, що дозволяють їм змінювати форму ринку аудиторських послуг в Україні. Іноземні компанії є досить потужним конкурентом для українських аудиторських підприємств, проте єдине, у чому вітчизняні фірми можуть поступитися "Великій четвірці" — цінова політика послуг.

Розглянемо більш детально основні статистичні дані Реєстру аудиторів та суб'єктів аудиторської діяльності (САД) щодо кількості аудиторських фірм та приватних підприємств [31, с.327]. На кінець 2020 року в Україні налічувалось 2713 зареєстрованих аудиторів, з яких в аудиторських фірмах працювало 2153 фізичні особи. На рисунку 2.2. представлено період 2016-2020, під час якого спостерігається зменшення коефіцієнту щодо зареєстрованих аудиторів.

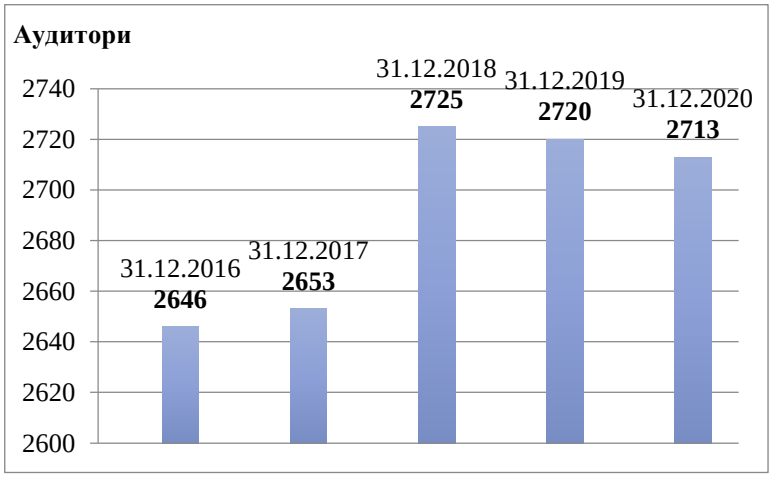

Рисунок 2.2 – Динаміка зареєстрованих аудиторів у період 2016-2020 років [35]

Практика свідчить про те, що станом на 31.12.2020 в Реєстрі аудиторів та суб'єктів аудиторської діяльності було 893 САД: 851 аудиторські фірми і 42 фізичних осіб-підприємців, які здійснюють свою діяльність у сфері аудиту. Перше місце за найбільшою кількістю зареєстрованих САД посідає місто Київ та Київська область — приблизно 433 аудиторських фірм та 17 фізичних осіб-підприємців. Харківська, Дніпропетровська та Одеська області посідають відповідно друге, третє та четверте місця за кількістю зареєстрованих аудиторських фірм і приватних підприємств. Найменшу кількість серед аудиторських організацій у розрізі регіонів займають Кіровоградська, Херсонська, Чернівецька, Луганська й Тернопільська області [35, с.4-6].

Порівняльні дані стосовно динаміки розвитку аудиторських фірм та приватних підприємств у розрізі регіонів за 2019-2020 роки представлено на рис. 2.3.

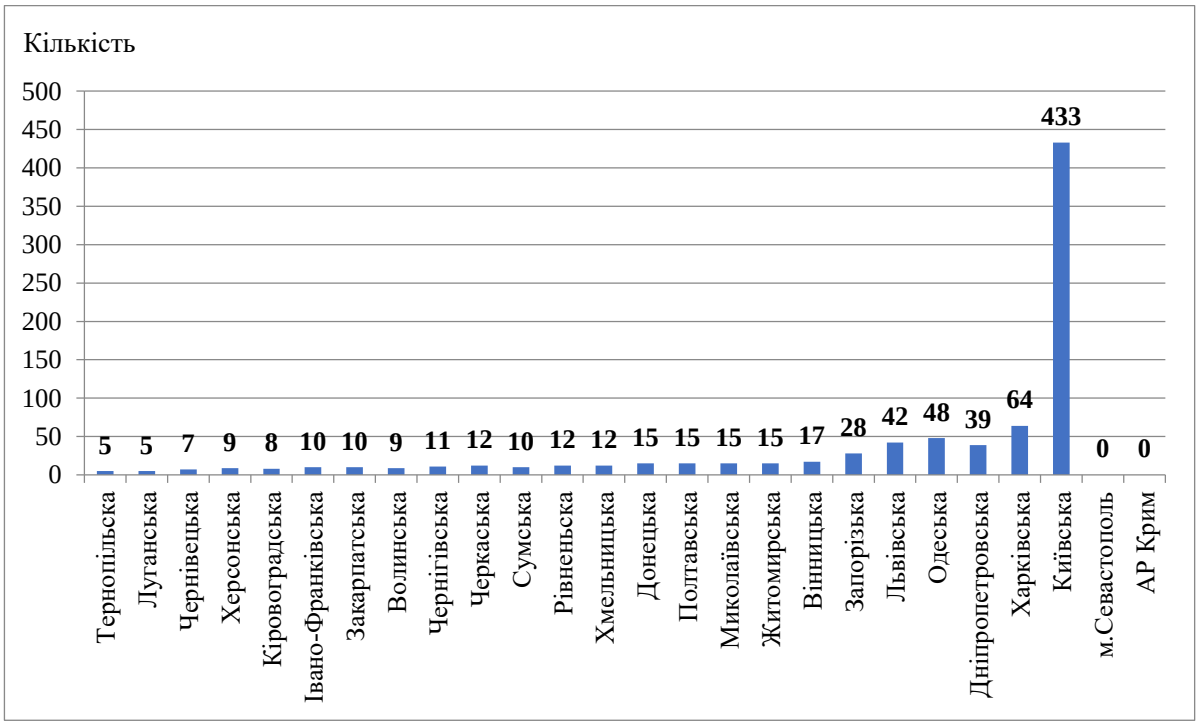

Рисунок 2.3 – Кількість аудиторських фірм у розрізі регіонів України [35]

Під час проведеного аналізу стану аудиторської діяльності в Україні можна дійти висновку, що лише 5% від усіх зареєстрованих організацій та

аудиторських фірм відповідають заданим критеріям для проведення якісного та ефективного аудиту.

Задля вирішення вищевказаних недоліків і основних проблем щодо організації та ведення аудиторської діяльності в Україні розглянемо різні шляхи удосконалення і розвитку аудиту, які сприяють підвищенню його ефективності [36, с.81-82, 37, с.45]:

– запровадження нової системи забезпечення і регулювання аудиторської діяльності;

– оформлення внутрішньо-фірмових нормативних документів аудиторської фірми, робочої документації і методичних рекомендацій з аудиторської діяльності;

– попереднє дослідження об’єкту контролю з метою подолання організаційних питань аудиторських фірм і систем якості аудиторських послуг;

– вдосконалення підготовки спеціалістів-обліковців у вищих навчальних закладах задля застосування знань до потреб практики у сфері проведення зовнішнього контролю якості;

– раціональний підхід щодо організації державного контролю за витрачанням бюджетних коштів;

– розробка і реалізація чіткого механізму формування цін на аудит та аудиторські послуги шляхом комплексного дослідження міжнародного досвіду;

– підвищення громадської оцінки суспільної вагомості професії аудитора.

Поліпшення аудиторської діяльності в Україні сприятиме не лише розвитку і вдосконаленню національному аудиту, а й держави загалом і в цілому завдяки змінам у бюджеті доходів і витрат ревізійного апарату державної контрольної служби адміністрування.

Детальний аналіз основних прогалин у питанні аудиторської діяльності надасть змогу [34, с.340]:

– економно використовувати державні кошти для забезпечення існування контрольно-ревізійного апарату;

– отримати додатковий дохід під час виявлення організацій аудиторських фірм, які приховують окремі економічні результати досліджень;

– уникнути випадків шахрайства і махінацій з метою приховування фактів про грошові махінації;

– здійснювати якісну перевірку з контролю якості наданих аудиторських послуг професіональними спеціалістами з аудиту.

Отже, стрімкий розвиток аудиту в Україні набирає широких обертів, проте водночас постає величезна кількість проблемних питань, які негативно впливають на загальний стан підприємства, стійкість і стабільність якої безпосередньо залежать від результатів діяльності фірми. Лише комплексний і системний підхід щодо усунення цих проблем стане основою для підвищення якості аудиторських послуг в Україні на міжнародному рівні.

2.2 Дослідження методів проведення аудиту інформаційної безпеки

Питання організації ефективної роботи в підприємстві безпосередньо залежить від належного формування проведення аудиторських перевірок [38, с.28]. Незалежно від часу, періоду й ситуації проведення аудиту старший спеціаліст-аудитор використовує всю сукупність необхідних методів для збору, оцінювання, перевірки й аналізу отриманих даних. Хоч заданий набір застосовуваних методів і процедур аудиту не має чіткої визначеності в аудиторських робочих документах, проте є одним із необхідних процесів для результативної перевірки.

2.2.1 Метод і методичні прийоми аудиту

Детально проаналізуємо й розкриємо визначення сутності поняття “метод”, який походить від грецького metodos і означає “шлях до чого-небудь”, “дослідження” [39, с.103].

У найбільш загальному розумінні метод для будь-якої науки — це прийом дослідження об’єктів пізнання (явищ, процесів, систем) за допомогою наукового пізнання до встановлення істини [38, с.28, 40, с.46].

Проблемам дослідження сутності основних прийомів і процедур аудиту присвячені численні праці провідних дослідників, проте переважна більшість спеціалістів з аудиторської діяльності за браком єдиного підходу й до сьогодення користується лише незначною кількістю наявних наукових методів. Під час огляду заданого питання виникає необхідність усестороннього й об’єктивного вивчення та науково-обґрунтованій класифікації необхідних для використання методів і методичних прийомів проведення аудиту.

Однією із найпоширеніших класифікацій методів аудиту є їхній безпосередній поділ на всезагальні, загальнонаукові та конкретно-наукові методи [40, с.46].

Всезагальний метод — це спосіб пізнання середовища, яке спирається на принцип матеріалістичного монізму, за якого різні типи буття або субстанції (світ, предмети і явища) зводяться до єдиної матеріальної основи [40, с.46]. Сутність методу полягає в тому, що всі конкретні об'єкти і процеси знаходяться у відносинах взаємозв'язку і взаємообумовленості між собою, якісні зміни супроводжуються докорінними змінами предмета або явища.

Застосування всезагального методу повинно враховуватися в разі вирішення пізнавальних і соціально-практичних проблем під час проведення фундаментальних досліджень.

Розвиток науки відбувається на основі застосування загальнонаукових методів здійснення внутрішнього аудиту, що зумовлює широкий спектр теоретичних прийомів і прикладних наукових досліджень, які звільнені від конкретного змісту пізнання [38, с.29, 40, с.46].

До загальнонаукових методів прийнято відносити:

– аналіз (від грец. analysis — "розклад") — це метод наукового дослідження, який передбачає вивчення об'єкта умовного або практичного поділу на поодинокі складові елементи (частини об'єкта, ознаки і властивості), де кожна складник досліджується окремо, але в межах єдиного цілого об'єкта [39, с.103, 40, с.46]. Основною умовою задля підвищення й підтримання рівня ефективності внутрішнього аудиту є володіння на високому рівні достатніми знаннями щодо методики економічного аналізу. Це дасть змогу зважено, комплексно й системно вивчати різні аспекти в механізмі фінансово-кредитного регулювання за допомогою аналізу та контролю показників економічного суб'єкта [41, с.72];

– синтез (від грец. synthesis — “з’єднання”, “сполучення”) — це метод у внутрішньому аудиту, який дає можливість поєднати й дослідити всі складники елементів об’єкту під час процесу аналізу частини, встановити взаємозв’язок між ними й розглянути предмет як єдину цілу структурну одиницю [40, с.46, 42, с.161];

– порівняння (від лат. similis — “подібний”) — це метод наукового пізнання, який є доцільним під час зіставлення й логічного аналізу предметів та явищ дійсності, а також знаходження спільного, притаманного, що може бути властивим двом або декільком об’єктам дослідження [39, с.104, 40, с.51]. Цей метод спрямований на виявлення суперечностей, факту відхилень від облікових даних під час проведення внутрішнього розслідування інцидентів корпоративного шахрайства, розкрадання та інших зловживань з боку спеціалістів із внутрішнього аудиту за отриманими результатами здійснення перевірки;

– індукцію (від лат. inductio — “наведення”) — це науковий метод, завдяки якому внутрішнім аудитором робляться загальні висновки про властивості великої кількості елементів з огляду на вивчені ознаки в деяких частинах даних елементів об’єкта перевірки методично за планом [40, с.47, 42, с.162];

– дедукцію (від лат. deductio — “низводжу”, “відводжу”) — це методичний прийом наукового пізнання під час якого об’єкт досліджується загалом і в цілому, водночас висновки внутрішнього аудиту про певний елемент із великої кількості здійснюється на основі підтверджених знань про властивості кількості відповідними розрахунками й деякими вибірковими перевірками складників частин об’єкту [39, с.103]. Дедуктивний метод дослідження застосовують для вивчення фінансово-господарської діяльності конкретної організації, оцінювання ефективності системи управління, у межах якої здійснюється дія об’єкту [40, с.47]. Його використовують також для оцінки

системи внутрішнього контролю, яка дає змогу встановити кількість необхідних виконуваних аудиторських процедур: чим більш надійною буде система внутрішнього контролю, тим меншу кількість аудиторських процедур може планувати висококваліфікований спеціаліст з аудиту. Процес наукового дослідження увесь час змінює своє положення від індуктивного до дедуктивного узагальнення і, у такий спосіб, продовжується нескінченно;

– абстрагування — (від лат. abstrahere — “відволікати”) — метод наукового пізнання, завдяки якому дослідник переходить від конкретних ознак об’єкта, відношень предметів і явищ до загальних понять, гіпотез і законів [40, с.45], під час якого відокремлюються другорядні властивості, які ускладнюють процес проведення обстеження;

– формалізацію — (від лат. formalis — “складений за формою”) — метод теоретичного дослідження об’єктів за допомогою віддзеркалення їхнього змісту і структури в примітній за якою-небудь знаково-символічною характерною ознакою за допомогою штучних мов. Цей метод забезпечує повноту огляду галузі досліджуваної проблеми, узагальненість підходу до їхнього розв’язання; однозначність символіки штучної мови надає однозначності розуміння й чіткості фіксації певних значень об’єктів пізнання [40, с.59];

– аналогію (від грец. analogia — “відповідність”, “схожість”) — це метод наукового дослідження, на основі якого досягається здобуття наукових знань про явища і процеси, які мають подібність з іншими об’єктами [40, с.48];

– моделювання (від лат. modulus — “міра”, “аналог”, “зразок”, “взірець”) — метод відтворення й розроблення спостереження з метою наукового вивчення об’єкту у взаємодії із зовнішнім середовищем. Під час застосування заданого методу, використовують мову структурно-функціонального моделювання, виключно діалектико-матеріалістичний підхід до аналізу явищ і об’єктів природи. Точність характеризується за допомогою

порівняння отриманого результату під час відтворення з прообразом основного об’єкта дослідження [42, с.145];

– конкретизацію (від лат. concretus — “густий”, “твердий”) — прийом дослідження стану об’єктів в усій їхній багатогранності, високоякісному об’єктивно-реальному різноманітті згідно з умовами існування та історичного процесу розвитку [42, с.161-162].

На відміну від загальнонаукових науково-практичні (спеціальні) методи є більш обмеженими і притаманні більшою мірою внутрішньому аудиту безпеки, до яких належать: усний запит, огляд, спостереження, обстеження, ревізія, інспектування, ведення аналітичної документації.

2.2.2 Методичні прийоми проведення і організації аудиторської перевірки

Досить часто в науково-довідковій літературі й навчальних джерелах поняття “метод” і “прийом” застосовуються як синоніми, у нашому випадку ці погляди прийнято вважати тотожними.

Попередньо здійснивши детальний огляд основної класифікації методів внутрішнього аудиту, детально розглянемо думку професора з обліку й аудиту інформаційної безпеки Немченко В.В щодо доречності класифікації методів внутрішнього аудиту на методичні прийоми проведення перевірки і її організації (рис.2.4) [43, с.39].

Спільно з розвитком людського суспільства і її історико-економічної науки в загальному обсязі поступово набирають обертів як методи проведення внутрішнього аудиту, так і його предмет дослідження.

Фактична перевірка дає змогу визначити кількісний і якісний стан досліджуваного об’єкта, який визначається шляхом способів перевірки фактичного стану активів.

До прийомів фактичного контролю науковець Немченко В.В. відносить: обстеження, опитування, обмірювання, перерахунок, зважування, сканування, експеримент, підтвердження, фактичний контроль стану активів та деякі інші [39, с.103, 43, с.48]. Детально розглянемо ті методи, які стосуються аудиту безпеки ІС.

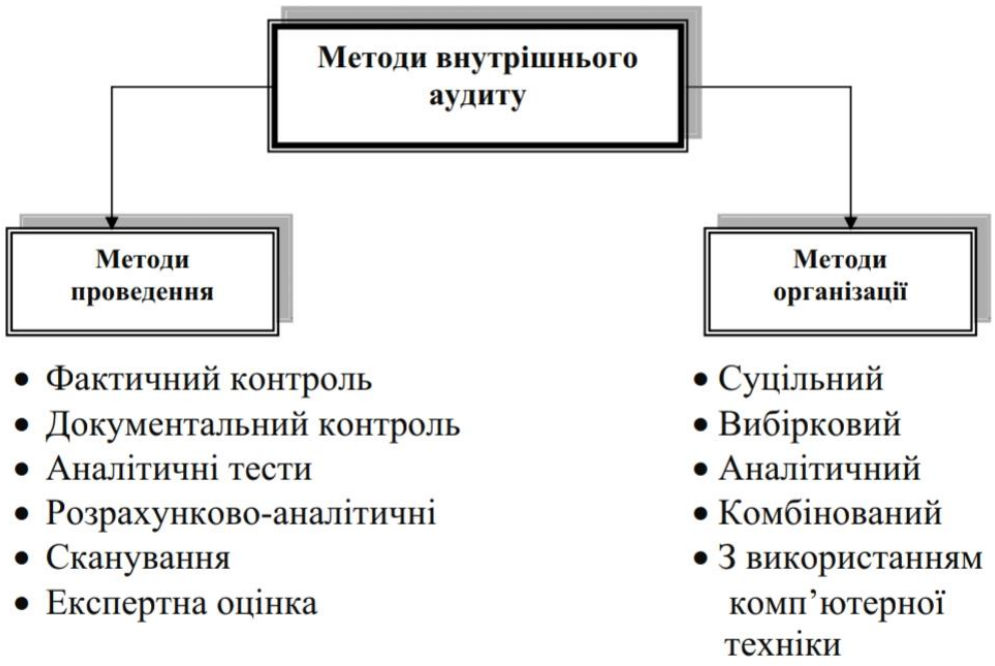

Рисунок 2.4 – Класифікація методів внутрішнього аудиту [43, с.40]

Обстеження — це метод безпосереднього вивчення й дослідження деяких об'єктів внутрішнього аудиту підприємства, що перевіряються. У результаті проведення заданого етапу внутрішній аудитор здобуває інформацію про те, на яких ділянках діяльності досліджуваного об'єкта аудиту безпеки становище несприятливе і становить загрозу в організаційно-виробничій діяльності [39, с.105, 43, с.41-42].

Опитування — це метод збору фактичної офіційної й неофіційної інформації та оцінних даних в усній і письмовій формі в повноправних осіб на початковій стадії перевірки аудитором задля проведення оцінки обсягів і ступеня складності робіт, які необхідно здійснити під час складання програми аудиту безпеки [40, с.54].

Документальний контроль — перевірка необхідних документів і записів за формою, змістом і суттю [43, с.44].

Аналітичні тести — це методи зіставлення між собою даних в абсолютних і відносних одиницях (індекси, коефіцієнти, проценти та інше) [43, с.46].

Розрахунково-аналітичні прийоми — це група штучних методів, які використовують економічно-математичний і статистичний аналіз розрахунків.

Сканування — це постійний і поелементний перегляд інформації з метою ознайомлення та перевірки її актуальності, відповідності зовнішнім і внутрішнім нормативних документам [39, с.106].

Метод експертної оцінки застосовуються для отримання змінних емпіричних даних під час перевірки документів, якості виконання обслуговування й робіт [39, с.106, 40, с.55]. Заданий метод проведення базується на окремих замовленнях фахівця сектору внутрішнього аудиту. Експерти різних галузей мусять надавати змістовну і ґрунтовну оцінку щодо діяльності об’єкта, яка залежить від попередньо наданих йому необхідних матеріалів і сформованих запитань. За результатами виконання експертної оцінки складається висновок із розгорнутими і правильно сформованими відповідями на запитання, які були поставлені внутрішнім аудитором.

У практиці аудиторської роботи виділяють основну групу прийомів організації перевірки, до якої належать: суцільна (документальна і фактична), вибіркова, аналітична й комбінована перевірка [43, с.47]. Деякі дослідники додатково виділяють методичний прийом організації, який включає в себе застосування комп’ютерного обладнання. Виділення заданого методу не є доречним, через те що за сучасних обставин не використання інформаційних технологій під час аудиторських перевірок не є можливим [44, с.138]. Актуальне програмне забезпечення виступає в ролі своєрідного інструменту і є невід’ємною частиною будь-якого процесу виконання того чи іншого методу;

дає змогу охопити більший обсяг вибірки, здійснити ефективний аналіз і провести додаткові самостійні процедури, узагальнити нормативну та законодавчу інформацію.

Під час суцільного способу організації відбувається перевірка всіх наявних масивів даних щодо процесів і явищ, які відбулись у клієнта під час періоду, який перевіряють [39, с.103, 43, с.40]. На підставі результатів суцільної перевірки аудитор робить висновок про достовірність, повноту й законність усіх операції і звітних даних за весь період, що підлягав перевірці. Характерні перевірки в процесі безперервного способу організації є найбільш точними, а ступінь ризику невиявлення помилок зводиться до мінімального. Головним недоліком заданого прийому є споживання великих трудових і матеріальних ресурсів. Суцільні перевірки застосовуються тільки в тих випадках, коли необхідно зібрати докази, завдані збитки й можливу шкоду в результаті встановлення факту правопорушення.

Вибірковий спосіб організації перевірки передбачає використання лише частини аудиторських процедур, що дає змогу аудитору отримати достатні докази і здійснити оцінку певних характеристик обраних даних на основі визначених документів, які підлягають перевірці [43, с.47]. Формування обсягу вибірки залежить від рівня довіри до системи внутрішнього контролю, мети проведення перевірки й сукупності отриманих даних.

Характерна вибірка повинна віддзеркалювати всі основні властивості множини однорідних об’єктів, які є головним предметом дослідження. Якщо під час проведення вибіркової дослідження певних процесів було встановлено серйозні факти порушень і помилок, то сукупність інформації повинна бути досліджена суцільним методом.

Аналітична перевірка передбачає собою оцінку фінансових показників за допомогою визначення ймовірних залежностей між ними на підставі даних звітності [43, с.47]. Аналітичний спосіб організації використовується для

формулювання тих чи інших подій розвиватися в певному напрямі, взаємозв’язків між економічними свідченнями і виявлення головних причин викривлень, обчислення економічних коефіцієнтів для здійснення оцінки фінансового стану. Визначення аналітичних процедур під час здійснення аналітичної перевірки розкривають динамічний аналіз показників у зіставленні з минулим виконуваним планом [39, с.105].

Зі свого боку комбінована перевірка виступає в поєднанні суцільної, вибіркової та аналітичної перевірки.

Отже, аудиторська перевірка — нелегкий і довготривалий процес, тому і виникає необхідність зменшити часовий проміжок виконання перевірок, не знижуючи якості й не збільшуючи виникнення потенційного аудиторського ризику. Передбачається застосування методики аудиту безпеки, під якою розуміють спосіб дослідження дій і подій у системі аудиторської перевірки та її організації для конкретизування об’єктивної істини.

2.3 Аналіз актуальної методики проведення аудиту інформаційної безпеки

За останнє десятиліття професія внутрішнього аудитора стала однією із найскладніших, з порівняно високим рівнем відповідальності та ціною помилки спеціальністю, яка стрімко розвивається через зумовлювання економічної поведінки суб'єктів господарювання. З появою високоякісних спеціалістів і нових фахівців у сфері аудиторських послуг в Україні, основне завдання яких полягає в підвищенні ефективності функціонування організації, існування образу ревізорів, які здійснюють перевірку діяльності закладу, поступово відходить на другий план.

На сучасному етапі розвитку економічної ситуації процес організації і здійснення аудиторської перевірки є нелегким і довгочасним, тому виникає необхідність у забезпеченні в скороченні максимальної тривалості робочого часу виконуваних перевірок, що впливають на рівень якості аудиторського ризику. Організація й методика аудиту передбачає сукупність взаємопов'язаних способів, прийомів і окремих методів аудиту з метою встановлення об'єктивної істини формування аудиту [39, с.102-103]

Насамперед необхідно чітко розрізняти між собою два поняття — метод і методика, оскільки останнє твердження більш ширше й визначає теорію про сукупність методів і технічних прийомів дослідження стану та поведінки об'єктів, натомість метод являє собою спосіб організації практичного або теоретичного освоєння дійсності.

Головною задачею з питань ІТ і безпеки є інформаційна підтримка основної діяльності організації.

Із кожним днем усе більше й більше проникнення інформаційних систем і технологій в усі сфери людської діяльності спричинили нагальність і

необхідність у вивченні інформаційного менеджменту, виділення найбільш ефективних методологій і створення стандартів у цій області.

Оцінка ризиків є однією із невід'ємних складових процесу впровадження в більшість стандартів. На відміну від законів та нормативних актів, які також потребують проведення оцінки ризиків під час побудови системи для забезпечення внутрішнього контролю безпеки, стандарти у сфері ІБ є більш оптимальним рішенням щодо виконання вимог законодавства. У зв'язку із широким різноманіттям стандартів забезпечення аудиту ІБ, організації нерідко стикаються з проблемою вибору найбільш оптимального та придатного для них нормативного документу [45, с.27]. Розглянемо детально один із найвідоміших стандартів у сфері забезпечення аудиту IT-безпеки — COBIT.

COBIT (Control Objectives for Information and Related Technology) — це система найкращих практик і процедур з управління IT, які допомагають організації досягти стратегічних цілей шляхом ефективного використання доступних ресурсів та мінімізації IT-ризиків.

COBIT надає комплексну та цілісну методологію, яка допомагає підприємству у вирішенні питань оптимізації керівництва й управління IT, аудитом IT та IT-безпекою. Методологія COBIT є досить універсальною й корисною для будь-якого підприємства, незалежно від розмірів і сфери діяльності деякої виробничої установи. Відкритий IT-стандарт допомагає підприємствам здобути оптимальну цінність від IT, при цьому належним чином підтримуючи баланс між реалізацією переваг та оптимізацією рівнів ризику і використанням ресурсів [46, с.13].

COBIT надає можливість керувати IT у рамках усього підприємства, враховуючи при цьому потреби та інтереси зацікавлених сторін, що причетні до проекту.

Зростаюча кількість нормативних документів та стандартів робить керівництво та управління корпоративними інформаційними технологіями (IT)

більш важливими. Ефективне управління IT стало одним із найважливіших питань для багатьох компаній. З цієї головної причини було розроблено велика кількість фреймворків, які реагують на потребу бізнесу, котрий постійно змінюється. У зв'язку із заснуванням міжнародної професійної асоціації аудиту та контролю інформаційних систем ISACA (Information Systems Audit and Control Association) у США в 1967 році, яка була орієнтована на IT управління, керівництво працювало разом задля розроблення і створення найкращих практик, однією з яких стала структура COBIT [47, с.68, 69].

Перше видання цього фреймворку було випущено в 1996 році, а у квітні 2012 року відбувся реліз поточної версії — COBIT 5.

Структура COBIT допомагає організаціям оптимізувати власні процеси управління IT дотримуючись при цьому договірних угод та нормативних і правових вимог. COBIT надає інструменти, які встановлюють і визначають пріоритети чітких і реалістичних IT-цілей. Наприклад, модель зрілості COBIT може допомогти користувачам оцінити необхідний рівень продуктивності для IT-елемента щодо виконання організаційного завдання.

Крім того, COBIT надає організаціям доступ до якісної інформації, яка стимулює прийняття оптимальних рішень і досягнення бізнес-цілей. Остання версія COBIT добре інтегрується з нинішними фреймворками, такими як ITIL (англ. Information Technology Infrastructure Library, бібліотека інфраструктури інформаційних технологій, яка відображає організацію компанії й надає послуги у сфері IT-технологій) і TOGAF (англ. The Open Group Architecture Framework, широко поширена інфраструктура програмних рішень для планування, проектування, впровадження і застосування архітектури IT підприємства), що дає змогу організаціям використовувати комбінацію інструментів відповідно конкретних завдань і практик.

COBIT складається з п’яти фундаментальних принципів (рис.2.5), які керують управлінням IT в організації і фактично забезпечують можливість щодо практичних дій із керівництва [46, с.13].

Розглянемо кожен із цих принципів детально.

Принцип 1. Відповідність вимогам зацікавлених сторін.

Підприємства існують для того, щоби створювати цінність для своїх внутрішніх та зовнішніх зацікавлених сторін за допомогою підтримання балансу між отриманням користі та оптимізацією ризиків і ресурсів. У COBIT 5 перелічені всі необхідні процеси та інші чинники впливу, які підтримують створення головних бізнес-цінностей завдяки IT [46, с.14]. Модель COBIT 5 можна модифікувати таким чином, щоб ці рекомендації відповідали конкретному контексту організації, так як задачі, котрі постають перед кожної організацією, суттєво відрізняються один від одного. Досягнення заданої задачі можливе завдяки каскаду цілей — перетворення високорівневих цілей підприємства до рівня керованих конкретних IT-цілей і пов’язаних із ними процесів і практик.

Рисунок 2.5 – Принципи COBIT 5

Принцип 2. Комплексний погляд на підприємство.

Розглядаючи підприємство комплексно як невід'ємну частину керівництва, методологія COBIT 5 описує всі функції і процеси задля керування та управління IT, котрі беруть свій початок на основі набору факторів впливу. Вони відносяться до всіх аспектів, які мають відношення до керівництва IT на підприємстві та є універсальними та застосовуваними на всіх етапах створення цінності [46, с.23].

Принцип 3. Застосування єдиної інтегрованої методології.

Єдину інтегровану методологію зручно використовувати для керівництва та управління IT. COBIT об'єднала в собі елементи сучасних стандартів ISO/IEC 27002, ISO/IEC 20000, ISO/IEC 15504 та інших зводів знань таких як ITIL, Val IT, RiskIT.

Використання заданого підходу дозволяє детальніше розглянути зв'язок між уже використовуваними на підприємстві стандартами, а також розвинення окремих компетенцій під час вирішення складних прикладних задач у сфері організації управління IT.

Принцип 4. Забезпечення цілісності підходу.

Задля забезпечення на підприємстві ефективного та раціонального керівництва та управління IT необхідне застосування у свої діяльності цілісності підходу з урахуванням багатьох взаємопов'язаних компонентів.

У COBIT 5 описаний цілий набір чинників впливу, які забезпечують використання системи керівництва та управління IT і сприяють вирішенню задач на підприємстві належним чином. Методологія COBIT 5 містить у собі сім чинників впливу (рис.2.6) [46, с.14, 27]:

1. Принципи, політики й підходи забезпечують перетворення бажаної поведінки в практичні рекомендації по оперативному керівництву підприємства.

2. Процеси описують організований та структурований набір практик і заходів для виконання певних задач, які забезпечують досягнення IT бізнес-цілей, які направлені на здобуття набору результатів.

3. Організаційна структура є однією із найважливіших складових для прийняття ключових рішень на підприємстві.

4. Культура, етика й поведінка людей і всього підприємства цілком і взагалі часто недооцінюється в якості окремої складової успішності керівництва та управління.

5. Інформація є ключовим продуктом і використовується в будь-якій організації задля праці та керування підприємства.

6. Послуги, інфраструктура й додатки забезпечують підприємство головними інструментами з обробки інформації.

7. Персонал, навички й компетенції потрібні для успішного виконання усіх видів діяльності, прийняття правильних та відповідних рішень, коригувальних дій.

Рисунок 2.6 – Чинники впливу на підприємстві відповідно COBIT 5

Принцип 5. Поділ керівництва та управління.

У методології COBIT 5 проведена чітка межа між керівництвом та управлінням. Ці складові включають у себе різноманітні види діяльності, вимагають організаційних структур та виконують певні цілі та завдання.

У розумінні COBIT 5, різниця між керівництвом та управлінням заключається в наступному: керівництво забезпечує досягнення головних бізнес-цілей підприємства шляхом оцінки потреб внутрішніх та зовнішніх зацікавлених сторін, існуючих умов та варіантів, постійного моніторингу фактичної відповідності і ступеню виконання вимог, які встановлені відносно напрямку й цілям підприємства; натомість управління полягає в плануванні, керуванні та контролюванні діяльності у відповідності напряму, визначеним органом керівництва для досягнення бізнес-цілей підприємства [46, с.14].

3 РОЗРОБКА МЕТОДИКИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА СТІЙКІСТЬ ДО АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Опис методики проведення аудиту інформаційної безпеки на стійкість до атак соціальної інженерії

Проведення комплексного IT-аудиту інформаційної безпеки для підприємства малого й середнього бізнесу повинен складатися з п’яти послідовних етапів:

1. Планування та ініціювання процедури аудиту.
2. Збір та документування інформації аудиту.
3. Аналіз отриманих даних аудиту.
4. Вироблення рекомендацій.
5. Підготовка аудиторських звітних документів.

На першому етапі відбувається ініціювання аудиту інформаційної безпеки керівництвом. Начальник служби безпеки призначає аудитора, чітко визначає й документально затверджує його права та обов’язки в посадових інструкціях, надає необхідне завдання і встановлює мету проведення аудиту інформаційної безпеки. Аудитор має володіти необхідними навичками в галузі забезпечення інформаційної безпеки задля виявлення й мінімізування ризиків та загроз, які виникають під час програми аудиту завдяки правильно обраним інструментам і методам аудиту [45, с.96, 48, с.58].

Спільно із замовником аудиту інформаційної безпеки розробляється регламент ладу проведення обстеження. Зазвичай регламент містить таку основну інформацію [18, с.88]:

– склад робочої групи для проведення аудиту інформаційної безпеки від виконавця й замовника;

– час і порядок проведення робіт;

– місце розташування об’єкта замовника аудиту інформаційної безпеки;

– перелік інформаційних і програмних ресурсів, які розглядаються у вигляді об’єктів захисту від потенційних загроз інформаційній безпеці.

Другий етап аудиту інформаційної безпеки підприємства, відповідно до узгодженого регламенту, полягає в зборі вихідних даних про поточний стан інформаційних технологій та є найбільш складним і тривалим процесом. Основна проблема в довготривалості процесу полягає в тому, що аудитор увесь час має взаємодіяти з багатьма посадовими особами організації. Задля успішного й ефективного проведення цього етапу необхідно використовувати основні методи одержання інформації: опитування, перевірки, анкетування, інтерв’ювання за напрямами, збір важливих відомостей щодо програмного й апаратного забезпечення.

Лише отримання повної, достовірної й точної інформації під час здійснення збору вихідних даних дає змогу провести якісний аудит інформаційної безпеки. Перелік необхідних вихідних даних для здійснення аудиту інформаційної безпеки для підприємства представлено на таблиці 3.1 [18, с.88-89, 49, с.43].

Детально розглянемо методи для збору вихідних даних [18, с.89]:

1. Інтерв’ювання співробітників замовника.

Головне завдання інтерв’ювання — дослідження поведінки і процесів системи шляхом використання опитувань персоналу організації з метою отримання і вивчення різних думок та ідей, які можна віднести до цілей аудиту. Задля отримання більш широкого бачення реальності важливим фактором серед інтерв’ювання є одержання різних позицій і точок зору співробітників замовника. Наприклад, отримання фактів та інформації від працівників на центральному й місцевому рівнях, співробітників внутрішніх і зовнішніх зацікавлених сторін тощо.

Таблиця 3.1 – Перелік вихідних даних, необхідних для аудиту безпеки

Тип інформації	Склад вихідних даних
Організаційно-розпорядча документація з питань інформаційної безпеки	– політика ІБ інформаційної системи; – нормативно-правова документація; – робота користувачів в ІС
Інформація про апаратне забезпечення хостів	– активне мережеве устаткування й обладнання; – периферійне обладнання та комплектуючі
Інформація про загальносистемне ПЗ	– відомості про встановлену робочу ОС на станціях і серверах, СУБД в ІС;
Інформація про прикладне ПЗ	– перелік встановленого прикладного ПЗ: загального та професійного (спеціального) призначення; – опис практичних завдань, які вирішуються прикладним ПЗ
Інформація про засоби захисту, що встановлені в ІС	– налаштування та конфігурація засобів; – схема комплексу встановлених засобів захисту
Інформація про топологію ІС	– карта функціонування локальної інформаційно-обчислювальної мережі; – типи каналів у системах зв’язку в ІС; – мережеві протоколи в ІС; – схема і класифікація інформаційних потоків

Результати інтерв'ювання мають чітко відповідати встановленим вимогам аналізу й контролю якості; повинні бути ретельно перевірені, перш ніж думки та свідчення будуть використані у визначенні аргументів та оцінці пропозицій.

Метод одержання даних про функціонування ІС шляхом інтерв'ювання представників замовника надає керівному складу компанії більш чітко зрозуміти вимоги, які висуваються до системи ІБ.

2. Заповнення опитувальних листів.

Опитувальний лист — це анкета, яка застосовується аудитором для попередньої оцінки стану об'єкта [50, с.12]. Використання даного методу для збору вихідних даних дозволяє суттєво зменшити час проведення аудиту інформаційної безпеки.

Основні правила складання опитувального листа для проведення аудиту інформаційної безпеки [50, с.12]:

– питання мають бути стислими, лаконічними і зрозумілими для опитуваних;

– питання можуть бути закриті (набір усіх можливих варіантів відповіді), напівзакриті (містять варіанти відповідей, проте можна внести власну відповідь) і відкриті (передбачають самостійну та розгорнуту відповідь респондента в довільній формі);

– послідовність формування питань цілком і в повній мірі залежить від поетапності проведення аудиту інформаційної безпеки;

– кількість питань не має перевищувати встановлений мінімум, проте має бути достатньою для оцінки стану об'єкта, що перевіряється.

Співробітниками замовника самостійно заповнюються опитувальні листи з конкретної тематики. У разі неповного викладення інформації на поставлені питання, відбувається додаткове інтерв'ювання співробітників замовника задля чіткості та зрозумілості відповідей.

3. Аналіз організаційно-розпорядчої та технічної документації.

За отриманими результатами наданого комплекту організаційно-розпорядчої та технічної документації формується програма й деякі методики проведення аудиту з урахуванням відповідних засобів і програмно-технічного забезпечення.

4. Використання спеціалізованих інструментальних засобів і ПЗ.

Дозволяють у повному обсязі отримати належну інформацію про склад та налаштування програмно-апаратного забезпечення ІС підприємства. Завдяки системам аналізу захищеності мережі можна виявляти різноманітні вразливості в мережевих ресурсах, аналізувати й надавати відповідні рекомендації щодо їх мінімізації [51, с.25-26]. До таких систем можемо віднести такі програмні засоби для аналізу захищеності ОС, як Microsoft Baseline Security Analyzer (MBSA), Internet Scanner компанії Internet Security Systems (ISS) і XSpider компанії Positive Technologies: програмний інструмент MBSA визначає стан безпеки підприємства шляхом оцінювання відсутніх оновлень безпеки в Microsoft Windows; платформа безпеки ISS для підприємств включає в себе оцінювання безпеки і віддалений моніторинг безпеки; сканер мережевого рівня XSpider виконує дистанційні перевірки вузлів мережі та дає змогу оцінити поточний стан захищеності IT-інфраструктури.

Під час третього етапу аналізу отриманих вихідних даних у процесі аудиту інформаційної безпеки відбувається систематизація здобутих результатів обстеження та ідентифікація виявлених вразливостей, виконується оцінювання поточного рівня захищеності інформаційної системи підприємства.

Використовувані аудиторами методи аналізу даних визначаються окремими специфічними підходами до проведення аудиту інформаційної безпеки, які можуть суттєво відрізнятися один від одного.

Одним із найскладніших підходів є аналіз ризиків. Завдяки проведенню даного етапу аудитором здійснюється оцінка реальних загроз порушення ІБ і

розробляються відповідні рекомендації та індивідуальний набір вимог безпеки для обстежуваної ІС задля мінімізування недоліків. У результаті розв'язання поставлених задач, отримана інформація виступає в ролі звіту про проведене обстеження.

Проведення аналізу ризиків дає змогу:

– здійснити своєчасну й об'єктивну оцінку наявних загроз;

– ідентифікувати та визначити пріоритети критичних ресурсів ІС;

– визначити вразливі місця, потенційні та реальні загрози;

– виділити основні вимоги щодо захисту конфіденційної інформації, яка регулюється законом;

– отримати експертну оцінку висновків і рекомендацій.

Під час аналізу ризиків відбувається:

– класифікацій інформаційних ресурсів;

– аналіз і оцінка вразливостей ІС;

– моделювання дій зовнішніх потенційних зловмисників;

– оцінка ризику ІБ [45, с.96-101].

Найбільш практичним є підхід, який за свою основу використовує стандарти інформаційної безпеки. Нормативні документи надають різні базові набори вимог щодо розробки та експлуатації ІС із питань керування ІБ і захисту даних від несанкціонованого доступу в залежності від рівня захищеності ІС. Головною задачею аудитора є коректне визначення відповідного набору вимог стандарту, виконання якого необхідно забезпечити для ІС. Відносна легкість і надійність даного підходу робить його більш поширеним у практичному застосуванні, так як він надає можливість робити доцільні висновки про стан ІС витрачаючи при цьому мінімальну кількість ресурсів.

Останній і найбільш ефективний підхід має на увазі комбінування двох попередніх. Основний базовий набір вимог безпеки щодо ІС визначається стандартом ІБ, додаткові — на основі безпосереднього аналізу ризиків.

За результатами проведеного аналізу отриманих даних стану ІС розробляються відповідні рекомендації щодо нейтралізації виявлених загроз і вразливостей інформаційної безпеки підприємства, вдосконалення системи захисту інформації. Рекомендації аудитора мають бути конкретними та детально аргументованими і відсортованими за ступенем важливості [48, с.60, 49, с.43].

На основі проведеного аудиту інформаційної безпеки формується аудиторський звіт, у якому міститься опис головних цілей проведення аудиту, характеристика досліджуваної інформаційної системи, результати аналізу отриманих даних аудиту інформаційної безпеки, конкретні висновки [30, с.1419], які узагальнюють їх та містять оцінювання ступеня вразливості інформаційних активів, мереж до можливих кібератак із метою крадіжки особливо чутливої й конфіденційної інформації. Крім того, аудитором надаються рекомендації з усунення наявних недоліків і вдосконаленню інформаційної системи захисту підприємства, підвищення рівня ефективності функціонування.

Необхідність проведення регулярного аудиту ІБ компанії дає змогу оцінити поточний стан захищеності ресурсів ІС та їх здатність протистояти постійно змінюваним зовнішнім і внутрішнім загрозам ІБ, а також відповідності ІС нормативним документам зі стандартизації.

3.2 Огляд інструментарію впровадження атак соціальної інженерії

На думку багатьох спеціалістів із безпеки ІС найуразливішим місцем у ланці будь-якої системи є людина, помилки якої можуть викликати негативні наслідки для організації [52, с.346].

Методи соціальної інженерії стали основою для розвинених сталих загроз підвищеної складності, які у свою чергу забезпечують швидкий доступ отримання несанкціонованого доступу до інформаційних систем і ресурсів жертви. Створення відповідних методів захисту від засобів соціальної інженерії не є простою задачею, проте яка потребує нагального вирішення.

Періодичність проведення аудиту безпеки ІС із застосування засобів соціальної інженерії дозволяє виявити слабкі місця політики ІБ підприємства і співробітників, проте заданий процес не є дешевою послугою для керівника організації, тому аж ніяк не кожна компанія може дозволити це собі.

Широкого застосування серед більшості організацій малого й середнього бізнесу отримав безкоштовний додаток Social-Engineer Toolkit (SET). Заданий програмний продукт надає змогу звичайному користувачеві здійснити прості атаки соціальної інженерії в автоматизованому режимі. Основні можливості даного за стосунку полягають у наступному:

– здійснення масової email атаки;
– виконання форматування файлу з навантаженням;
– застосування методів атак (метод експлойта для браузера Metasploit, метод атаки збору облікових даних, метод атаки з Java аплетом, метод множинних веб-атак та інші).

Функціонал сучасного і відносно легкого у використанні набору інструментів може бути використаний під час проведення зовнішнього або внутрішнього аудиту безпеки ІС у процесі тесту на проникнення, який орієнтований на створення і реалізацію потенційних векторів атак [52, с. 347].

Для запуску SET оберемо в основному меню пункти Applications – Exploitation Tools – Social Engineering Toolkit (Додатки – Інструменти експлуатації – Інструменти соціальної інженерії) або введемо в командному рядку терміналу команду: root@kali:~# setoolkit (рис. 3.1).

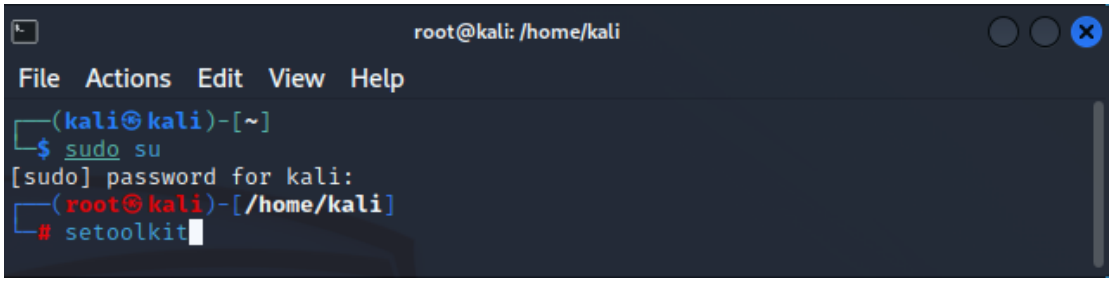

Рисунок 3.1 — Запуск утиліти SET

Утиліта SET успішно запущена, а в терміналі з'явився логотип, інформація та параметри, які можна застосувати під час запуску відповідних інструментів (рис.3.2).

Пункти головного меню утиліти SET:

1. Social-Engineering Attacks – Атаки соціальної інженерії
2. Fast-Track Penetration Testing – Прискорене тестування на проникнення
3. Third Party Modules – Сторонні модулі
4. Update the Social-Engineer Toolkit – Оновити набір для соціальної інженерії
5. Update SET configuration – Оновити конфігурацію SET
6. Help, Credits, and About – Допомога та інформація про програму
7. Exit the Social-Engineer Toolkit – Вихід із програми

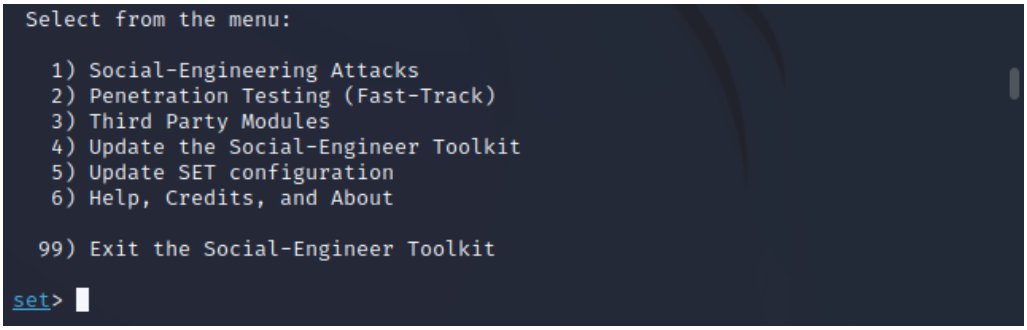

Рисунок 3.2 — Фреймворк SET успішно запущений

Детально розглянемо один із векторів потенційних атак — фішингову атаку задля збору облікових даних користувача.

Під час виконання цієї атаки створимо фейкову копію відомого нам сайту, яка дозволить нам отримати облікові дані користувача. Для того, щоби користувач міг відвідати сайт, необхідно надіслати посилання на нього через електронну пошту використовуючи заголовок чи тему, яка зацікавить потенційну жертву. Користувачу буде запропоновано увійти в систему і все — конфіденційні дані будуть отримані хакером.

1. Введемо команду setoolkit у головному меню й натиснемо пункт 1) Social Engineering Attacks (Атаки соціальної інженерії) (рис.3.3).

Рисунок 3.3 — Запуск утиліти SET і початок атаки соціальної інженерії

2. Для того, щоб обрати 2) Website Attack Vectors (Вектори атаки на сайт), введемо у командному рядку 2 (рис.3.4).

3. Задля отримання облікових даних введемо у командному рядку цифру 3 (рис.3.5-3.6)

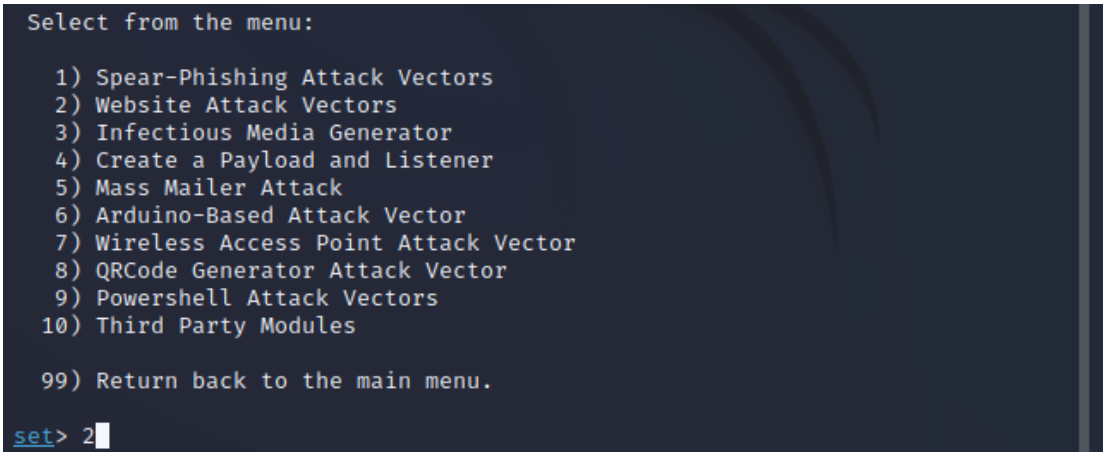

Рисунок 3.4 — Обираємо напрям атаки на сайт

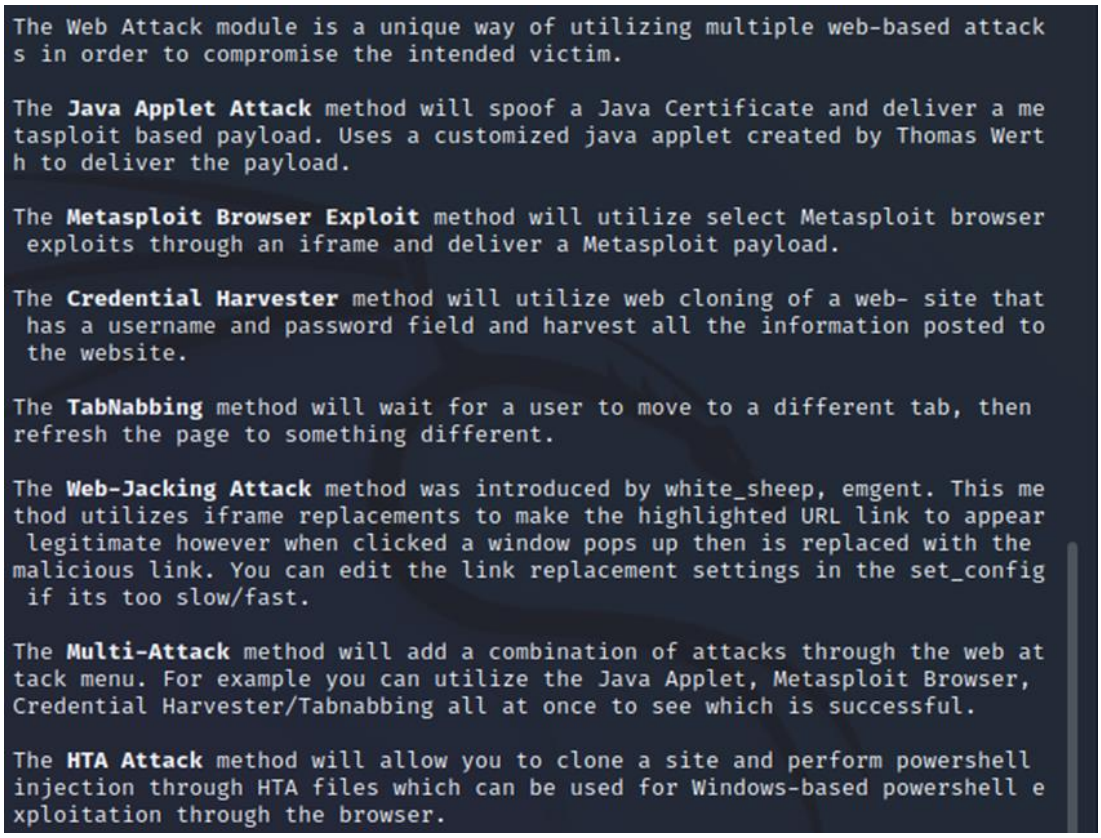

Рисунок 3.5 — Перелік веб-атак

У завантаженому модулі Credential Harvester Attack Method є три варіанти розвитку подій: використання веб-шаблонів, клонування сайту і

користувацький імпорт. Для нашого сценарію обираємо варіант 2) Site Cloner (Клонування сайту) (рис.3.7)

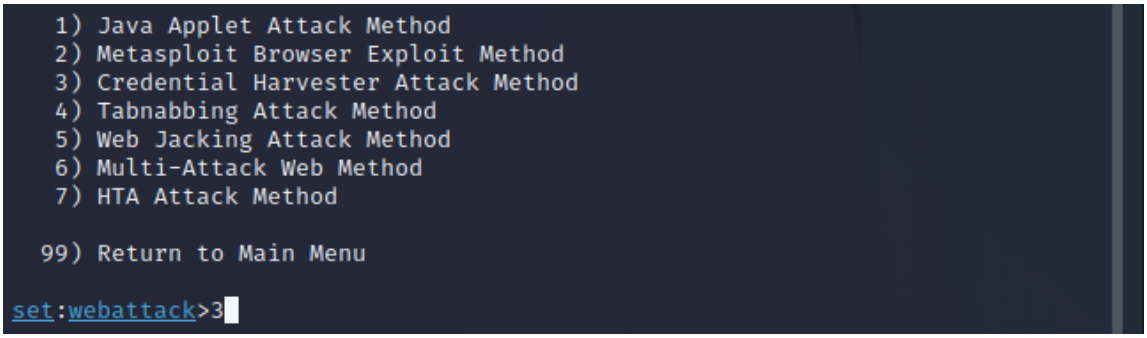

Рисунок 3.6 — Обираємо Credential Harvester Attack Method

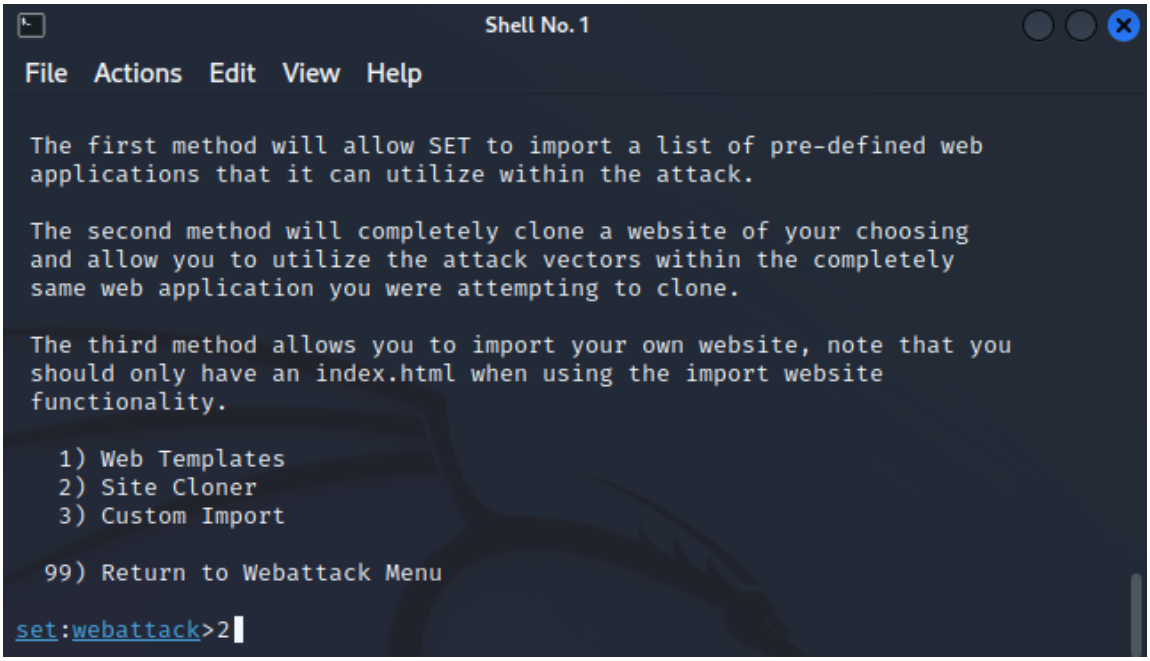

Рисунок 3.7 — Обираємо варіант використання веб-шаблонів

У першу чергу необхідно ввести IP-адресу, на якій буде розміщений сайт, тобто адрес комп'ютера, на якому знаходимось. Задля перевірки IP можна використати команду ifconfig в іншому терміналі, і ця адреса автоматично з'явиться у командному рядку (рис.3.8).

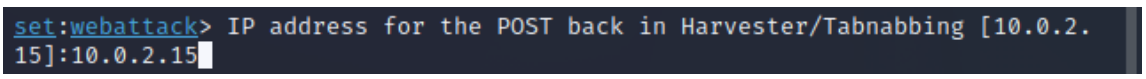

Рисунок 3.8 — IP-адреса тестової машини у командному рядку

IP-адреса тестової машини — 10.0.2.15. Після того, як IP-адреса буде введена, необхідно обрати сайт, який будемо використовувати для клонування.

У нашому випадку обираємо середовище змішаного навчання в СумДУ mix.sumdu.edu.ua і вхід на сайт (рис.3.9).

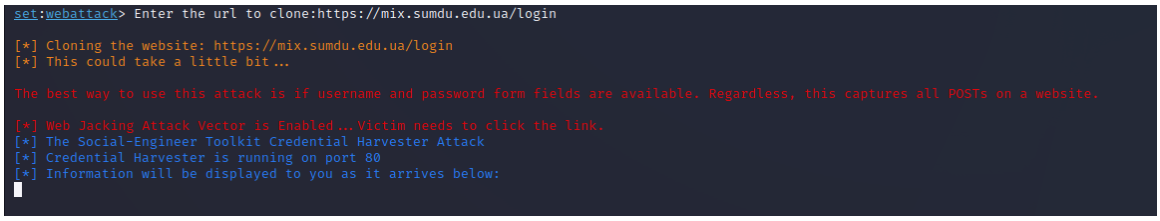

Рисунок 3.9 — Створюємо клон сайту

Для підтвердження створення клону сайту, виконаємо тест у браузері Kali перейшовши за IP-адресою 10.0.2.15 тестової машини (рис.3.10).

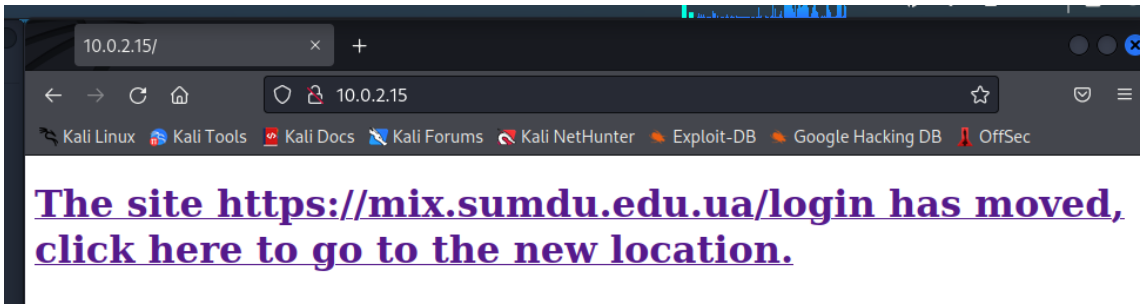

Рисунок 3.10 — Тест у браузері Kali за IP-адресою

Заносимо дані логіну та паролю для авторизації у системі MIX (рис.3.11).

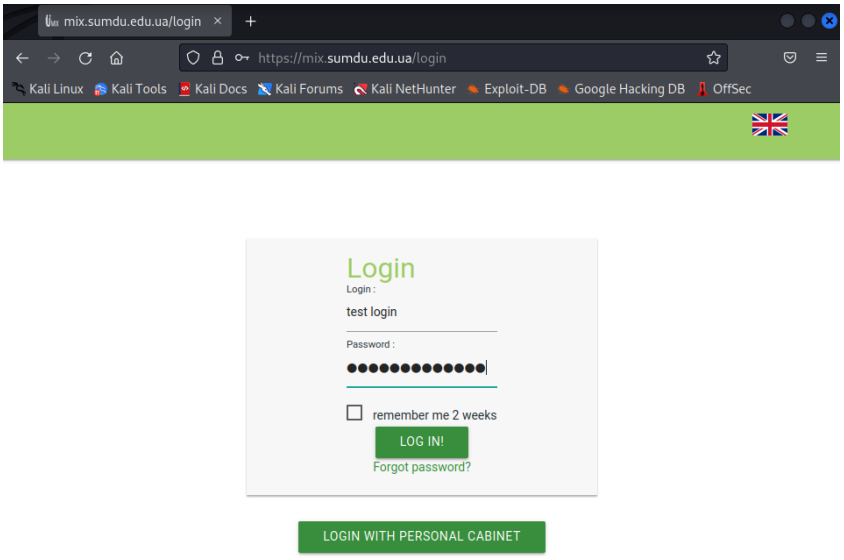

Рисунок 3.11 — Авторизація у системі MIX

Рисунок 3.12-3.13 свідчить про те, що конфіденційні дані для авторизації у системі MIX було успішно викрадено — SET відправляє адресу електронної пошти жертви і її пароль та заносить персональні відомості в .xml файл.

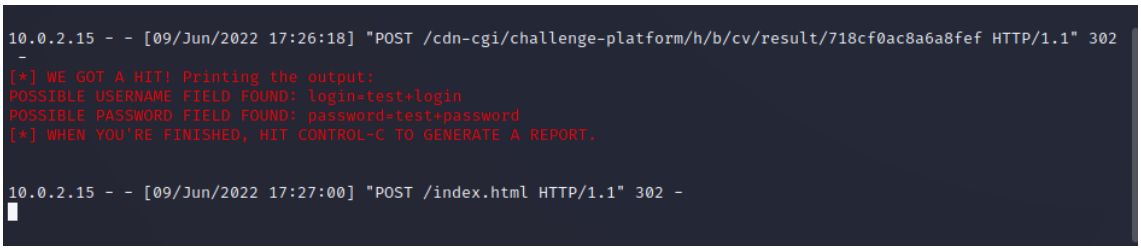

Рисунок 3.12 — Успішне виконання збору даних інструментом SET

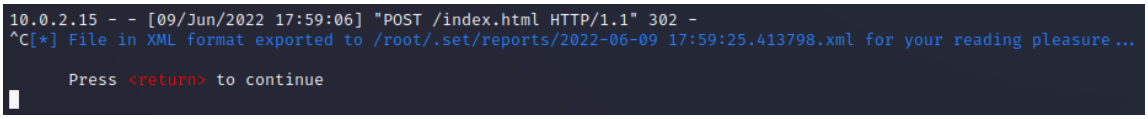

Рисунок 3.13 — Створення .xml файлу з обліковими даними потенційної жертви

Перевіримо наявність створеного .xml файлу з конфіденційними даними студента для входу в обліковий запис у системі MIX. Перш за все отримаємо привілегії користувача root задля отримання максимальних прав і можливостей працювати із системою. Введемо у командному рядку Kali Linux команду kali@kali:~ sudo su і змінимо поточний робочий каталог на той, де знаходиться файл з даними завдяки команді root@kali:~# cd (рис.3.14).

Рисунок 3.14 — Отримання привілегій користувача системи root і зміна поточного каталогу

Виведемо вміст каталогу і переглянемо інформацію щодо файлів. Для цього скористаємося командами ls (рис.3.15) і cat (рис.3.16) відповідно.

Рисунок 3.15 — Виведення вмісту каталогу на екран

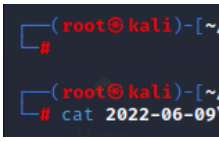

Рисунок 3.16 — Зчитування даних із файлу і виведення їх вмісту

Рисунок 3.17 свідчить про те, що конфіденційні дані потенційної жертви було успішно збережені до створеного .xml файлу. Збільшений варіант для зручності перегляду вмісту файлу зображено на рис.3.18.

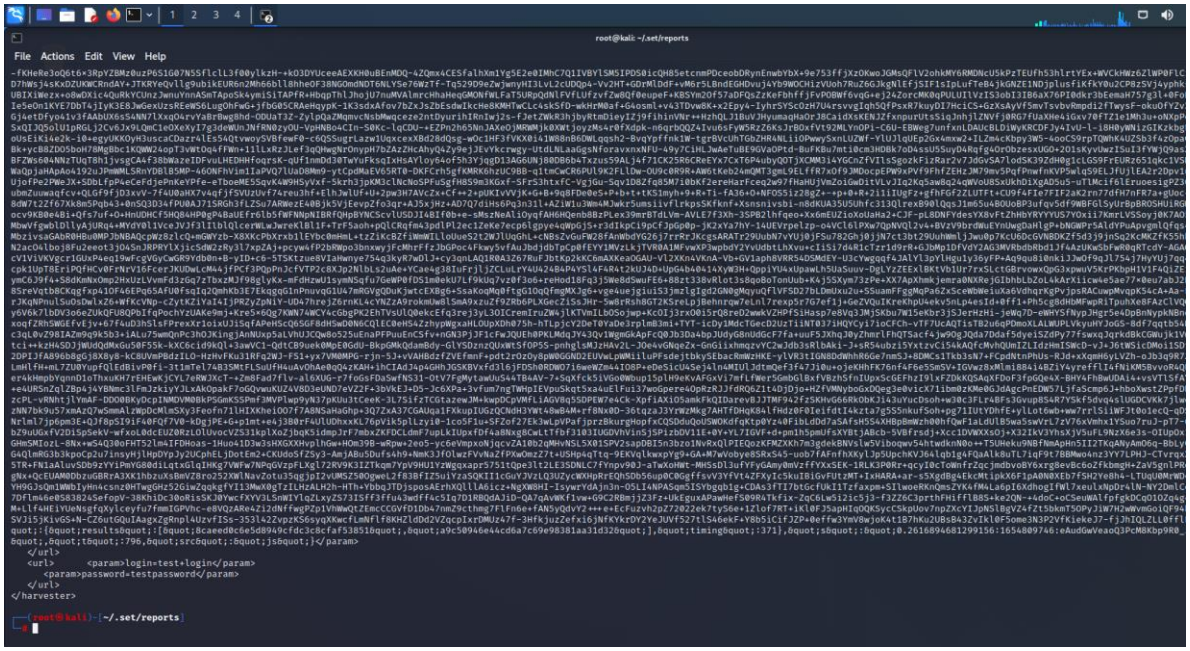

Рисунок 3.17 — Перегляд вмісту .xml файлу

Рисунок 3.18 — Персональні дані студента для входу в обліковий запис у системі MIX

ВИСНОВКИ

Аудит інформаційної безпеки дає змогу оцінити поточний стан захищеності ресурсів інформаційної системи та їх здатність протистояти постійно змінюваним зовнішнім і внутрішнім загрозам, а також відповідності нормативним документам зі стандартизації. Він проводиться з метою кількісної та якісної оцінки рівня захисту від ймовірних атак, а також може вирішувати досить широкий спектр запитань. Починаючи визначенням рівня системи безпеки й закінчуючи приведенням раніше створеної системи у відповідність до оновлених вимог, упорядкуванням і систематизацією нині існуючих заходів, спрямованих на забезпечення захисту. За допомогою нього можемо збирати, аналізувати інформацію стосовно системи, яку перевіряємо.

У процесі роботи було виокремлено загальну характеристику сучасних загроз для підприємств малого й середнього бізнесу, досліджено методи проведення атак із використання інструментів соціальної інженерії.

Детально розглянуто питання особливостей аудиту інформаційної безпеки для підприємств малого бізнесу, виділено методи проведення аудиту інформаційної безпеки та проаналізовано актуальні методики проведення аудиту інформаційної безпеки.

Розроблено методику й загальні принципи аудиту інформаційної системи підприємств на стійкість до атак методами соціальної інженерії з детальним описом послідовних етапів роботи під час проведення аудиту; здійснений огляд інструментарію Social-Engineer Toolkit задля впровадження атак соціальної інженерії.

СПИСОК ЛІТЕРАТУРИ

1. Скулиш Є. Д. Інформаційна безпека: нові виклики українському суспільству. Інформація і право. № 2 (5). 2012. С. 175–183.

2. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової безпеки України. Теорія та практика державного управління. №1 (48). 2015. С.1-5.

3. Глобальна та національна безпека: підручник / авт. кол.: В. І. Абрамов, Г. П. Ситник, В. Ф. Смолянюк; за заг. ред. Г. П. Ситника. Київ: НАДУ, 2016. 784 с.

4. Антонова С. Є. Інформаційна безпека / С. Є. Антонова, Г. Ф. Мартинюк. Державне управління: удосконалення та розвиток. 2019. № 11. С.7.

5. Hoffman Lance J. Modern methods for computer security and privacy. Englewood Cliffs: Prentice-Hall, 1977. p.268.

6. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. 2012. № 2. С.162-169.

7. Дзьобань О. П. Інформаційне насильство та безпека: світоглядноправові аспекти: монографія / О. П. Дзьобань, В. Г. Пилипчук; [за заг. ред. В. Г. Пилипчука]. Харків: Майдан, 2011. 244 с.

8. Баранов А. А. Концептуальні питання інформаційної безпеки України. Нормативно-правова база захисту: Зб-до матеріалів. К., 1997. С. 53-58.

9. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. Інформація і право. № 2(14). 2015. С. 111-120.

10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

11. Качан О.І. Інформаційна безпека підприємства в умовах глобалізації. Розвиток малого та середнього бізнесу в умовах глобалізації

світової економіки : матеріали виступів Всеукраїнського економічного форуму з міжнародною участю (в онлайн форматі) (27 квітня 2017 року). Житомир: ЖДТУ, 2017. 392 с.

12. Лаптєв М. С. Загрози економічній безпеці підприємств в сучасних умовах. Вчені записки університету «КРОК». Серія «Економіка». № 44. 2016. С. 111-116.

13. Шатковський М. О. Вплив соціальної інженерії на інформаційну безпеку організацій. К., НТУУ. «КПІ», 2015, с.4.

14. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. Національна безпека та оборона. № 1. 2001. С. 70-76.

15. Яковенко В. С., Казеян Н. К. Соціальна інженерія в Інтернет-просторі. Інформаційні технології та моделювання економічних процесів. Вип. III–IV(63–64). 2016. С. 119–126.

16. В. Мохор, О. Цуркан, В. Цуркан, та Р. Герасимов. Оцінювання захищеності інформації в комп'ютерних системах за соціоінженерним підходом, Selected Papers of the XVII International Scientific and Practical Conference «Information Technologies and Security». Київ, 2017. С.1-6.

17. Половенко Л. П., Мерінова С. В. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. Підприємництво та інновації. №10. 2019. 183-187.

18. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки − основа ефективного захисту підприємства. Кібербезпека: освіта, наука, техніка. №1. 2018. С. 86−93.

19. Кравчук Д. І. Аудит безпеки корпоративних інформаційних систем. Молодий вчений. №10, 2015, с. 697-700.

20. Варчук О. А., Амурова О. В., Крисенко А. В. Внутрішній та зовнішній аудит: відмінності. Одеський національний політехнічний університет, Одеса, 21-25 травня 2013. С.78-79.

21. Бутинець Ф. Ф. Аудит: підручник для студентів спеціальності «Облік і аудит» вищих навчальних закладів – 3-тє вид., доп. і перероб. – Житомир: ПП «Рута», 2006. – 512 с.

22. Кулаковська Л. П. Організація і методика аудиту : Навч. посібник/ Л.П. Кулаковська, Ю.В. Піча. К.: Каравела, 2004.- 568 с.

23. Назарова К. Сучасні тенденції трансформації внутрішнього аудиту. Вісник Київського національного торговельно-економічного університету. № 6. 2011. С. 94-101.

24. Потопальська Г. Г. Зовнішній та внутрішній аудит в Україні. Український соціум. №. 1. 2005. С. 6.

25. Савченко В. Я. Аудит: Навч.-метод. посібник для самост. вивч. / В. Я. Савченко, В. О. Зотов, С. А. Кириленко та ін. К.: КНЕУ, 2003. 268 с.

26. Спіцина Н. В., Кравцова С. В. Внутрішній аудит: підходи до визначення, відмінності від зовнішнього аудиту. Бізнес Інформ, № 5. 2020. С.342-348.

27. Шеремет А. Д., Суйц В. П. Аудит: Класичний університетський підручник. - 5-е вид., Перероб. та дод. - М.: ІНФРА-М, 2005. 448 с.

28. Чернелевський Л. М., Беренда Н. І. Аудит. Навч. посібник. — К.: Міленіум, 2002. 466 с.

29. Бондар М.І. Навч. посібник. — К.: КНЕУ, 2003. — 188 с.

30. Голубничий, Д. Ю., Коломійцев, О. В., Третяк, В. Ф., Рязанін, С. Г. Технології аудиту кібербезпеки інформаційних систем. Scientific Collection «InterConf», (36): with the Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26 - 28, 2020) in Washington, USA: EnDeavours Publisher, 2020. p. 333 – 342.

31. Соболєв В.М. Основні проблеми та перспективи розвитку аудиту в Україні / В.М. Соболєв, Т.Л. Слюніна, Т.В. Розіт // БізнесІнформ. №11. 2013. С. 324–328.

32. Бугай Н. О. Особливості аудиту підприємств-банкрутів: концептуальні методичні аспекти. Економічний дискус. Міжнародний науковий журнал. Випуск 4. 2017. С. 8–14.

33. Закон України “Про аудиторську діяльність” від 22.04.1993 № 3125-XII (Редакція станом на 01.10.2018) [Електронний ресурс] / Верховна Рада України – Режим доступу: https://zakon.rada.gov.ua/laws/show/3125-12

34. Платонова І. А. Проблеми та перспективи аудиту в Україні. Науковий вісник Полтавського університету економіки і торгівлі. № 4 (49). 2011. С.337-341.

35. Аудиторська палата України: орган аудиторського самоврядування [Електронний ресурс]. – Режим доступу: https://www.apu.com.ua/ (дата звернення 24.04.2022)

36. Дулачик О. І., Кушнір А. М., Мариняк О. О. Сучасний стан, проблеми та перспективи розвитку аудиту в Україні. Розвиток соціально-економічних систем в геоекономічному просторі: теорія, методологія, організація обліку та оподаткування. 2017, С. 81-82.

37. Мулик Я. І. Аудиторська діяльність в Україні: сучасний стан, реформування та розвиток. Агросвіт. № 7. 2020. С. 37–47.

38. Гончар І. І. Методичні прийоми і процедури в аудиті різних форм господарювання. Агросвіт. № 24. 2010. С. 28-31.

39. Кійко Ю. Т. Методичні прийоми і процедури проведення внутрішнього аудиту діяльності банку. Вісник Університету банківської справи. № 3 (30). 2017. С.102-110.

40. Каламбет С.В. Методологія наукових досліджень : навч. посіб. / С.В.Каламбет, С.В.Іванов, Ю.В.Півняк. Дніпропетровськ, 2015. 192 с.

41. Чепелюк Г. М. Методичні інструменти внутрішнього аудиту кредитної установи. Фінансовий простір. № 4. 2011.

42. Публічне управління та адміністрування: теоретичні та практичні аспекти: Навч. посібник / С. В. Панченко, О. Г. Дейнека, О. В. Дикань та ін. – Харків: УкрДУЗТ, 2019. 380 с.

43. Немченко В. В. Практичний курс внутрішнього аудиту : підручник / Немченко В. В., Хомутенко В. П., Хомутенко А. В. ; за ред. Немченко В. В. – К. : Центр учбової літератури, 2008. 240 с.

44. Гаркуша С. А. Комп'ютерний аудит в системі аналізу бухгалтерської інформації / С. А. Гаркуша, О. О. Довжик // Економічний аналіз : зб. наук. праць / Тернопільський національний економічний університет; редкол.: В. А. Дерій (голов. ред.) та ін. – Тернопіль : Видавничо-поліграфічний центр Тернопільського національного економічного університету «Економічна думка». Том 15. № 2. 2014. С. 136-141.

45. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О. Г., Гнатюк С. О., Казмірчук С. В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с.

46. ISACA, Rolling Meadows. COBIT 5: A business framework for the governance and management of enterprise IT. 2012. 94 c.

47. Pasquini Alex, Emidio Galiè. COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process.Proceedings of FIKUSZ 13. 2013. p. 67-76.

48. Хаджинова О. В., Куртяник М. С., Аудит інформаційної безпеки підприємства. Manager. Bulletin of Donetsk State University of Management, 90 (1), с. 53-63. 2021.

49. Проскуріна Н.М.. Аудиторські процедури при проведенні аудиту інформаційної безпеки підприємства : дис... к.е.н., доцент. Запоріжжя, 2010. С.40-44.

50. Посилкіна О. В., Світлична К. С. Розробка алгоритму проведення комбінованого аудиту в умовах побудови інтегрованої системи менеджменту

якості на фармацевтичних підприємствах. Управління, економіка та забезпечення якості в фармації. № 3. 2009. С. 9-15.

51. В. В. Яцків, І. З. Якіменко. Моніторинг мережевої безпеки : опорн. консп. лекцій / уклад. Тернопіль : ФО-П Шпак В. 2019. – 44 с.

52. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – Київ : Нац. акад. СБУ, 2018. 408 с.