ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія протидій соціальному інженеренгу в організації»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
(код, найменування спеціальності)
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Данило ДРОСЬ

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
ДРОСЬ Данило
(ПРІЗВИЩЕ, Ім’я)

Керівник: ГАЙДУР Галина
д.т.н, професор (ПРІЗВИЩЕ, Ім’я)

Рецензент:
(ПРІЗВИЩЕ, Ім’я)

Київ 2024

ЗМІСТ

ВСТУП 5

1. АНАЛІЗ ПРОБЛЕМИ ЗАСТОСУВАННЯ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ОРГАНІЗАЦІЯХ 7

1.1. Цілі соціальної інженерії в організації 7

1.2. Методи та типи атак соціальної інженерії 15

1.3. Аналіз загроз від соціальної інженерії в організації 19

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ОРГАНІЗАЦІЯХ 23

2.1. Методи атак реалізованих за допомогою соціальної інженерії 23

2.2. Засоби захисту від атак реалізованих за допомогою соціальної інженерії 27

3. РОЗРОБКА НАВЧАЛЬНОЇ СИСТЕМИ ПРОТИДІЇ АТАКАМ РЕАЛІЗОВАНИХ ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ОРГАНІЗАЦІЇ 32

3.1. Визначення актуальних загроз та уразливостей від атак реалізованих за допомогою соціальної інженерії 32

3.2. Огляд реалізації захисту від атак реалізованих за допомогою соціальної інженерії 61

3.3. Реалізація навчальної системи протидії атакам на основі методів соціальної інженерії 62

3.3.1. Реалізація інформаційно-довідкового блоку 62

3.3.2. Реалізація блоку тестування 63

3.3.3. Реалізація блоку контролю результатів тестування 73

3.4. Практичне застосування (тестування) навчальної системи для персоналу компанії..... 75

3.5. Аналіз результатів тестування, висновки 75

ВИСНОВКИ 76

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 80

ДОДАТКИ 83

ВСТУП

Актуальність теми. Нові інформаційні технології створюють новий інформаційний простір і відкривають абсолютно нові можливості, які докорінно змінюють уявлення про технології отримання та обробки інформації. Надаючи величезні можливості, інформаційні технології несуть в собі і небезпеку, великий набір можливих загроз, реалізація яких може призводити до непередбачуваних і навіть катастрофічних наслідків. Наприклад, збій в інформаційних технологіях, що застосовуються в управлінні атомними станціями або хімічними підприємствами можуть призвести до екологічних катастроф.

Крім того, сам факт використання інформаційних технологій, наприклад, в банківській сфері стає неможливим без організації відповідного рівня захищеності інформаційних ресурсів, що забезпечує конфіденційність, цілісність і доступність інформації.

Сучасний рівень розвитку обчислювальної техніки та засобів віддаленого доступу до неї надає значні можливості при організації зберігання і передачі інформації, розподіленої обробки даних, електронного документообігу, існування яких неможливе без забезпечення надійного захисту збереженої і переданої по мережі інформації.

Таким чином, захист інформації неможливий без організації відповідної захищеності комп’ютерного обладнання. Будь-яка сучасна комп’ютерна система складається з трьох складових компонентів: апаратна складова (Hardware), програмне забезпечення (Software) і людина (оператор, користувач, або фахівець, який обслуговує роботу системи). Для забезпечення захисту перших двох компонент відомо досить багато програмно-апаратних рішень і продуктів, що дозволяють забезпечити необхідний рівень безпеки, а ось третя компонента (людина), в силу своїх особливостей, є слабкою ланкою в системі захисту і забезпечення комп’ютерної безпеки системи в цілому.

Будь-яка автоматизована система (АІС), незалежно від характеру оброблюваної інформації, складається не тільки з програмно-технічних засобів і підтримуючої роботу АІС інфраструктури, а й з обслуговуючого персоналу і користувачів інформаційної системи. У цих умовах набули поширення хакерські атаки з використанням прийомів отримання необхідного (несанкціонованого) доступу до інформації, заснований на використанні слабкостей людського фактора. Набір таких прийомів і методів маніпулювання поведінкою людини отримав назву «соціальна інженерія». За даними статистики, серед вдалих зломів інформаційних систем 80% припадає на використання соціальної інженерії.

Таким чином, розробка і реалізація засобів захисту комп'ютерних систем від атак соціальних хакерів і соціальної інженерії є найактуальнішим завданням на сучасному етапі.

Метою даного дослідження є обґрунтування та аналіз технології протидій соціальному інженеренгу в організації.

Для вирішення поставленої задачі, в першому розділі кваліфікаційної роботи проведено аналіз теоретичних питань проблеми застосування атак соціальної інженерії на підприємстві. У другому розділі розглянуті поняття, методи, прийоми і способи захисту від атак методами соціальної інженерії. У третьому розділі розглянута розробка і реалізація навчальної системи протидії атакам методами соціальної інженерії. Висновок містить основні висновки, виявлені в ході проведення дослідження в рамках кваліфікаційної роботи магістра.

Структура та обсяг роботи. Дана робота складається з вступу, трьох розділів, які поділяються на підрозділи, висновків, списку використаних джерел. Загальний обсяг роботи становить 87 сторінок. Список використаних джерел налічує 26 найменувань.

1. АНАЛІЗ ПРОБЛЕМИ ЗАСТОСУВАННЯ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ОРГАНІЗАЦІЯХ

1.1. Цілі соціальної інженерії в організації

Соціальна інженерія на підприємстві це використання психологічних та соціальних методів для впливу на співробітників або клієнтів з метою досягнення певних цілей організації. Це може включати вплив на мотивацію співробітників, створення сприятливого робочого середовища, підвищення продуктивності або збільшення відвідуваності клієнтами. Соціальна інженерія може бути використана як у позитивних, так і у негативних цілях, тому важливо ретельно розглядати її методи та наслідки.

Організації можуть використовувати соціальну інженерію для досягнення різноманітних цілей, зокрема [16]:

– Збільшення продуктивності працівників. Організації можуть використовувати соціальну інженерію, щоб створити сприятливу робочу атмосферу, збільшити згуртованість команди та підвищити мотивацію працівників.

– Забезпечення безпеки організації. Часто соціальна інженерія використовується для зменшення ризиків, пов’язаних з конфіденційністю даних, фізичної безпеки та безпекою комп’ютерних мереж.

– Покращення взаємодії зі споживачами. Організації можуть використовувати соціальну інженерію, щоб залучити споживачів до своїх продуктів та послуг, підвищити лояльність споживачів та підвищити їх задоволеність.

– Збільшення прибутковості. Організації можуть використовувати соціальну інженерію, щоб залучати нових клієнтів, збільшувати обсяг продажів та підвищувати прибутковість.

– Побудова позитивного іміджу організації. Соціальна інженерія може бути використана для підвищення репутації організації, залучення

висококваліфікованих працівників та партнерів, а також для підвищення інтересу до організації в громадськості.

Питання розвитку засобів і методів організації захисту інформаційної безпеки в організації на сьогоднішній день знаходиться в центрі уваги розробників. Якщо провести аналіз інформаційної безпеки за останні п’ять років, то буде чітко видно зниження частки атак на програмно-апаратні компоненти комп’ютерних систем і зростання ролі атак з використанням технологій соціальної інженерії. Людина є слабкою ланкою в організації будь-якого захисту, зловмисник завжди може знайти людину в якійсь компанії, що має доступ до конфіденційної інформації, і запропонувавши цій людині солідну винагороду, може отримати доступ до цієї інформації [20].

Недбале ставлення співробітників організації, які повинні були сумлінно виконувати всі інструкції щодо дотримання збереження інформації, може надати шанс зловмисникам, які не мають при собі навіть простого технічного обладнання і без фінансових витрат безперешкодно і дуже легко пройти загороджувальний рівень безпеки.

Наслідки цих дій насправді можуть бути жахливими. Можна навести безліч прикладів зараження вірусами, наприклад, WannaCry і PetyaA, що призвели до величезних втрат, або хвиля з зараженням вірусом шифрувальником, що пройшлася по всьому світу, зупиняючи роботу найбільших світових компаній і навіть простих користувачів. Цей вірус не оминув і Україну. Жертвами атак стали великі вітчизняні компанії, які зазнали колосальних збитків безпосередньо в економічному плані [25].

Щоб ефективно відбивати або боротися з загрозами, їх необхідно постійно вивчати і дуже добре розбиратися в них. Фахівцями інформаційної компанії було проведено опитування щодо дослідження різних загроз інформаційній безпеці. Серед аудиторії в 5150 осіб опитаних були і фахівці з інформаційної безпеки та системні адміністратори і навіть керівники всіх рівнів, які знають проблеми інформаційної безпеки не з чуток. Розглянемо результати даного опитування. Найбільш високий відсоток за результатами

опитування отримала внутрішня погроза – 92,63%, це якісь події, що відбувалися всередині компаній, крім того в багатьох організаціях реально відбувалася якась витік відомостей, тому дана загроза за результатами досліджень показала найвищий відсоток. Інакше кажучи, виходячи з відсотків опитування менше 10% або тільки одна організація з 10 не зможе потрапити в руки зловмисників. Також в ході дослідження стало зрозуміло, що в 55,23% випадках витік інформації є спеціально спланованим співробітниками компанії для вилучення і отримання вигоди. Співробітники компаній здійснюють протиправні діяння через те, щоб розбагатіти, продавши інформацію конкурентам, або зрозуміти структуру бізнесу і відкрити свою власну справу. Також недбала поведінка співробітників компаній, яка порушує всі принципи безпеки пересилання документації не на потрібний адресат, відправка логінів і паролів стороннім і багато іншого зайняла близько 24% витоків [3].

Тільки через співробітників, що мають конфіденційний доступ до інформаційних баз, які викрадають різного роду інформацію, різні комерційні організації втрачають свою фінансову вигоду, а також різні патенти на своє виробництво і комерційну перспективу в 62% ситуацій. У 37,3% випадках працівники починають збирати інформацію з метою подальшого її використання. Приблизно знаходяться в одному строю і ті співробітники які готові продати різні відомості конкурентам, таких близько 37,1%. Але і є такі, які намагаються примножити свій дохід за рахунок фінансів організації, де вони трудяться, їх близько 26,3% [27].

Дане дослідження визначила, що відповідальними за витоки інформаційних даних виявилися 25,3% співробітників відділу продажів, 24% – провідні спеціалісти; 22% – менеджери; 12% – тимчасові співробітники; 8% – системні адміністратори; 4% – секретарі; 2% – бухгалтерія; 4% – інші співробітники. Отже, 60% з найбільш актуальних загроз – це внутрішні, коли співробітники крадуть інформацію і користуються їй для свого особистого збагачення. Працівники будь-яких організацій можуть безперешкодно

отримати і скористатися будь-якою цінною інформацією в своїх інтересах. 33,4% опитаних висловилися, що не варто забувати про недбалість співробітників, які необдумано сприяли витоку інформації. І тільки 7% бояться шкідливих наслідків від хакерів.

Спеціалісти називають три причини, які змушують співробітників компанії зробити розкрадання інформації (рис. 1.1):

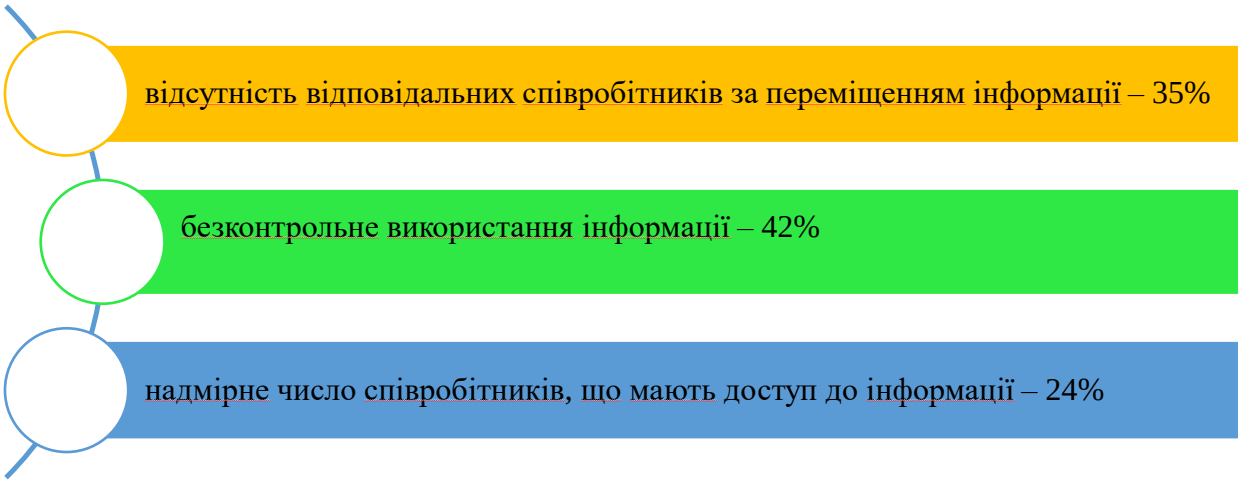

Рис. 1.1. Причини, які змушують співробітників компанії розкрадати інформацію

Джерело: розроблено автором

Також наведемо список найбільш затребуваної інформації зловмисниками (рис. 1.2):

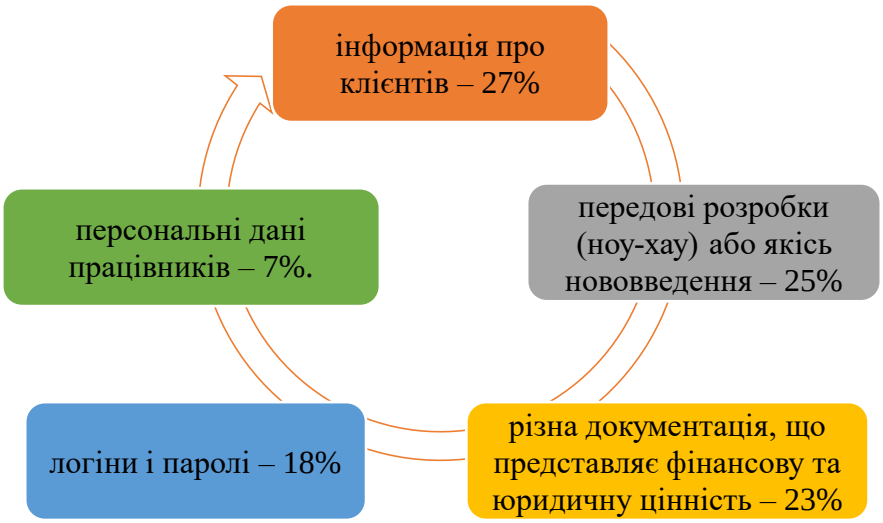

Рис. 1.2. Список найбільш затребуваної інформації зловмисниками

Джерело: розроблено автором

Як правило повністю довіряють своїм співробітникам тільки 11% керівників компаній. При цьому, постійні навчання з інформаційної безпеки проводяться в 52% випадків, а в 78% випадків співробітники організацій інструктуються під підпис і несуть особисту відповідальність за збереження відомостей. Тому співробітники, які мають доступ до конфіденційної інформації, можуть стати реальною загрозою для інформаційної та фінансової безпеки компанії [14].

Таким чином, зовнішня загроза, пов'язана з людським фактором, залишається вельми актуальною і вимагає постійного захисту інформації. Насправді, віруси-шифровальщики на сьогоднішній день, не так актуальні, тому що вони ще недостатньо поширені, хоча їх загрози можуть і будуть зростати щороку. І багато хто вже стикаються з цією загрозою. Але якщо взяти «фітинг», то він на відміну від хакерських атак на сьогоднішній день продовжує набирати обертів. І напевно багато хто з цим вже зіштовхуватися.

Основна маса співробітників з великою відповідальністю підходять до оновлення кодів доступу до інформаційних баз даних, логінів і акаунтів [22]:

- 11% обов'язково змінюють свої логіни і паролі кілька разів на місяць;
- 29% обов'язково змінюють не рідше одного разу на місяць;
- 25,1% змінюють один раз на квартал;
- 14% змінюють один раз на півроку;
- 7% ігнорують виконання даних заходів.

Постійне вивчення і систематичний контроль за своїми співробітниками проводять лише 71% опитаних, а ось контроль за обміном цінної інформації роблять лише 36%. Тому в багатьох компаніях захист засобів інформації або інформаційна безпека знаходиться не на досить високому рівні. Різні компанії просто вважають, що у них є антивірус і цього достатньо, щоб захиститься від різного роду загроз.

Отже, наразі дуже гостро стоїть питання створення інформаційно-довідкової системи або системи підвищення безпеки інформації в організації.

При забезпеченні інформаційної безпеки в організації вирішуються наступні завдання (рис. 1.3):

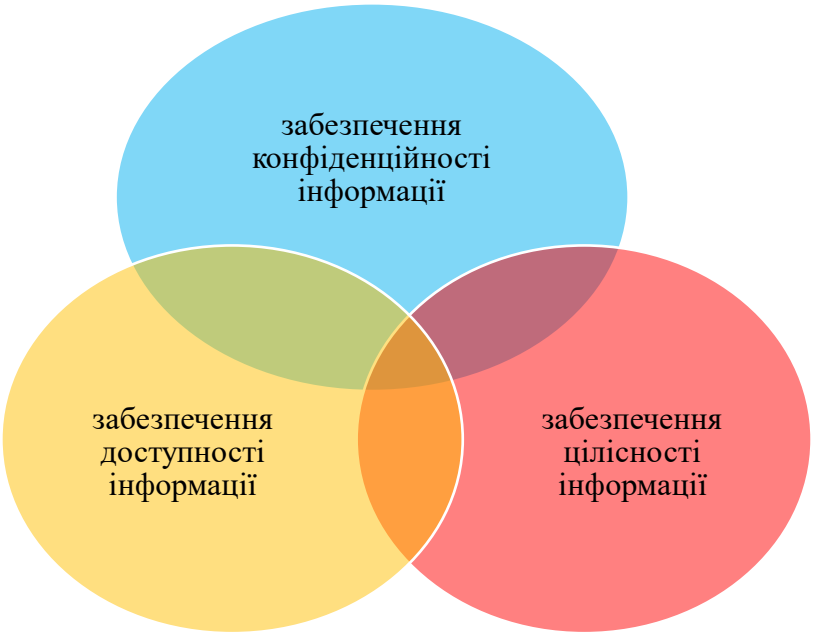

Рис. 1.3. Завдання інформаційної безпеки в організації

Джерело: розроблено автором

Поняття інформаційної безпеки можна визначити як захист різного роду відомостей і різних видів даних від незаконного розгляду або використання в своїх цілях третіми особами, а також можливого пошкодження даних відомостей і відправки шкідливого програмного забезпечення. Також інформаційна безпека має на увазі надійний захист будь-якого роду відомостей від дій, що призводять до її не узгодженого поширення. Впливи, яким піддаються погано захищені інформаційні дані різних структур визначаються наступним чином: інформаційна безпека (information security): має на увазі всі аспекти, пов’язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності, невідмовності, підзвітності, автентичності та достовірності інформації або засобів її обробки [21].

Впливи на слабозахищені інформаційні ресурси з боку деяких зовнішніх загроз можуть бути фатальними. Прикладами таких впливів можуть бути [21]:

– зломи зловмисників або порушників, які можуть так само використовувати і шкідливе програмне забезпечення і використовувати соціальну інженерію;

– виведення з ладу різної програмної техніки, необхідної для роботи, по причини різного роду вразливостей;

– можливі помилки, які може допустити персонал, при роботі з комп'ютерними системами будь-яких компаній;

– всілякі природні катаклізми, наприклад, пожежі, землетруси, несприятливі стани атмосфери, різні перешкоди, сторонні сигнали або шуми.

Інформаційну безпеку можна забезпечувати і підтримувати на достатньо високому рівні, але незважаючи на введення всіх захисних заходів, як правило залишаються слабкі місця. Але за умови виконання різного роду заходів, що забезпечують не тільки наприклад нерозголошення інформаційних даних і їх цілісності, а також збереження достовірності інформаційних даних, не тільки особами, що відповідають за безпеку, але і всіма співробітниками певної організації.

Гарантія інформаційної безпеки різних інформаційних даних, можлива лише при дотриманні всіх вимог і правил, пропонованих до забезпечення захисту. При забезпеченні інформаційної безпеки вирішуються наступні завдання [10]:

1) забезпечення конфіденційності інформації;

2) забезпечення цілісності інформації;

3) забезпечення доступності інформації.

Конфіденційність передбачає забезпечення доступу до інформації тільки санкціонованих користувачів відповідно до рольовим доступом.

Забезпечення цілісності даних – поняття, що визначає незмінність інформації, її зміни допускаються відповідним правомірним чином працівниками з відповідними правами. Наприклад: в екзаменаційну відомість – в інформаційній системі факультету має право вносити інформацію тільки викладач. Отже, «зберегти цілісність» означає не

допустити ніякі зміни інформації, крім дозволених способів. Крім того, повинні бути засоби, що дозволяють виявити і припинити всі неправомірні зміни.

Доступність інформації виражається в можливості доступу до інформації певному колу осіб з відповідним рольовим доступом. Таким чином доступність означає можливість ознайомлення з будь-якими відомостями відповідно до прав. Такий вид доступу називається санкціонованим, при порушенні порядку доступу говорять про несанкціонований доступ, який відноситься до порушення інформаційної безпеки.

Спільно з основними поставленими завданнями інформаційної безпеки існують і інші важливі завдання, до яких можна віднести забезпечення достовірності, забезпечення невідмовності, забезпечення підзвітності та автентичності.

Крім завдань інформаційної безпеки існують і загрози інформаційної безпеки, які можуть призвести до порушення інформаційної безпеки. Загрози завжди використовують слабкі місця в захисті інформаційної системи, які називають вразливістю. Вразливості виявляються при проведенні аналізу системи інформаційної безпеки компанії.

Загрози розрізняють по ряду ознак [18]:

– за метою впливу – здатність загрози пошкодити або знищити інформації:

– по об’єкту атаки – об’єктом атаки може бути структура системи, де знаходиться інформація, дані, програмне забезпечення, будь-яке обладнання, яке підтримує комп’ютерну систему;

– наявність людського фактору – людина може допускати помилки, що призводять до порушення інформаційної безпеки (як випадкові, так і не випадкові);

– природні стихійні фактори.

Для запобігання загрози необхідно точно визначити джерело небезпеки в самій системі або за межами інформаційної системи.

Основний принцип або метод захисту інформації повинен бути комплексним. Даний принцип здатний об’єднати різні системні процеси, для виявлення і запобігання різного роду загроз інформаційної безпеки.

Основою інформаційної безпеки є законодавчі та нормативні документи. Будь-які дії, пов’язані з інформаційною безпекою, зобов’язані виконуватися в рамках закону. Передбачені законодавством акти показують своє ставлення до зловмисників, які намагаються завдати шкоди інформаційній безпеці компаній.

1.2. Методи та типи атак соціальної інженерії

Соціальна інженерія, як часом її називають мистецтвом злому людського свідомості, останнім часом набула високу популярність у зв’язку з підвищенням ролі соціальних мереж, електронної пошти, інформаційних технологій, поширенням мобільних пристроїв онлайн-комунікацій в нашому житті. У сфері інформаційної безпеки даний термін широко використовується для позначення цілого ряду технік і прийомів, використовуваних кіберзлочинцями. Аналіз успішно проведених шахрайських атак дозволяє зробити висновок, що слабкою ланкою в організації захисту інформаційних систем і ресурсів є не уразливості апаратних або програмних засобів, а сама людина. Більшість атак соціальних інженерів засновані на особливостях прийняття людьми рішень і використовуються шахраями в різних комбінаціях для створення найбільш підходящої стратегії обману в кожному конкретному випадку. У зв’язку з цим для фахівців в області захисту інформації підкреслюється необхідність надбання знань в області загальної та прикладної соціології та психології для здійснення комплексного інженерного підходу до організації інформаційної безпеки підприємства з урахуванням соціальної реальності [16].

Потрібно розуміти, що соціальна інженерія використовує як правило нетехнічні загрози безпеці. Всілякий набір використовуваних загроз вимагає

обов’язкового ознайомлення і інформування про них. Крім того, необхідно обов’язкове навчання користувачів різного рівня, починаючи від керівництва компаній, а також включаючи технічний персонал, службу безпеки і т.д.

В 2022 році найбільший відсоток склали різні хитрощі соціальної інженерії незважаючи на те, що багато користувачів, почувши слово «кібербезпека», починають думати про троянського хробака, хакерів і як від них захиститися. При цьому геть забуваючи, про різні людські слабкості, довірливість і нарешті простий обман, не кажучи про жадібність, страхи, співчуття тощо. Незважаючи на те, на сьогоднішній день для забезпечення інформаційної безпеки використовується досить професійна система захисту, крім цього фахівцями на комп’ютерну техніку встановлюються брандмауери, крім цього різні системи виявлення та запобігання вторгнень в комплексі з антивірусними програмами аналізують мережі, досить чітко прописуються протоколи, різні сигнатури антивірусних програм, які сприяють високому ступеню захисту інформаційної безпеки від деяких зовнішніх загроз, використовується надійне програмне забезпечення. Але завжди бувають слабкі місця [13].

Соціальна інженерія – це різні способи і методи маніпуляції людьми з метою отримання якоїсь інформації, що може зацікавити шахраїв або зловмисників, з використанням знань людського стану або психіки. Основним завданням зловмисників буде отримання доступу до інформації, використовуючи не програми злому, а довірливість людей, користувачів, як правило різних сервісів [26].

Соціальна інженерія залежить, як правило, від різних особливостей або закономірностей людської психології, яку дуже добре знають зловмисники і нею користуються. Іноді соціальну інженерію називають психологічними прийомами для людини. Різні методи соціальної інженерії можуть бути і цілком законні, з урахуванням законодавства.

Всі загрози з метою отримання якоїсь конфіденційної інформації від потрібного для зловмисника користувача і націлені на певну людину за

допомогою різних способів і методів соціальної інженерії, можна розділити на кілька груп. Загрози, які виходять від шахрая, що використовує телефон, де шахрай під різними обманними приводами виманює потрібні для нього відомості, отримали назву «вішинг». Через засоби мобільного зв'язку, як через інструмент впливу можна впливати на людей. При спілкуванні по телефону з іншою людиною нескладно представитися якоюсь іншою людиною, а якщо додати знання психології і переконати співрозмовника в передачі якихось конфіденційних відомостей, а то й часто перевести якусь грошову суму на банківський рахунок, який надасть зловмисник, не складе труднощів. Тільки за 2022 рік на території Київської області Міністерством внутрішніх справ України було зареєстровано 287 злочинів, пов'язаних з даним видом шахрайства, а саме з соціальною інженерією. Злочини були пов'язані з обманом по банківських картах, кредитам, різного роду оголошенням, біржовим угодам і навіть наданням інтимних послуг. Найбільша сума, яка була втрачена довірливими громадянами склала 3600000 грн, тільки після цього довірлива громадянка звернулася в поліцію.

Так само при розслідуванні даних кримінальних справ, було відзначено, що всі жертви знали про подібного роду шахрайства, але все одно потрапляли в мережі соціальної інженерії. Різного роду конкуренти можуть, використовуючи прийоми соціальної інженерії, а також проводити дослідження інших компаній з метою отримання інформації для їх розорення [27].

Не менш поширений метод соціальної інженерії – «смішинг». Це в принципі різновид фішингу. Суть даного прийому полягає в наступному: за допомогою СМС повідомлень зловмисник відправляє інформаційне повідомлення з посиланням на фішинговий сайт. Прикладом цього можуть бути СМС повідомлення, що приходять з різних сайтів оголошень, де спочатку йшла формальна бесіда, а потім буде вказано посилання, яка буде містити шкідливу програму. Для безпеки в таких випадках фахівці радять акуратно ставитися до СМС повідомлень сумнівного характеру, які можна розгледіти

при уважному зверненні і відповідно їх ігнорувати. Ні в якому разі не переходити за посиланнями. Крім того, не варто проводити спілкування, передзвонювати абоненту, який не відомий.

Також загрози можуть виходити від електронних листів і посилань. У соціальній інженерії дана загроза отримала назву «фітинг». Все це насправді відбувається за рахунок масових розсилок електронних листів нібито від якихось, можливо соціальних мереж, де людина безпосередньо зареєстрована або якихось інших інтернет-ресурсів, може бути навіть новин або якогось виграшу в новорічному розіграші призів. Можуть прийти будь-які повідомлення, що містять неправдиву інформацію, метою якої є одне завдання – змусити інтернет-користувача перейти за цим посиланням [24].

Отже, соціальна інженерія спрямована не на комп'ютери і ноутбуки, не на комп'ютерні мережі, а відповідно на її користувачів, тобто на людину. Зловмисникам, які працюють в даній сфері соціальної інженерії, цікаві тільки люди, які володіють фінансами, якими вони (зловмисники) будуть намагатися заволодіти. Крім того, їм так само цікаві і користувачі мережі Інтернет, які можуть володіти якоюсь інформацією, що представляє інтерес для зловмисника. До таких користувачам можна віднести і співробітників різних комерційних підприємств, а також державних установ і навіть дітей. Дані методи застосовується з метою виконання фінансових операцій, таких як злом і крадіжка відомостей включаючи CVV коду з карт, отримання одноразових банківських паролів та інших важливих відомостей. Шахраї або зловмисники однозначно використовують соціальну інженерію для отримання своєї фінансової вигоди, ставлячи собі за мету збагатитися за рахунок інших людей, тому не гребують нічим, навіть отриманням будь-якої інформації, що носить чисто конфіденційний інтерес.

Для захисту від соціальної інженерії та її атак, різних компаній однозначно необхідно навчати співробітників своєчасно розуміти і визначати шахрайські дії соціальної інженерії і звичайно ж правильно профілактувати. До речі на сьогоднішній день в деяких браузерах, а також в телефонних

компаніях з’явився так званий «антифішинг», який реагують на підозрілу активність будь-яких сайтів або телефонних номерів, повідомляючи це клієнтам або користувачам комп’ютерних мереж про можливу небезпеку. Крім цього, так само працюють і спам-фільтри, які виявляють і показують, як спам, блокуючи подальші дії шахраїв.

Особливо зросли атаки соціальної інженерії у зв’язку з підвищенням і необхідністю ролі соціальних мереж, електронної пошти та інших видів онлайн-комунікації в умовах пандемії коронавірусу COVID-19, що охопила весь світ, так як користувачі зіткнулися з різного роду обмеженнями особистих контактів і свободи пересування. Провідними фахівцями та експертами в сфері ІТ-технологій зафіксовано стрімке, більш ніж в два рази, зростання комп’ютерної злочинності, в першу чергу, здійснення фінансових шахрайств прийомами соціальної інженерії. Найпоширенішим злочином стало розкрадання фінансових коштів з особистих рахунків громадян.

1.3. Аналіз загроз від соціальної інженерії в організації

Більшість сучасних компаній витрачають величезні гроші на закупівлю та розробку захисних заходів та засобів, але в той же час працівники можуть надати весь спектр інформації для проникнення в систему необхідні зловмиснику, що позбавляє його необхідності прямого злому системи.

Соціальну інженерію можна розділити на дві основні категорії [23]:

– Методи, засновані на технологіях: являють собою різні сайти обманки і підроблені сайти, основна мета подібного змусити користувача повірити, що він взаємодіє з реальною інформаційною системою і змусити його надати персональні дані.

– Методи, засновані на людській психології: маніпуляцію особливостями людської психології пов’язані з інтересом до нової інформації або жагою наживи.

Однак найчастіше ці категорії тісно переплітаються між собою та соціальну інженерію простіше класифікувати за методами атак.

Як основні атаки методом соціальної інженерії можна виділити такі [20]:

Фішинг – одна з основних технік шахрайства в Інтернеті, спрямована на отримання даних авторизації користувачів. До найпоширенішого методу фішингової атаки можна віднести підроблені листи, які надсилаються жертвам електронною поштою. Подібні листи виглядають як офіційні листи від платіжних систем банків чи інших організацій, яким користувач потенційно довіряє. У подібних листах можуть бути форми введення персональних даних або посилання на різні web ресурси, що імітують офіційні сторінки. Найчастіше подібні підроблені листи неможливо з першого погляду відрізнити від їхнього оригінального виконання, але при трохи уважнішому вивченні стає ясно що з ними щось не так.

Основною причиною довіри у користувачів до подібних листів може бути не грамотність у сфері безпеки або будь-які технічні проблеми в системах з якими потенційна жертва могла зіткнутися.

Кві про кво (послуга за послугу) – дана техніка є прямим контактом зловмисника з жертвою по телефону або електронною поштою. Зловмисник може представитися як працівник служби технічної підтримки і проводити опитування на наявність технічних неполадок на робочому місці користувача або системі, або повідомити про їх наявність. Далі зловмисник повідомляє про необхідність усунення знайдених неполадок, і в процесі вирішення подібних проблем підштовхує жертву на вчинення дій, що дозволяє зловмиснику руками жертви встановити необхідне програмне забезпечення або виконати необхідні команди на комп’ютері жертви.

Зворотня інженерія – вид атаки схожий на кві про кво. Цей вид атаки спрямовано на створення ситуацій, у яких жертва сама змушена зв’язатися з атакуючим. Як приклад ця атака може бути реалізована наступним чином: зловмисник надсилає електронною поштою лист, що містить контакти вигаданої служби підтримки, і через деякий час спровокувати технічні

проблеми на робочому місці жертви. Жертва, зіткнувшись з неполадками з високою ймовірністю сама зв’яжеться зі зловмисником, сподіваючись отримати допомогу і часто буде готова виконувати інструкції по телефону. Наслідком такої технічної допомоги можуть бути практичні будь-які наслідки, довірлива жертва у зв’язку з технічною неграмотністю може і не запідозрити, що інструкції, які отримуються з іншого кінця дроту, можуть призвести до жахливих наслідків.

Претекстинг – дана атака найчастіше є дзвінками з використанням програмного забезпечення для відеоконференцій або звичайного телефону. Для успішної реалізації даної атаки необхідна попередня розвідка, зловмиснику необхідно знати якомога більше даних про свою жертву таких як (ім’я, дату народження, назви проєктів над якими вона працює, назва відділів, а також імена начальників та інших працівників відділу). Оперуючи даною інформацією, зловмисник входить у довіру до потенційної жертви і змушує жертву поділитися будь-якою інформацією, яка цікавить атакуючого.

Троянський кінь – дана техніка цілком ґрунтується на цікавості користувачів. Атака методом троянського коня схожа з фішингом і також передбачає відправку жертві повідомлення з вірусним вкладенням або посиланням на нього і якимось привабливим повідомленням його відкрити. Це може бути повідомлення про виграш лотереї або пропозицію оновити антивірус. Довірливий користувач може запустити цю програму, тим самим надавши зловмиснику доступ до своєї системи.

Атака на водопої – ґрунтується не так на зараженні якомога більшої кількості машин, але на підвищенні ймовірності зараження. Атакуючий користується довірою жертв до найчастіше відвідуваних сайтів і у разі присутності на них уразливостей виробляє модифікацію сайту, додаючи різні експлойти, які згодом будуть виконані на комп’ютерах користувачів для встановлення шкідливого програмного забезпечення.

Дорожнє яблуко – один із найбільш проблемних методів для різних організацій, які мають будь-які загальнодоступні приміщення, такі як столові,

паркування або туалети. Атака передбачає використання фізичних носіїв, зокрема флеш накопичувачів. Зловмисник підкидає накопичувач із шкідливим ПЗ у подібні місця, а для стимуляції інтересу може нанести на флеш накопичувач будь-які позначки у вигляді логотипів компаній або різних підписів.

Отже, дії хакерів можна умовно поділити на етапи [19]:

1. Проведення первинної розвідки:

Протягом останніх 10 років активний розвиток отримують соціальні мережі і різні месенджери які щільно увійшли в ужиток великої кількості людей, чим і користуються зловмисники. Переважна більшість працівників великих компаній є активними користувачами месенджерів та соціальних мереж. Багато хто з них публікує фотографії та різні записи, які виглядають мало інформативними, проте можуть послужити ключем для запуску та реалізації успішної атаки. Як подібна інформація можуть виступати: фотографії, різна інформація про користувачів, геодані.

Окремо подібні дані можуть і не становити особливої небезпеки, проте згрупувавши їх зловмисник зможе отримати чітке уявлення про справи людини, яка його цікавить.

Сучасна мережа Інтернет влаштована таким чином, що з неї практично неможливо видалити інформацію, вся інформація, що потрапляє в неї, дуже швидко поширюється між людьми і сайтами, а також проходить резервне копіювання. Також небезпеку становлять програми-хробаки, які активно розповсюджуються в них, подібні програми створюють заманливі публікації від імені заражених користувачів.

2. Розвиток довірчих відносин:

Після закінчення первинної розвідки та отримання інсайдерської інформації зазвичай намагаються налагодити контакт із особою, яка має доступ до корисних ресурсів. Метою подібних дій є маніпуляція над психологічною схильністю людини довіряти більш авторитетним особам.

Зловмисник може видати себе за авторитетне обличчя у будь-якій сфері цікавій жертві, і користуючись цим спробувати отримати паролі користувача та доступ до його сесій.

3. Використання та експлуатація відносин:

На цьому етапі зловмисник ставить за мету закріпити авторитет перед жертвою. І з допомогою засобів маніпуляції привести її до вигідного йому емоційного стану. Подібну маніпуляцію можна використовувати для:

– отримання персональної інформації або доступу до закритих приміщень;

– для маніпуляції іншими особами;

– подання соціального інженера іншим членам організації як довіреної та авторитетної особи.

4. Реалізація атаки:

На останньому етапі відбувається безпосередня реалізація раптової атаки. Добре реалізованою атакою вважається та, що залишає у жертви відчуття правильно скоєних дій, що дає вікно для реалізації наступних атак.

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ОРГАНІЗАЦІЯХ

2.1. Методи атак реалізованих за допомогою соціальної інженерії

Для впливу на людину соціальні інженери використовують численні і різноманітні техніки і методики психологічного впливу. Зупиняючись на атаках соціальної інженерії, стає ясно, що атаки впливають на рівень підсвідомості, так як в більшості злочинів потерпілі чули про такий або подібний вид шахрайства. Ці знання важливі для подальшого запобігання від дії атак соціальної інженерії [23].

Всі класифікації атак соціальної інженерії спрямовані на те, щоб людина, на яку впливає зловмисник, добровільно повідомила інформацію, яка буде представляти якийсь інтерес і якою можна буде користуватися. Не варто забувати, що зловмисник може видати себе за кого завгодно, попередньо зібравши інформацію про об’єкт своєї атаки – через соціальні мережі, або за допомогою результатів різних інтернет-опитувань, придбання інформації у недобросовісних компаній тощо. Такий прийом отримав назву «претекстинг», коли зловмисник заздалегідь зібрав максимальну інформацію про об’єкт, щоб не викликати у нього підозри. І тут все дії зловмисника засновані на створенні довірчих відносин і досягнення довіри у об’єкта атаки. І так як правило зловмисники представляються співробітниками, банків або ж біржовими гравцями і намагаються отримати максимальну інформацію у довірливих осіб [23].

Самим, напевно, поширеним інструментом зловмисників, в соціальній інженерії, на сьогоднішній день є фішинг. Це англійське слово означає «риболовля». Зловмисниками спеціально створюються схожі сайти, так би мовити сайти двійники, у надії, що неуважні користувачі увійдуть на підроблений сайт, при цьому залишать там свої дані авторизації, які потрібні шахраям. Найбільш підроблені сайти на сьогоднішній день – це сайти кредитно-фінансових організацій, хоча для входу як правило запитується код підтвердження і без довіри користувачів зловмиснику даної інформації не отримати, зловмисник буде всіляко намагатися виманити даний код підтвердження. Також підробки сайтів поширені в різних страхових

компаніях, наприклад, з автострахування автомобілів, і звичайно ж всіляких інтернет-магазинів. Отримавши паролі і логіни неуважних користувачів, зловмисники починають збирати інформацію, щоб потім скористатися їй в своїх корисливих інтересах. За різними даними статистичних служб близько 45% Інтернет користувачів, які отримували електронні листи від невідомих джерел, при переході якраз і потрапляли на такі фітингові сайти або сайти-підробки. Де через свою неуважність залишали свої логіни і пароль.

Для отримання такого роду інформації або так би мовити для усипляння пильності користувачів, крім довірливості, зловмисники також використовують інші почуття людини. Наприклад, жадібність, величезне бажання до отримання вигоди користувачем і боязні будь-яких ситуацій. Раніше це були фінансові піраміди, де зловмисники заманювали своїх жертв обіцянками, що скоро піде фінансовий прибуток і їм. Зараз представляються співробітниками брокерських компаній [24].

На сьогоднішній день фішинг носить в основному комбінований характер. Частина плану атаки соціальної інженерії зловмисник як правило все одно запускає через шкідливу програму, або видобуває відомості шляхом обману, а другу частину атаки він виконує на довірі, жадібності або страху користувача, щоб отримати остаточну конфіденційну інформацію.

Також не варто забувати про таке почуття людей як бажання допомогти нужденним. Почуття співчуття і допомоги закладено в багатьох простих людях і це дуже добре, але зловмисники в гонитві за своїм збагаченням ні з чим цим не вважаються, а навпаки користуються. Тому зловмисник розуміє, що якщо він постане перед користувачем нещасним і битим якоюсь трагедією, то користувач всіляко постарається його підтримати і допомогти.

Розглянемо ще кілька методів соціальної інженерії, які можуть представляти інтерес, а потім порівняти їх з техніками. Зловмисник може запропонувати користувачеві якийсь варіант, який може здатися не зовсім прийнятним, а потім пропонує більш м’який варіант, який більше сприйнятний користувачу. Хоча насправді зловмисник заздалегідь знає, що

вибере користувач і створює всього лише уявну ілюзію. Даний метод в соціальній інженерії називається від противного.

В соціальній інженерії існує також змішаний метод, який використовується в соціальній інженерії. Даний метод працює комбіновано, включаючи в себе всі раніше розглянуті методи [26].

Однією з технік соціальної інженерії є так званий «плечовий серфінг», який полягає в тому, що користувач, не звертаючи увагу на інших осіб вводить свої дані, щоб авторизуватися на якомусь сайті. А сторонні особи прекрасно можуть бачити цю інформацію.

Трохи зупинимося на так би мовити випадках, коли сам користувач, будучи впевнений у якихось комп'ютерних фахівцях, сам надає всі свої дані необхідні для авторизації так званому спеціалісту, сподіваючись, що це може допомогти прискорити процес відновлення його комп'ютерної техніки. А сам фахівець під час усунення якихось поломок проводить маніпуляції з отримання якоїсь інформації і залишається поза підозрою. У такому випадку говорять про зворотну соціальну інженерію.

Зупинимося також на техніці соціальної інженерії з підкиданням флешок, а також отриманні флешок для скачування з них музики або фільмів. Іноді цю техніку називають в соціальній інженерії технікою «дорожнього яблука» або приманкою. Іноді флешки просто підкидають, а цікавість співробітників, які знайшли цю флешку, при її використанні можуть заразити комп'ютерну техніку шкідливими програмами.

Ще одним технічним прийомом соціальної інженерії може бути дзвінок зловмисника, який представляється співробітником технічної підтримки і нібито хоче допомогти поліпшити роботу комп'ютера користувача. Спочатку зловмисник пропонує алгоритм дій користувачу. В результаті чого виводить користувача на сайт з шкідливим програмним забезпеченням або отримує віддалений доступ.

Як правило багато хто думає, що соціальна інженерія – це фішинг, обман в соціальних мережах, а також різного роду обман з використанням

мобільного зв’язку або підкидання заражених флешок. Але в реальності все не так-то просто. Насправді у соціальній інженерії все взаємопов’язано і використовуються різного роду комбіновані прийоми і методи, які можуть насправді представляти реальну загрозу користувачам.

2.2. Засоби захисту від атак реалізованих за допомогою соціальної інженерії

У боротьбі з методами соціальної інженерії різні засоби захисту від шкідливого програмного забезпечення просто не ефективні, оскільки зловмисники атакують користувачів, людину і через неї отримують доступ до інформації [27].

Розглянемо основні розробки протидії та реалізації захисту від атак методами соціальної інженерії. Сучасні комп’ютерні мережі і різні комп’ютерні пристрої звичайно ж відкривають компаніям нові і дуже хороші перспективи для більш вигідної стратегії та введення на ринок нових продуктивних розробок. Але для всього цього, тобто для використання в максимальних обсягах різного роду перспектив, однозначно потрібні надійні, гарантовані рівні інформаційної безпеки. Звичайно ж головним завданням будь-яких фахівців з розробки та реалізації засобів захисту від деяких зовнішніх загроз, є забезпечення інформаційної безпеки, що відповідно дозволить створити всі передумови для успішного розвитку комерційних і некомерційних структур. При створенні таких розробок фахівці повинні так само враховувати всілякі ризики в області інформаційної безпеки і намагатися максимально знизити ризик.

На сьогоднішній день фахівці різних компаній роблять свій упор в розвиток навчання співробітників своїх компаній для підвищення інформаційної безпеки, протидії атакам методами соціальної інженерії.

Забезпечення інформаційної безпеки не може бути тільки за рахунок високих технологій на базі технічних засобів, в обов’язковому випадку

потрібні грамотні програмні рішення, якими і щодня займаються фахівці різних систем для створення програм з навчання співробітників.

Зупинимося безпосередньо на людському факторі, так як людина управляє всіма технічними процесами і самої технікою. 80% закінчених атак припадало на людину. Необхідно звернути увагу, по-перше, на хмарну безпеку, де може зберігатися величезна кількість інформації, як великих компаній, так і простих користувачів. Це наприклад фотографії паспортів, якихось різних, може бути навіть фінансових документів. Тому шкідливі загрози дуже небезпечні компаніям, зважаючи на втрати різної дуже цінної інформації, в тому числі і фінансової, не кажу вже про простих користувачів, тому має величезне значення для розробки і реалізації засобів захисту від деяких зовнішніх загроз різного рівня користувачів. Але як не дивно в багатьох навіть дуже великих компаніях не приділяється увага такому рівню захисту, як проведення навчання співробітників від можливих загроз і їх правильної поведінки для створення впевненої безпеки. В першу чергу це звичайно ж навчання як розпізнати і як себе правильно вести при виявленні якихось підозрілих електронних повідомлень, телефонних дзвінків від абонентів яких немає у вашому списку і посилань на веб-сайти. Крім того, такого роду навчання допоможе співробітникам і в той момент, коли вони будуть перебувати поза робочим часом, відповідно будуть простими користувачами, але завдяки навчанню вони зможуть захистити свою особисту інформацію, принаймні, як мінімум в соціальних мережах [20].

Потрібно пам’ятати, що будь-який технічний пристрій або людський фактор має вразливість, дуже важливий для зловмисників. Так як зловмисник і шукає такі місця, а краще навіть кілька слабких місць, для його вторгнення. Тому при розробці та реалізації засобів захисту від деяких зовнішніх загроз інформаційної безпеки необхідно враховувати, що тільки надійний захист може допомогти убезпечити себе не тільки простим користувачам, але і різного рівня компаніям, починаючи від дрібних і закінчуючи дуже великими [18].

При розробці та реалізації засобів захисту від деяких зовнішніх загроз інформаційної безпеки не варто забувати про раніше існуючі, так би мовити вироблені практичні захисні методи, які дуже вдало справлялися з різного роду атаками зловмисників. Тому однозначним фундаментом в успішному захисті компанії від різних загроз буде проведення занять з навчання співробітників компаній. У проведенні занять повинно бути не тільки ознайомлення і вивчення засобів виявлення і запобігання вторгнень, але і, хоча б найпоширеніші методи і техніки соціальної інженерії.

Моделювання ситуацій може дати чудовий результат. Крім цього рекомендується при проведенні занять ділити співробітників на команди. Відповідно одна команда зловмисників, яка повинна представити різні види загроз, а інша захисту з діями по відбиттю атак даного роду. В кінці заняття обов’язково необхідно проведення аналізу можливих помилок, допущених співробітниками.

Крім того, при розробці проведення занять з персоналом компаній необхідно враховувати вивчення такого роду інформації [17]:

– як правильно встановлювати безпечні поштові та веб-шлюзи, які зможуть фільтрувати шкідливі посилання, які приходять у вигляді спаму;

– за допомогою яких засобів захисту можливо здійснювати перевірку електронних листів і звертати особливу увагу, які прийшли не зі своєї корпоративної мережі;

– як провести настройку системи оповіщення на виявлення деяких адрес сервісів, схожих на ім’я своєї компанії;

– для співробітників безпеки обов’язково проводити поділ всієї корпоративної мережі на різні структурні елементи і встановити окремий доступ до кожної групи, враховуючи службову ієрархію, і звичайно ж проведення щоденного контролю;

– так само для співробітників, які здійснюють безпеку компаній і IT-фахівців, необхідно враховувати роботу персоналу з дуже важливою

інформацією, то тоді вводити захист за допомогою як мінімум дворазової перевірки ідентифікатора;

– постійно відстежувати такі випадки, коли співробітник компанії викачує ту чи іншу інформацію компанії, коли це не потрібно. Обов'язково відстежувати всі дії по скачуванню інформації з кабінетів компанії, особливо коли вже закінчений робочий день;

– завжди контролювати і постійно перевіряти всі облікові записи, до яких є найбільш широкий доступ. Звичайно ж в обов'язковому порядку адміністративні мережі, так як при здійсненні вторгнень зловмисники можуть залишити там свій слід;

– при виявленні в мережі збільшених LDAP-запитів, потрібно розуміти, що це може бути підготовка до атаки і проведення вивчення мережі компанії. Тому при виявленні подібного роду дій приймати відповідні заходи;

– регулярно проводити установку свіжих автоматизованих програмних засобів на всіх системах, станціях і робочих місцях;

– спільно з IT фахівцями регулярно проводити аналіз всіляких загроз шкідливих атак на систему. Крім того, співробітники компаній, які мають допуск до конфіденційної інформації компанії, зобов'язані знати все процедури щодо запобігання шкідливих атак;

– якщо ж все таки буде виявлена атака, то спільно з IT-фахівцями слід оперативно знайти і усунути всі таємні входи в систему.

Не варто забувати, що на сьогоднішній день в Інтернеті крім корисної інформації, з нормальними сайтами, існує і інформація, яка розкриває техніку і методи соціальної інженерії Відповідно шахраї, познайомившись з такого роду інформацією можуть значно підвищити свої навички соціальної інженерії ,а також можуть знайти вже готове програмне забезпечення, з докладними інструкціями. Наприклад, можна навести поширені останні час ролики, які можна виготовити самому, просто скачавши програму з Інтернету. Суть цієї програми в тому, що до будь-якого, наприклад, персонажу з якого-небудь фільму або простого короткого ролика можна підставити, наприклад,

особу відомого співака або спільного знайомого. Таке відео називається діпфейковим. В інтернет-джерелах так само можна навчитися, як обійти протоколи безпеки багатофакторної аутентифікації, крім того і заходи перевірки ідентифікатора.

З урахуванням вищесказаного, щоб не стати жертвою соціальної інженерії простим користувачам, а тим більше співробітникам компаній, необхідно дотримуватися простих правил:

– ніколи не слід відкривати електронні листи, від невідомих або сумнівних джерел;

– по закінченні робочого дня необхідно завжди відключати комп'ютерну техніку і ставити складні паролі для авторизації при включенні;

– мінімальним захистом комп'ютера повинна бути антивірусна програма, яка зможе убезпечити від деяких атак.

Оскільки атаки соціальної інженерії як ніколи актуальні, нами були розроблені чіткі інструкції для персоналу організацій проти їх дій:

1. Ніколи не вірте на слово у телефонних або VoIP дзвінках. Навіть якщо вам дзвонять по внутрішньому телефону компанії. Необхідно перевіряти кожен номер з базою номерів організації чи є ця людина тією, ким представилася.

2. Ніколи нікому не повідомляйте або надсилайте свій пароль ні в якому разі, навіть якщо це пряма вимога начальника або від цього залежить виконання важливого завдання. Ви повинні чітко усвідомлювати всі ризики, пов'язані з витоком корпоративних даних.

3. Ніколи не використовуйте на робочому пристрої особисті або незнайомі носії інформації, якщо ви принесли із собою або знайшли незнайомий пристрій або носій інформації віднесіть його в IT відділ де його спільно з вами перевірять на наявність загроз і відкриють на ізольованому пристрої, у разі підтвердження безпеки пристрою вам буде видано дозвіл на його використання або пошук особи, яка його втратила.

4. Завжди перевіряйте відправників електронних листів і в жодному разі не відкривайте їх, якщо вони прийшли з незнайомої вам адреси. Подібні листи можуть мати заголовки або цікаві вам вкладення, ні в якому разі не відкривайте їх в них можуть бути віруси. Повідомте про подібний лист ІТ відділу та службу безпеки.

5. Ви повинні використовувати унікальні паролі у різних системах. Паролі повинні бути дійсно унікальні, оскільки паролі частково збігаються, сильно підвищується шанс того, що зловмисники зможуть підібрати пароль, якщо ж вам складно запам’ятовувати паролі використовуйте менеджери паролів. Однак використовуйте різні менеджери та майстер паролів для робочих та неробочих цілей.

6. Ніколи не відчиняйте двері незнайомим людям, кожен відвідувач має бути у супроводі офіційно представленого до нього співробітника.

7. Ніколи не відчиняйте двері навіть знайомим людям. Навіть знайомі вам співробітники можуть становити небезпеку, оскільки вони можуть бути звільнені і з метою помсти планувати інсайдерську атаку. У випадку, якщо ви або будь-хто інший забули перепустку у своєму кабінеті, необхідно зв’язатися з начальником або службою безпеки для вирішення цієї ситуації.

3. РОЗРОБКА НАВЧАЛЬНОЇ СИСТЕМИ ПРОТИДІЇ АТАКАМ РЕАЛІЗОВАНИХ ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ОРГАНІЗАЦІЇ

3.1. Визначення актуальних загроз та уразливостей від атак реалізованих за допомогою соціальної інженерії

Визначення актуальних загроз та уразливостей від атак реалізованих за допомогою соціальної інженерії буде проводитися на підприємстві ПрАТ «Оболонь».

Історія корпорації «Оболонь» починається у 1974 році, коли відбувся намив майданчика для будівництва броварні. Структура корпорації «Оболонь» формувалася довгі роки під впливом стратегії розвитку, яка спрямована на диверсифікацію виробництва, перехід на сировину власного виробництва, інноваційний підхід, абсолютну екологічну безпеку та повну соціальну відповідальність. Корпорація «Оболонь» об'єднує головний завод, два відокремлені цехи, два дочірніх підприємства та чотири підприємства з корпоративними правами. Загалом, у корпорації працює близько 7,5 тис. людей [9].

Основними структурними одиницями корпорації «Оболонь» є:

1) головний завод у місті Київ:

– ПрАТ «Оболонь» (виробництво пива, безалкогольної продукції, мінеральної води, пивної дробини та ін.);

2) дочірні підприємства:

– ДП ПрАТ «Оболонь» «Пивоварня Зіберта», м. Фастів, Київська обл. (виробництво пива);

– ДП ПрАТ «Оболонь» «Красилівське», м. Красилів, Хмельницька обл. (виробництво мінеральної води, слабоалкогольних та безалкогольних напоїв) [9].

Місце розташування ПрАТ «Оболонь»: Україна, 04655, м. Київ, вул. Богатирська, 3. Основні види діяльності ПрАТ «Оболонь»:

15.96.0 Виробництво пива.

15.97.0 Виробництво солоду.

15.98.0 Виробництво мінеральних вод та інших безалкогольних напоїв [9].

Корпорація «Оболонь» першою серед підприємств харчової промисловості у 2008 році сертифікувала чотири системи управління одразу. Під час аудиту, який здійснювали представники німецької компанії «DEKRA-ITS», «Оболонь» підтвердила відповідність вимогам ISO 9001:2008 (Системи управління якістю), ISO 22 000:2005 (Системи управління безпечністю харчових продуктів), ISO 14 001:2004 (Системи екологічного керування), OHSAS 18 001:2007 (Системи управління безпекою та гігієною праці). Впровадження цих систем управління підтверджує той факт, що «Оболонь» піклується про споживачів, суспільство, стан навколишнього середовища та співробітників підприємства. Завдяки виконанню всіх вимог споживач може бути впевненим в якості й безпечності продукції корпорації. Разом із головним заводом сертифікацію отримали два дочірніх підприємства: ДП ПрАТ «Оболонь» «Красилівське» та ДП «Пивоварня Зіберта» у м. Фастів отримали сертифікат згідно з вимогами ISO 9001-2008 і ISO 22 000:2005 [9].

Організаційна структура управління ПрАТ «Оболонь» являється лінійно-функціональною та має наступний вигляд (рис. 3.1).

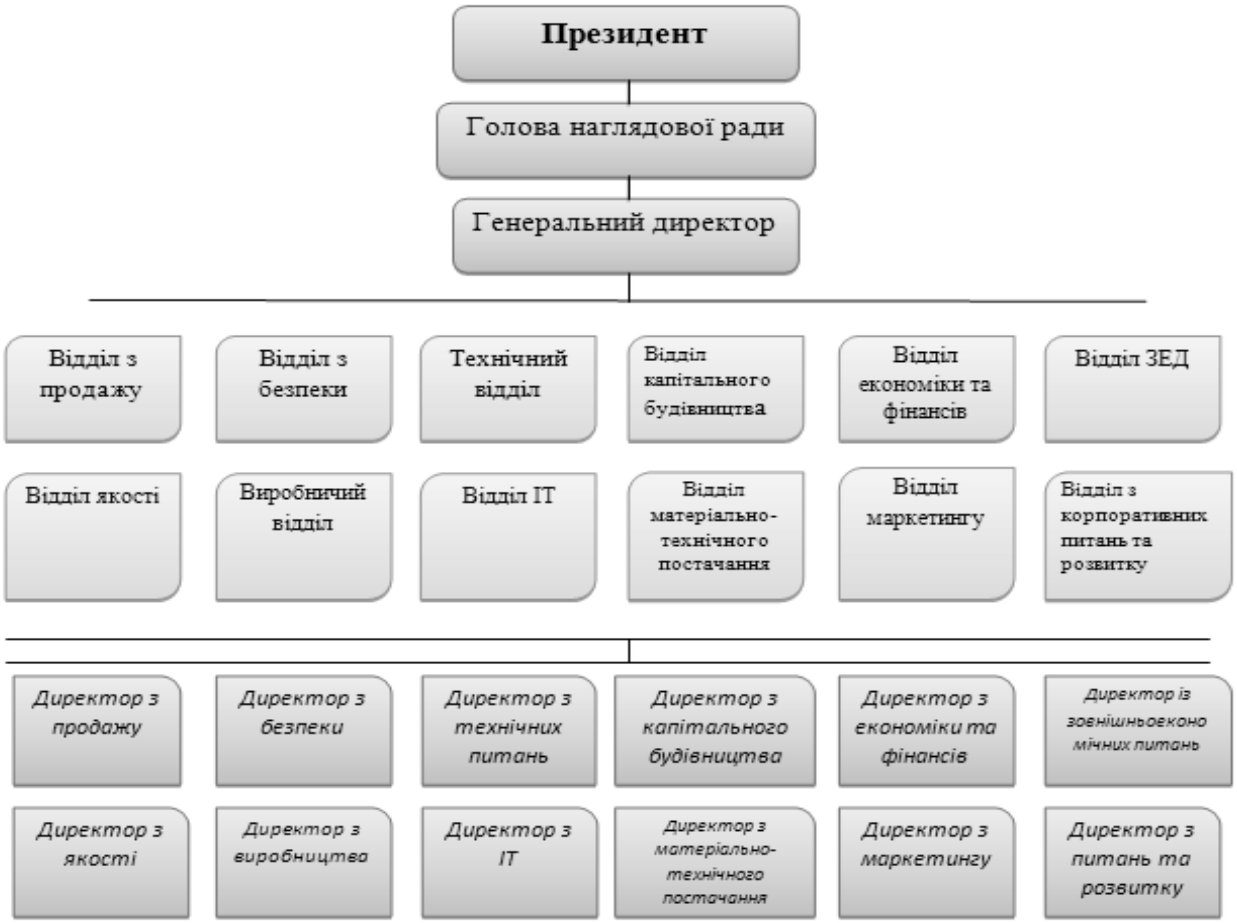

Рис. 3.1. Організаційна структура управління ПрАТ «Оболонь»

Джерело: [9]

У табл. 3.1 проведено аналіз динаміки виробництва продукції ПрАТ «Оболонь» у розрізі асортиментних груп.

Таблиця 3.1

Аналіз динаміки виробництва продукції ПрАТ «Оболонь» у розрізі асортиментних груп упродовж 2021-2022 рр.

Найменування продукції (видів, товарних груп)	Вироблено продукції в натуральному виразі, од.		Відхилення	
	2021 р.	2022 р.	Абсолютне, +/-	Відносне, %
Пиво Premium	19745524	22853525	+3108001	+15,74
Пиво Uppermainstream	18437662	21815556	+3377894	+18,32
Пиво Mainstream	17911328	19175109	+1263781	+7,06
Пиво Discount	16077131	17099171	+1022040	+6,36

Продовження табл. 3.1

Найменування продукції (видів, товарних груп)	Вироблено продукції в натуральному виразі, од.		Відхилення	
	2021 р.	2022 р.	Абсолютне, +/-	Відносне, %
Регіональні сорти пива	12153546	13730325	+1576779	+12,97
Сокові та соковмісні напої	9808964	12273527	+2464562	+25,13
Сучасні напої	9489973	10525368	+1035395	+10,91
Ностальгічна серія безалкогольних напоїв	9713267	9305300	-407967	-4,20
Квас живого бродіння	6714754	8850050	+2135296	+31,80
Мінеральна вода	7783373	8686160	+902787	+11,60
Слабоалкогольні напої	7049694	7848501	+798807	+11,33
Сидр	6571208	7684612	+1113403	+16,94
Промислові товари	6507410	7557142	+1049731	+16,13
Сухарики	6347915	7447882	+1099967	+17,33
Грінки	5183599	7247572	+2063973	+39,82
Разом	159495350	182099800	+22604450	+14,17

Джерело: складено автором за даними підприємства

Отже, упродовж 2021-2022 рр. спостерігаємо збільшення обсягу виробництва продукції ПрАТ «Оболонь» на 22604450 одиниць, або на 14,17%.

У табл. 3.2 проведено аналіз основних показників діяльності ПрАТ «Оболонь».

Таблиця 3.2

Основні показники діяльності ПрАТ «Оболонь» упродовж 2021-2022 рр.

Найменування продукції (видів, товарних груп)	Одиниці виміру	Періоди		Відхилення	
		2021 р.	2022 р.	Абсолютне, +/-	Відносне, %
1	2	3	4	5	6
1. Обсяг реалізації продукції в натуральному виразі	од.	159495350	182099800	+22604450	+14,17

Продовження таблиці 3.2

1	2	3	4	5	6
2. Обсяг виробництва продукції у вартісному вираженні у:					
діючих цінах	тис. грн.	5986592	8649174	2662582	44,48
3. Чистий дохід (виторг) від реалізації продукції	тис. грн.	5986592	8649174	2662582	44,48
4. Собівартість реалізованої продукції	тис. грн.	4877463	5751536	874073	17,92
5. Адміністративні витрати	тис. грн.	423695	470629	46934	11,08
6. Витрати на збут	тис. грн.	790218	684010	-106208	-13,44
7. Повні витрати на виробництво і реалізацію продукції	тис. грн.	6091376	6906175	814799	13,38
8. Прибуток (збиток) від реалізації продукції	тис. грн.	-104784	1742999	1847783	-1763,42
9. Прибуток (збиток) чистий	тис. грн.	-130821	1114681	1245502	-952,07
10. Витрати на 1 грн. чистої виручки від реалізації	грн.	1,02	0,80	-0,22	-21,53
11. Рентабельність діяльності (продаж)	%	-2,15	16,14	18,29	-
12. Рентабельність продукції	%	-2,68	19,38	22,06	-
13. Середньоспискова чисельність промислово-виробничого персоналу	осіб	3329	3192	-137	-4,12
14. Продуктивність праці	тис. грн./осіб	1798,32	2709,64	911,33	50,68

Джерело: складено автором за даними підприємства

Отже, упродовж 2021-2022 рр. спостерігаємо позитивне збільшення обсягу реалізації продукції ПрАТ «Оболонь» у натуральному вираженні на 14,17%. Також відбулося зростання чистого доходу від реалізації продукції ПрАТ «Оболонь» на 2662582 тис. грн. Поряд зі збільшенням чистого доходу

підприємства відбулося зростання собівартості реалізованої продукції ПрАТ «Оболонь» на 874073 тис. грн., або на 17,92%.

Упродовж 2021 р. ПрАТ «Оболонь» вело збиткову діяльність – чистий збиток склав 104784 тис. грн. Негативним моментом у діяльності ПрАТ «Оболонь» стало від'ємне значення показників рентабельності діяльності (продаж) та рентабельності продукції, що пов'язано із збитковою діяльністю підприємства. У 2022 р. спостерігаємо отримання прибутку 1114681 тис. грн., що свідчить про розширення діяльності. Упродовж 2021-2022 рр. спостерігаємо скорочення середньоспискової чисельності промислово-виробничого персоналу на 137 осіб, або на 4,12%. Зменшення чисельності персоналу із одночасним зростанням обсягу виробництва продукції у вартісному вираженні позитивно позначилося на збільшенні продуктивності праці на 911,33 тис. грн./ос., або на 50,68%.

Проведемо аналіз показників ліквідності, платоспроможності, ділової активності та рентабельності підприємства ПрАТ «Оболонь» за 2021-2022 рр. (табл. 3.3).

Таблиця 3.3

Аналіз показників ліквідності, платоспроможності, ділової активності та рентабельності підприємства ПрАТ «Оболонь» за 2021-2022 рр.

Показники	Роки		
	Періоди		Абсолютне відхилення від рівня 2020 р, +/-
	2021	2022	
Показники ліквідності			
Коефіцієнт покриття	1,83	1,78	-0,05
Коефіцієнт швидкої ліквідності	0,22	0,27	0,05
Коефіцієнт абсолютної ліквідності	0,01	0,01	0
Показники фінансової автономії			
Коефіцієнт автономії	0,003	0,005	0,002
Коефіцієнт фінансування	0,02	0,02	0
Коефіцієнт маневреності власного капіталу	6,65	8,17	1,52

Продовження табл. 3.3

Показники	Роки		
	Періоди		Абсолютне відхилення від рівня 2020 р, +/-
	2021	2022	
Показники ділової активності			
Коефіцієнт оборотності активів	0,94	1,03	0,09
Коефіцієнт оборотності кредиторської заборгованості	1,73	1,84	0,11
Коефіцієнт оборотності дебіторської заборгованості	20,39	14,35	-6,04
Коефіцієнт оборотності основних засобів	1,28	1,47	0,19
Коефіцієнт оборотності власного капіталу	75,87	81,85	5,98
Коефіцієнт рентабельності активів	0,06	0,02	-0,04
Коефіцієнт рентабельності власного капіталу	4,63	1,79	-2,84
Коефіцієнт рентабельності діяльності	-0,021	0,16	0,181

Джерело: Розроблено автором самостійно за звітністю підприємства

Таким чином, аналізуючи дану таблицю, можемо сказати, що ПрАТ «Оболонь» у 2022 році було ліквідним, фінансово стійким, але діяльність його була збитковою, рівень рентабельності дяльності становив 18,29%.

На стан господарської діяльності підприємства великий вплив здійснює зовнішнє середовище. Основне призначення аналізу системи управління якістю напоїв полягає у визначенні можливостей і загроз, на шляху розвитку ПрАТ «Оболонь», а також його стратегічних альтернатив. Аналіз системи управління якістю напоїв є складовою так названого SWOT-аналізу.

Завдання аналізу полягає у знаходженні реальних можливостей, для забезпечення конкурентних переваг підприємства. Основне призначення зовнішнього аналізу – виявити й усвідомити можливості та загрози, що можуть впливати на діяльність ПрАТ «Оболонь» сьогодні або в майбутньому.

Можливості ПрАТ «Оболонь» являють собою позитивні фактори (тенденції та явища) системи управління якістю напоїв, що можуть сприяти збільшенню обсягу продажу та прибутку.

Загрозами є негативні фактори (тенденції і явища) системи управління якістю напоїв, що можуть призвести за відсутності відповідної реакції товариства до значного зменшення обсягу продажу та прибутку. Тому слід провести SWOT-аналіз діяльності ПрАТ «Оболонь» (табл. 3.4).

Таблиця 3.4

SWOT-аналіз ПрАТ «Оболонь»

		Сильні сторони	Слабкі сторони
		1. Незалежність від усіх постачальників. 2. Збільшення товарообігу (висока рентабельність). 3. Вища за середню обізнаність про стан ринку. 4. Знання про найважливіші стратегічні групи(можливості захисту від конкурентів). 5. Професійна підготовка спеціалістів (тренінги, курси, семінари) 6. Чіткі розуміння та знання потреб споживачів (спеціальні маркетингові навички)	1. Значні витрати на транспортування товару до покупця (1% від вартості товару) 2. Брак фінансових ресурсів (перевага залученого капіталу над власним) – складає 4%
Можливості	1. Економічний розвиток країни (захист бізнесу з боку держави). 2. Зниження податкових ставок (до 18%) 3. Розширення ринку збуту, (збільшення об'ємів поставок). 4. Подолання конкуренції за рахунок якості та ціни товару (більш вигідні умови продажу)	Сила і можливості 1. Стати основним постачальником будівельних матеріалів і товарів народного споживання 2. Розробка нових шляхів просування напоїв з метою розширення ринків збуту.	Сила і загрози 1. Випробування в роботі та отримання позитивних результатів. 2. Зниження цін за рахунок збільшення об'ємів продаж
Загрози	1. Інфляція. 2. Ймовірність виникнення нових конкурентів (в т. ч. іноземних). 3. Зростання збуту товарів-замінників. 4. Уповільнений темп зростання ринку або спад.	Слабкість і можливості 1. Просування продукції з акцентуванням уваги на перевагах компанії. 2. Зниження цін за рахунок збільшення об'ємів продаж.	Слабкість і загрози 1.Погіршення фінансового стану підприємства. 2. Закриття проекту.

Джерело: складено автором

Так, після проведення SWOT-аналізу ПрАТ «Оболонь» можна дійти висновку, що на підприємстві переважають сильні сторони, а також воно має всі шанси для подальшого розвитку. Щодо слабких сторін, то підприємству варто направити свої зусилля на зменшення заборгованості та підвищення ефективності розвитку товариства. За результатами проведеного SWOT-аналізу ПрАТ «Оболонь» встановлюємо, що досліджуване товариство має низку сильних сторін і можливостей на ринку реалізації продажу напоїв.

ПрАТ «Оболонь» реалізує свою продукцію через такі канали збуту:

1) нульовий канал – без посередників продукція реалізується великим юридичним особам та державним установам (здебільшого такі компанії організують тендери), також без посередників здійснюються великі постачання на експорт;

2) одноріневий канал – через дилерів продукція реалізується дрібним юридичним та фізичним особам.

Продукцію ПрАТ «Оболонь» можна оплатити безготівковим розрахунком. Дилерам ПАТ «Оболонь» надаються знижки: 10% від 20 тис. грн.; 20% від 50 тис. грн. Продукція постачається в Києві протягом 5 діб, по регіонах – протягом 10 діб. Для дилерів підприємства також проводяться акції, найчастіше за все пропонується товар зі зниженою ціною на 5-10%, який має завеликі залишки на складах.

Слід відзначити, що постачальники мають значну ринкову владу над виробниками, що не мають вертикальної інтеграції. Вони встановлюють ціни, і малі підприємства змушені погоджуватись на них. Вибір комплектуючих для пива, солоду, мінеральних вод та інших безалкогольних напоїв на ринку України достатньо обмежений, а чисельність постачальників невелика.

Сировину і необхідні матеріали ПрАТ «Оболонь» закуповує у українських постачальників. Основні постачальники ПрАТ «Оболонь» і види ресурсів та матеріалів, які вони постачають, розглянемо за допомогою табл. 3.5. Головні постачальники сировини та матеріалів ПрАТ «Оболонь» розташовуються на невеликих відстанях від м. Київ, або в самому місті. Це

дозволяє зменшити транспортні витрати підприємства, пов’язані з доставкою сировини і матеріалів. Сировина та матеріали від постачальників завозяться на ПрАТ «Оболонь» в основному власним транспортом підприємства.

Таблиця 3.5

Основні постачальники ПрАТ «Оболонь»

№	Назва постачальника	Сировина, яка постачається	Місце розташування
1	Житомирська хмелефабрика	Хміль (пресований)	м. Житомир
2	Дубнівська хмелефабрика	Хміль (пресований)	м. Дубно
3	Колективні с/г підприємства	Ячмінь	Рівненська, Полтавська, Хмельницька області
4	Українська пивна компанія	Амилосубтилін, ферменти та ін.	м. Київ
5	ПАТ «Рівнеазот»	Вуглекислота	м. Рівне
6	Фірма «Утос» УВП	Кроненпробка	м. Рівне
7	ТОВ «Лілея»	Етикетка	м. Полтава
8	ПАТ «Новобуд»	Сода каустична	м. Львів
9	ТОВ «Тернопільдерев»	Пиломатеріали	м. Тернопіль
10	ПМП «Рост»	Металоконструкції	м. Полтава
11	Приватні підприємства	Ящики поліетиленові	м. Полтава

Джерело: складено автором

Узагальнена характеристика основних логістичних процесів у ланцюгах постачання ПрАТ «Оболонь» представлена у табл. 3.6.

Таблиця 3.6

Логістичні бізнес-процеси у ланцюгах постачання ПрАТ «Оболонь»

Процес	Виконавець	Зміст процесу	Результат процесу
Приймання вантажів	Оператор відділення	Отримання інформації про вантаж, місце доставки та одержувача, відправника, особливості оплати, оптимальний час доставки. Оцінка об'ємної ваги вантажу, визначення вартості перевезення	Вантаж прийнято, інформація щодо вантажу внесена в інформаційну систему, оформлена ТТН
Передача вантажу в зону зберігання та очікування комплектації	Працівник складу відділення	Переміщення вантажу з зони приймання та оформлення в зону зберігання та очікування комплектації (за необхідності – застосування складської техніки)	Вантаж розташовано у зоні зберігання відповідно до черги на відправлення
Комплектування вантажів на відправлення	Комплек-тувальник	Комплектування вантажів у транспортний засіб із врахуванням вимог «ощадливого виробництва» та вимог щодо збереження вантажів під час транспортування	Вантаж укомплектовано в транспортний засіб
Транспортування вантажів	Водій-експедитор	Перевезення вантажу транспортними засобами компанії або перевізниками-підрядниками	Вантаж транспортується до місця призначення (склад компанії або клієнту напряму)
Розвантаження та зберігання вантажів у відділенні логістичної компанії	Працівник складу	Розвантаження вантажів із транспортного засобу та розміщення на складі відділення компанії відповідно до умов зберігання	Вантаж розвантажено та розміщено на складі у відділенні компанії
Видача вантажу отримувачу	Оператор відділення	Видача клієнту вантажу із врахуванням додаткових вимог вантажовідправника (післяплата, тощо)	Вантаж отримано клієнтом

Джерело: складено автором

На рис. 3.2 наведено розподіл продажів пива, солоду, мінеральних вод та інших безалкогольних напоїв ПАТ «Оболонь» по областях України.

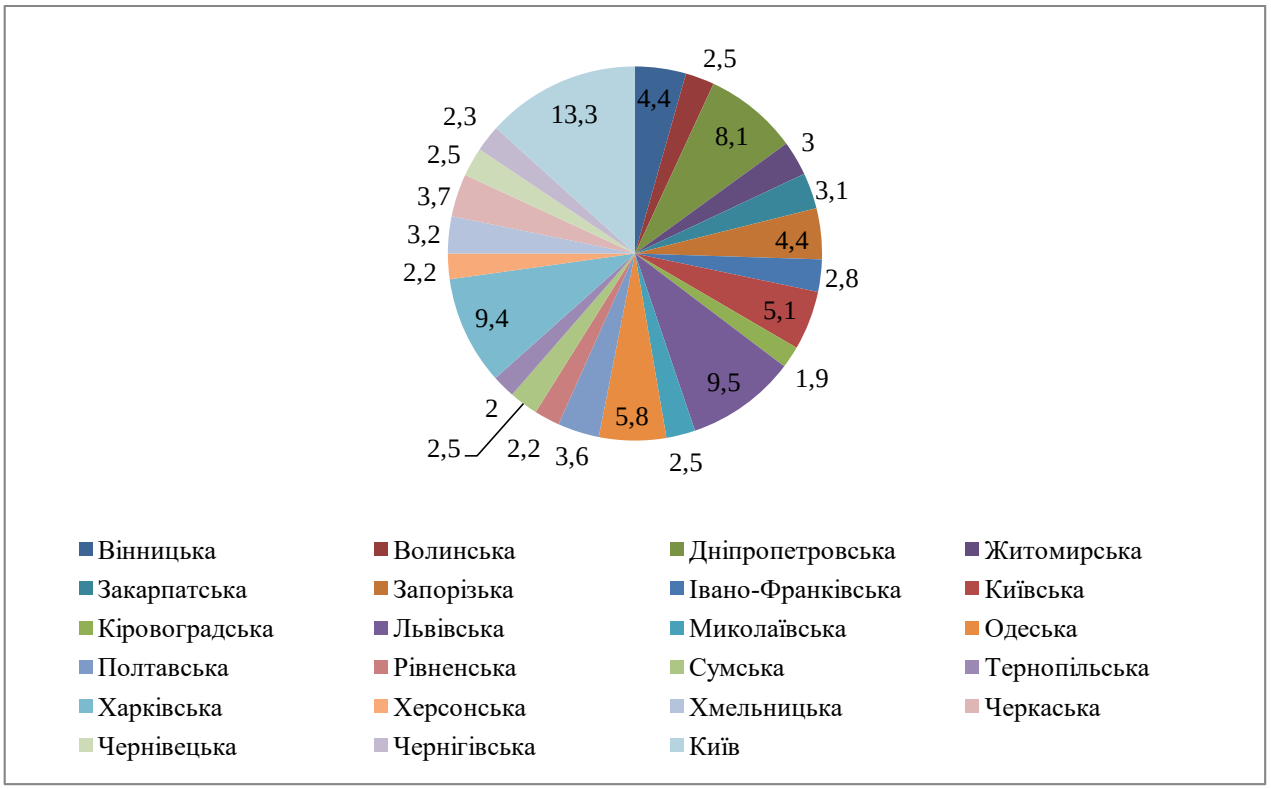

Рис. 3.2. Розподіл реалізації пива, солоду, мінеральних вод та інших безалкогольних напоїв ПрАТ «Оболонь» по областях за 2022 р. [13]

Джерело: складено автором

Згідно з даними рис. 3.2, розподіл реалізації продукції ПАТ «Оболонь» по областях такий: Вінницька – 4,4%; Волинська – 2,5%; Дніпропетровська – 8,1%; Житомирська – 3,0%; Закарпатська – 3,1%; Запорізька – 4,4%; Івано-Франківська – 2,8%; Київська – 5,1%; Кіровоградська – 1,9%; Львівська – 9,5%; Миколаївська – 2,5%; Одеська – 5,8%; Полтавська – 3,6%; Рівненська – 2,2%; Сумська – 2,5%; Тернопільська – 2,0%; Харківська – 9,4%; Херсонська – 2,2%; Хмельницька – 3,2%; Черкаська – 3,7%; Чернівецька – 2,3%; м. Київ – 13,3%.

Характеристика споживачів продукції підприємства ПрАТ «Оболонь» приведена у табл. 3.7.

Таблиця 3.7

Характеристика споживачів ПрАТ «Оболонь»

Група споживачів	Обсяг замовлень	Які чинники вплинули на вибір товару
Супермаркети (Ашан, Фреш, тощо)	50% замовлень	Специфіка діяльності підприємства – основна спеціалізація по виробництву напоїв
Оптові торгові компанії	25% замовлень	Специфіка діяльності підприємства – основна спеціалізація по виробництву напоїв
Фізичні особи	10% замовлень	Реалізація пива та безалкогольних напоїв на всі смаки, доступна ціна, висока якість товару

Джерело: складено автором

В ПрАТ «Оболонь» є два пікові періоди, протягом яких на склад поступає максимальна кількість замовлень. Перший період – з 12:00 до 14:00 (за цими замовленнями доставка товару клієнтам здійснюється за принципом «з сьогодні на сьогодні»), а другий період триває з 16:00 до 19:00 (доставка здійснюється «з сьогодні на завтра»).

Програма, що регулює прийомку, контроль, збирання та розподіл замовлень на складі, має назву EXIT. Вона забезпечує обробку замовлень за принципом «Fi-Fo» (first in – first out). Тобто, замовлення, що першими надійшли на склад, будуть збиратися та оброблятися у першу чергу.

На ПрАТ «Оболонь» у ролі вхідного потоку клієнтів виступають замовлення, що надходять у відділ збуту, у ролі каналів обслуговування – працівники складу, а у ролі вихідних потоків клієнтів – зібрані, проконтрольовані та відправлені зі складу до клієнтів замовлення.

Черги в організаціях характеризуються певним набором параметрів, а саме: середньою загрузкою працівника, що обслуговує чергу; середньою кількістю клієнтів, що очікують у черзі; середньою кількістю клієнтів у сервісні системі; середнім часом очікування у системі, а також ймовірністю знаходження n одиниць у системі.

Основними трьома величинами, необхідними для розрахунку параметрів черг, є: середня загрузка робітника, інтенсивність вхідного потоку та інтенсивність обслуговування.

Середня загрузка робітника – це відношення величини інтенсивності вхідного потоку заявок до інтенсивності обслуговування у сервісній системі. Тобто, ця величина показує те, скільки заявок у середньому обробляє (обслуговує) робітник.

Інтенсивність вхідного потоку показує те, скільки заявок надходить у сервісну систему підприємства за певний проміжок часу (зміна, доба), а інтенсивність обслуговування – скільки вхідних заявок обробляється (обслуговується) за такий же відрізок часу.

Отже, середня загрузка робітника розраховується за формулою:

$$\rho = \frac{\lambda}{\mu} \tag{3.1}$$

де ρ – середня загрузка робітника;

λ – інтенсивність вхідного потоку;

μ – інтенсивність обслуговування.

З внутрішньої документації ПрАТ «Оболонь» відомо, що інтенсивність вхідного потоку заявок на склад (кількість замовлень) становить в середньому за тиждень 1900 замовлень на добу. Зміна триває 12 годин (2 зміни за добу – денна та нічна). Отже, λ = 950 замовлень/зміна. Інтенсивність обслуговування (μ) становить 1000 замовлень/зміна Знаючи ці дві величини та послуговуючись формулою 2.7, можна знайти середню загрузку робітника:

$$\rho = \frac{\lambda}{\mu} = \frac{950}{1000} = 0{,}95$$

Якщо ρ = 0,95 помножити на 100%, то можна зробити висновок про те, що середня загрузка збиральника становить 95%.

Отже, тепер нам відомі всі три необхідні для розрахунків величини: ρ = = 0,95 , λ = 950 замовлень/зміна, а μ = 1000 замовлень/зміна.

За формулою 3.2 можна знайти середню кількість клієнтів, що очікують в черзі (для ПрАТ «Оболонь» це буде кількість замовників, які чекають на отримання замовленої продукції):

$$\overline{n}_l = \frac{\lambda^2}{\mu(\mu - \lambda)} \tag{3.2}$$

де $\overline{n}_l$ – середня кількість клієнтів, що очікують у черзі.

Для ПрАТ «Оболонь» цей показник дорівнюватиме:

$$\overline{n}_l = \frac{950^2}{1000(1000 - 950)} = 18{,}05$$

Тож, середня кількість клієнтів у черзі дорівнює 18,05.

Наступним показником є середня кількість клієнтів у системі, включаючи і тих замовників, чиї замовлення вже обробляються. Цей показник можна розрахувати за формулою 3.3:

$$\overline{n}_s = \frac{\lambda}{\mu - \lambda} \tag{3.3}$$

де $\overline{n}_s$ – середня кількість клієнтів у системі.

На складі ПрАТ «Оболонь» цей показник становить 19, який означає, що в середньому у сервісній системі організації знаходиться 19 клієнтів.

Середній час, який клієнти витрачають на очікування в черзі, та середній час очікування у сервісній системі можна знайти за формулами 3.4 і 3.5 відповідно:

$$\bar{t}_l = \frac{\lambda}{\mu(\mu - \lambda)} \tag{3.4}$$

$$\bar{t}_s = \frac{1}{\mu - \lambda} \tag{3.5}$$

де $\bar{t}_l$ – середній час очікування у черзі;

$\bar{t}_s$ – середній час очікування у системі.

В ПрАТ «Оболонь» $\bar{t}_l$ = 0,019 (годин), а $\bar{t}_s$ = 0,02 (годин).

Останнім параметром, що характеризує черги, є ймовірність знаходження певної кількості одиниць (n) в сервісній системі. Він розраховується за формулою 3.6:

$$P_n = (1 - \frac{\lambda}{\mu}) \times (\frac{\lambda}{\mu})^n \quad (3.6)$$

де P_n – ймовірність знаходження n одиниць у системі.

На ПрАТ «Оболонь» поточний рівень обслуговування для 19 клієнтів або меншої кількості являє собою вірогідність того, що у системі знаходиться від 1 до 19 замовлень. Тобто, якщо ми розраховуємо ймовірність знаходження 19 одиниць у системі, ми отримаємо результат: $P_n = 0,64$. Якщо цей результат помножити на 100%, то отримаємо висновок, що при завантаженості сервісної системи $\frac{l}{m} = 0,95$, вірогідність утворення у системі черги, яка складалася б з 19 або менше замовлень, становить 64%.

Для створення цілісної картини організації ланцюгів поставок асортименту продукції підприємства необхідно провести розрахунок певних показників (табл. 3.8).

Таблиця 3.8

Динаміка показників організації ланцюгів поставок продукції ПрАТ «Оболонь»

Показники	2020 р.	2021 р.	2022 р.	Відхилення +-		
				2021 / 2020	2022 / 2021	2022 / 2020
Частка логістичних витрат у сумарних витратах підприємства	9,41	49,64	17,00	+40,23	-32,64	+7,59
Коефіцієнт окупності логістичної системи	368,27	69,16	274,22	-299,11	+205,06	-94,05
Коефіцієнт рентабельності логістичної системи	5,47	0,98	5,41	-4,49	+4,43	-0,06
Рентабельність підприємства	1,88	1,77	2,50	-0,11	+0,73	+0,62

Джерело: складено автором

Варто відзначити, що особливістю організаційного забезпечення проведення комплексного аналізу ефективності логістичної діяльності в ПрАТ

«Оболонь» є закріплення за підрозділами підприємства обов’язків щодо формування інформаційних потоків та вибору відповідних методів оцінки ефективності логістичної діяльності.

У ПрАТ «Оболонь» впроваджено систему електронного документообігу «BAS Документообіг КОРП».

Система «BAS Документообіг КОРП» разом із широким набором додаткових модулів являє собою бізнес-рішення, спрямоване на ефективне вирішення самого широкого кола завдань роботи з електронними документами.

Система підтримує повний життєвий цикл документа в організації від створення проєкту документа до списання в справу й передачі в архів.

Функціонал підготовки документів дозволяє автоматизувати весь процес створення документа. Робота з проєктами документів має на увазі виконання наступних дій:

– створення реєстраційно-контрольна картка проєкту документа, у тому числі і «на виконання» розпорядницького документа;

– зміна проєкту зі збереженням попередніх версій;

– узгодження проєкту документа;

– затвердження проєкту документа;

– реєстрація документа, створеного на основі проєкту.

При роботі із проєктом виконується послідовна або паралельна маршрутизація, контролюються строки розгляду і строк підготовки проєкту в цілому.

Реєстрація і введення документів в систему. Для того щоб документ потрапив в систему, він повинен бути зареєстрований. При реєстрації формується реєстраційно-контрольна картка документа, в яку заносяться відомості про документ, і йому присвоюється реєстраційний номер. Реєструються як документи, що надійшли ззовні, так і створені всередині банку: листи, накази, договори, акти.

Система дозволяє в автоматизованому режимі реєструвати передані електронною поштою документи, в тому числі підписані електронним цифровим підписом.

Файли вихідних і внутрішніх документів за стандартною технологією можуть бути прикріплені до реєстраційно-контрольної картки. Для документів, які готуються в MS Word, реалізована спрощена процедура реєстрації прямо із середовища редактора.

У системі «BAS Документообіг КОРП» реалізоване поняття проєктів документів і підтриманий повний цикл роботи з проєктами: створення реєстраційно-контрольної картки проєкту документа, в тому числі й «на виконання» розпорядницького документа; зміна проєкту зі зберіганням попередніх версій; узгодження проєкту документа; затвердження проєкту документа; реєстрація документа, створеного на основі проєкту.

Для роботи з проєктами використовується спеціальний тип реєстраційної картки, що містить перелік посадових осіб, які візують та підписують проєкт, і маршрут візування. Виконавець проєкту документа може аналізувати хід візування й підписання проєкту.

Посадові особи, яким документ направлений на візування, можуть завізувати його, висловити свої зауваження й/або внести їх у файл документа. Для важливих документів факт візування може засвідчуватися персональним електронним цифровим підписом посадової особи.

Системою підтримується версійність проєктів документів. На будь-якій стадії узгодження проєкту можна призупинити роботу з поточним варіантом і на основі зауважень до нього створити новий. Історія роботи з варіантами проєкту документа може бути збережена.

При реєстрації погодженого й підписаного проєкту як внутрішнього або вихідного його реєстраційно-контрольна картка автоматично створюється на основі реєстраційної картки проєкту.

Переваги системи «BAS Документообіг КОРП»:

– Автоматизація: Система надає можливість автоматизувати весь процес документообігу. Вона дозволяє створювати, редагувати, зберігати та відстежувати документи, що спрощує роботу з ними.

– Зручність в користуванні: Система має інтуїтивно зрозумілий інтерфейс, що спрощує процес роботи з нею. Вона також надає можливість швидкого пошуку і сортування документів.

– Безпека: Система забезпечує високий рівень безпеки документів. Вона має можливість обмеженої доступності для користувачів, а також автоматичне резервне копіювання і захист від втрати даних.

– Ефективність: Система дозволяє оптимізувати робочі процеси, зменшити час на пошук і обробку документів, що покращує продуктивність роботи.

Недоліки системи «BAS Документообіг КОРП»:

– Вартість: Реалізація та підтримка такої системи може бути дорогим процесом, особливо для невеликих підприємств.

– Необхідність навчання: Користувачам системи може знадобитись час на навчання та оволодіння її функціоналом, особливо якщо вони раніше не працювали з подібними системами документообігу.

– Залежність від програмного забезпечення: Використання системи може стати проблемою, якщо на робочому місці виникають проблеми з програмним забезпеченням або обладнанням.

– Обмежена гнучкість: У деяких випадках система може не задовольняти унікальні потреби підприємства, оскільки вона встановлена як стандартна програма зі своїм функціоналом.

Мінімальні вимоги до комплексу технічних засобів гарантують сталу роботу системи, але не гарантують зручність користування системою. Мінімальна конфігурація сервера баз даних визначається робочим навантаженням в системі. Рекомендовані параметри змінені в сторону покращення для підвищення швидкості роботи системи та адаптації під розміри бази даних (табл. 3.9-3.12).

Таблиця 3.9

Технічна платформа сервера СКБД

Параметр	Мінімальне значення	Рекомендоване значення
Операційна система	Будь-яка з рекомендованих для СКБД Oracle	Windows 2000 Server SP4
Процесор	Pentium III 800 Mhz	Dual Pentium IV 2.4 Ghz
Об’єм ОЗП	1 Gb	2 Gb
Дискові масиви	20 Gb RAID 0-5	80Gb Ultra Wide SCSI-2 RAID 0-10
Резервне копіювання	Наявність накопичувачів CDRW	

Джерело: складено автором

Таблиця 3.10

Технічна платформа сервера застосувань

Параметр	Мінімальне значення	Рекомендоване значення
Операційна система	Windows 2000 Professional SP4	Windows 2000 Server SP4
Процесор	Pentium III 800 Mhz	Dual Pentium IV 2.4 Ghz
Об’єм ОЗП	1 Gb	2 Gb
Дискові масиви	20 Gb	30 Gb
ЛОМ	мережевий адаптер LAN 100	мережевий адаптер LAN 1000

Джерело: складено автором

Таблиця 3.11

Технічна платформа клієнтського місця

Параметр	Мінімальне значення	Рекомендоване значення
Операційна система	Windows 2000 Professional SP4 або Windows Vista	
Процесор	Celeron II 600 Mhz	Celeron 1.7 Ghz
Об’єм ОЗП	256 Mb	512 Mb
Дискові масиви	1 Gb вільного простору	
ЛОМ	мережевий адаптер LAN 10/100 BaseTX	

Джерело: складено автором

Таблиця 3.12

Технічні вимоги до локальної обчислювальної мережі

Параметр	Рекомендоване значення
Швидкість	100 Mb/s
Протоколи	TCP/IP
Організація	Домен Windows NT або Active Directory

Джерело: складено автором

Програмне забезпечення згідно з поставленим завданням реалізоване за допомогою мов Java та SQL. Прототип програмного забезпечення в даній

роботі реалізовано засобами MS Access. Для програмування інтерфейсу використано мови VBA, а для створення запитів та звітів – мова SQL.

Інформація про фінансову діяльність ПрАТ «Оболонь»:

1. В електронному вигляді знаходиться в ПЕОМ головного бухгалтера.

Електронна база даних про постачальників:

1. В електронному вигляді знаходиться в ПЕОМ директора.

Для захисту інформаційних ресурсів організації використовується антивірусне ПЗ, остання дата оновлення баз – 1 квітня 2023 року. Інші засоби захисту (програмні, організаційні, технічні) не використовуються.

На думку керівництва організації порушниками ІБ можуть бути:

1. Окремі злочинні елементи з метою отримання конфіденційної інформації про постачальників аптеки для подальшого їх переманювання конкурентами або інших протиправних дій.

2. Конкуруючі організації з метою прибрати цю організацію з ринку послуг.

У Додатку А табл. 1-3 модель зовнішнього, внутрішнього порушників та ненавмисні загрози компанії.

У табл. 3.13 наведено перелік загроз, які впливають на існуючі уразливості ресурсів організації.

Таблиця 3.13

Перелік загроз, які впливають на існуючі вразливості ресурсів ПрАТ «Оболонь»

Ресурс	Загрози	Вразливості
Інформація по постачальникам (ПЕОМ директора)	Витік інформації мережевим каналом	Спуфінг мережі
		Фішингові ресурси
	Витік інформації візуально-оптичним каналом	Використання камер
		Використання закладок
		Використання апаратури для прослуховування

Продовження табл. 3.13

Ресурс	Загрози	Вразливості
Інформація по постачальникам (озвучування в кабінеті директора)	Витік акустичним каналом	Жучки
		Використання направлених мікрофонів за межами КЗ
	Витік по віброакустичному каналу	Підслуховування через вібрацію архітектурно технічних систем
		Лазерні віброакустичні пристрої націлені на вікна
	Акустоелектричні технічні канали	Підключення до телефонної ліній
Інформація по постачальникам (ПЕОМ бухгалтера)	Витік візуально-оптичним каналом	Використання камер
	Зняття побічних ел-маг випромінюваннь	Використання апаратури для зняття через випромінення монітору
Інформація щодо фінансової діяльності (ПЕОМ бухгалтера)	Витік візуально-оптичним каналом	Використання камер
	Використання переносних носіїв	Заражені флеш карти

Джерело: складено автором

У табл. 3.14 наведено ступінь впливу існуючих загроз на уразливості ресурсів ПрАТ «Оболонь».

Таблиця 3.14

Ступінь впливу існуючих загроз на уразливості ресурсів аптеки

Загроза /Вразливість	Імовірність реалізації загрози через дану уразливість протягом року, P (V)	Критичність реалізації загрози через уразливість, ER
Ресурс 1. Інформація по постачальникам (ПЕОМ директора)		
Витік інформації мережевим каналом / Спуфінг мережі	0,5	0,8
Витік інформації мережевим каналом / Фішингові ресурси	0,6	0,7
Витік інформації візуально-оптичним каналом / Використання камер	0,6	0,6
Витік інформації візуально-оптичним каналом / Використання закладок	0,7	0,2

Продовження табл. 3.14

Загроза /Вразливість	Імовірність реалізації загрози через дану уразливість протягом року, P (V)	Критичність реалізації загрози через уразливість, ER
Витік інформації візуально-оптичним каналом / Використання апаратури для прослуховування	0,5	0,4
Ресурс 2. Інформація по постачальникам (озвучування в кабінеті директора)		
Витік акустичним каналом / Жучки	0,6	0,5
Витік акустичним каналом / Використання направлених мікрофонів за межами КЗ	0,7	0,4
Витік по віброакустичному каналу / Підслуховування через вібрацію архітектурно технічних систем	0,4	0,4
Витік по віброакустичному каналу / Лазерні віброакустичні пристрої націлені на вікна	0,2	0,3
Акустоелектричні технічні канали / Підключення до телефонної ліній	0,3	0,4
Ресурс 3. Інформація по постачальникам (ПЕОМ бухгалтера)		
Витік візуально-оптичним каналом/ Використання камер	0,7	0,6
Зняття побічних ел-маг випромінюваннь / Використання апаратури для зняття через випромінення монітору	0,7	0,8
Ресурс 4. Інформація щодо фінансової діяльності (ПЕОМ бухгалтера)		
Витік візуально-оптичним каналом / Використання камер	0,6	0,6
Використання переносних носіїв / Заражені флеш карти	0,7	0,8

Джерело: складено автором

Далі проводимо розрахунок рівня загрози по уразливості Th на основі використання формули:

$$Th_{c,I,a} = \frac{ER_{c,I,a}}{100} \times \frac{P(V)_{c,I,a}}{100}. \quad (3.7)$$

$ER_{c,I,a}$ – критичність реалізації загрози;

$P(V)_{c,I,a}$ – ймовірність реалізації загрози.

Для розрахунку рівня загрози CTh по всім вразливостям, через які реалізується дана загроза, використаємо формулу:

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th) \quad (3.8)$$

Результати розрахунків занесемо до табл. 3.15.

Таблиця 3.15

Відношення рівня загрози по уразливості Th на основі критичності і ймовірності реалізації загрози

Загроза/вразливість	Рівень загрози, Th $Th_{c,I,a} = \frac{ER_{c,I,a}}{100} \times \frac{P(V)_{c,I,a}}{100}$	Рівень загрози по всім вразливостям, через які реалізується дана загроза, CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$
Ресурс 1. Інформація по постачальникам (ПЕОМ директора)		
Витік інформації мережевим каналом / Спуфінг мережі	0,4	0,82
Витік інформації мережевим каналом / Фішингові ресурси	0,42	
Витік інформації візуально-оптичним каналом / Використання камер	0,36	0,4
Витік інформації візуально-оптичним каналом / Використання закладок	0,14	
Витік інформації візуально-оптичним каналом / Використання апаратури для прослуховування	0,2	0,2
Ресурс 2. Інформація по постачальникам (озвучування в кабінеті директора)		
Витік акустичним каналом / Жучки	0,3	0,58
Витік акустичним каналом / Використання направлених мікрофонів за межами КЗ	0,28	
Витік по віброакустичному каналу / Підслуховування через вібрацію архітектурно технічних систем	0,16	0,22

Продовження табл. 3.15

Загроза/вразливість	Рівень загрози, Th $Th_{c,I,a} = \frac{ER_{c,I,a}}{100} \times \frac{P(V)_{c,I,a}}{100}$	Рівень загрози по всім вразливостям, через які реалізується дана загроза, CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$
Витік по віброакустичному каналу / Лазерні віброакустичні пристрої націлені на вікна	0,06	
Акустоелектричні технічні канали / Підключення до телефонної ліній	0,12	0,12
Ресурс 3. Інформація щодо фінансової діяльності (ПЕОМ бухгалтера)		
Витік візуально-оптичним каналом / Використання камер	0,36	0,36
Використання переносних носіїв / Заражені флеш карти	0,56	0,56

Джерело: складено автором

Формула для розрахування загального рівня загроз CThR, діючих на заданий ресурс:

$$CThR = 1 - \prod_{i=1}^{n}(1 - CTh) \quad (3.9)$$

Розрахунки занесемо до табл. 3.16.

Таблиця 3.16

Загальний рівень загроз CThR, діючий на заданий ресурс

Загроза/вразливість	Рівень загрози по всім вразливостям, через які реалізується дана загроза, CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$	Загальний рівень загроз CThR, діючий на заданий ресурс $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$
Ресурс 1. Інформація по постачальникам (ПЕОМ директора)		
Витік інформації мережевим каналом / Спуфінг мережі	0,82	0,86
Витік інформації мережевим каналом / Фішингові ресурси		

Продовження табл. 3.16

Загроза/вразливість	Рівень загрози по всім вразливостям, через які реалізується дана загроза, CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$	Загальний рівень загроз CThR, діючий на заданий ресурс $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$
Витік інформації візуально-оптичним каналом / Використання камер	0,4	
Витік інформації візуально-оптичним каналом / Використання закладок		
Витік інформації візуально-оптичним каналом / Використання апаратури для прослуховування	0,2	
Ресурс 2. Інформація по постачальникам (озвучування в кабінеті директора)		
Витік акустичним каналом / Жучки	0,58	0,65
Витік акустичним каналом / Використання направлених мікрофонів за межами КЗ		
Витік по віброакустичному каналу / Підслуховування через вібрацію архітектурно технічних систем	0,22	
Витік по віброакустичному каналу / Лазерні віброакустичні пристрої націлені на вікна		
Акустоелектричні технічні канали / Підключення до телефонної ліній	0,12	
Ресурс 3. Інформація щодо фінансової діяльності (ПЕОМ бухгалтера)		
Витік візуально-оптичним каналом / Використання камер	0,36	0,69
Використання переносних носіїв / Заражені флеш карти	0,56	

Джерело: складено автором

Розраховуємо ризик по кожному ресурсу, для цього розрахунку використовується наступна формула:

$$R = CThR \times D \tag{3.10}$$

Критичність ресурсу D , наведено в таблиці 3.17.

Таблиця 3.17

Критичність ресурсів ПрАТ «Оболонь»

Ресурс	Значення (Грн)
Ресурс 1. Інформація про постачальників (Електронна база)	1000 000
Ресурс 2. Інформація про постачальників (озвучування в кабінеті директора)	900 000
Ресурс 3. Інформація щодо фінансової діяльності організації	250 000

Джерело: складено автором

Результати розрахунків ризиків ресурсу R наведемо у таблиці 3.18.

Таблиця 3.18

Ризики для об’єднаних ресурсів

Ресурс	Загальний рівень загроз по заданому ресурсу, CThR $CThR_1 = 1 - \prod_{i=1}^{n}(1 - CThR)$	Ризик ресурсу, грн $R = CThR_1 \times D$
Ресурс 1. Інформація по клієнтам (Електронна база)	0,86	860000
Ресурс 2. Інформація по клієнтам (озвучування в кабінеті директора)	0,65	585000
Ресурс 3. Інформація щодо фінансової діяльності організації	0,69	172500

Джерело: складено автором

Розрахунок ризику по інформаційній системі CR за формулою:

$$CR = \sum_{i=1}^{n} R \tag{3.11}$$

Результат розрахунків ризику по інформаційній системі CR в ПрАТ «Оболонь» дорівнює1617500 грн.

У ході проведення дослідження шляхом опитування користувачів комп'ютерних систем на підприємстві ПрАТ «Оболонь» вдалося виявити рівень компетентності користувачів та визначено актуальні уразливості та загрози від атак методами соціальної інженерії. Результати проведеного опитування дозволили зробити висновок, що найкращим захистом комп'ютерних мереж підприємства є ознайомлення співробітників з видами загроз і навчання способам протидії загрозам методами соціальної інженерії.

Для реалізації такого підходу підготовлено добре структуровані інформаційно-довідкові матеріали та певні питання, за якими передбачається проводити навчання та підготовку персоналу комп'ютерних систем. Результати опитування використано під час підготовки інформаційно-довідкових матеріалів та питань для реалізації блоку контролю результатів тестування у розробці навчальної системи протидії атакам методами соціальної інженерії.

У процесі опитування з'ясувалося, з якими загрозами соціальної інженерії стикався персонал комп'ютерних систем і проводився відбір найбільш значних ситуацій з метою використання в розробці навчальної системи. Було опитано 28 осіб, які мають доступ до комп'ютерної мережі, а також спеціалісти центру цифрового розвитку. Нижче наводиться відсоткове співвідношення актуальності деяких загроз, що розглядаються у процесі опитування.

Найбільш високий відсоток за результатами опитування отримала загроза, у реалізації якої зловмисник є іншою особою. Це питання набрало майже 85%. З цією ситуацією співробітники стикалися у службовий час, коли дзвонили конкуренти і зверталися з деякими проханнями.

Наступним із найпоширеніших питань стало питання, з яким стикалися опитувані співробітники, було питання про отримання якоїсь шуканої інформації під час роботи у пошукових системах. Користувачі стикалися із сайтами, призначеними для розкрадання паролів з вимогами авторизації. Це питання набрало 73% з усіх опитуваних. З питанням про злам електронної

пошти стикалися близько 53% опитуваних. При розгляді цього питання обговорено рекомендації про те, що можна надсилати електронною поштою, а що не можна і як поводитися при отриманні незнайомого листа.

Наступними рівними за відсотками, 45% стали питання, пов’язані з покупками в Google Play, критеріями злому особистої поштової скриньки та ціла низка інших ситуацій, які є по суті атаками методами соціальної інженерії, з якими зустрічалися співробітники.

3.2. Огляд реалізації захисту від атак реалізованих за допомогою соціальної інженерії

Щоб розробити ефективну навчальну систему протидії атак методами соціальної інженерії необхідно провести огляд реалізації захисту атак від методів соціальної інженерії та розглянути найефективніші способи захисту.

І якщо розглядати поняття захисту від проникнення якихось шкідливих атак шахраїв чи зловмисників, можна сміливо говорити, що без комбінованої чи комплексної роботи у цьому напрямі не обійтися. Даний захист звичайно передбачає різні методи перевірки інформації, що надходить, такі як автоматичні і звичайно ж ручні. Розглядаючи у цьому параграфі реалізацію захисту від атак соціальної інженерії. З усього вищесказаного в нашій випускній кваліфікаційній роботі стає зрозумілим, що найуразливішою ланкою є, звичайно ж, людина.

Людина відповідно користується та володіє інформацією різного роду, в тому числі і конфіденційного характеру, людські дії за природою неможливо запрограмувати, тому зловмисники не втрачають такої можливості, як атакувати людину методами та прийомами соціальної інженерії.

Соціальна інженерія має в своєму розпорядженні низку прийомів і методів, які дуже добре знайомі зловмисникам і якими вони дуже добре володіють і в комбінуванні з технічними засобами, непомітно підбираються до людини, яка по суті буде користувачем будь-яких мереж, а відповідно

отримують від цих дій якусь цінну інформацію чи фінансову вигоду. Як правило, зловмисники використовують психологічні маніпуляції граючи на людських слабостях.

Різні компанії замислюються, як цьому протистояти. Насправді звичайно існує деякі методики протидії соціальної інженерії, одна з якої є однозначним проведенням семінарських занять або проведення навчання співробітників компаній, основ протидії соціальної інженерії та підвищення інформаційної безпеки компаній.

3.3. Реалізація навчальної системи протидії атакам на основі методів соціальної інженерії

3.3.1. Реалізація інформаційно-довідкового блоку

Основним захистом або протидією атак соціальної інженерії в даний час є навчання співробітників, їх ознайомлення з основними методами та прийомами соціальних хакерів. З урахуванням результатів дослідження було ухвалено рішення про створення навчальної системи протидії атакам методами соціальної інженерії під назвою «Сігма1», за допомогою якої з’явиться можливість підвищити знання користувачів про інформаційну безпеку та протидіяти атакам соціальної інженерії.

Але без інформаційних складових це неможливо. У рамках виконання цієї роботи проведено дослідження в мережі Інтернет про скоєні злочини з використанням методів соціальної інженерії. З результатів проведеного дослідження вдалося зібрати найактуальніші питання, які будуть використовуватись у даній системі. Після цього розпочалася добірка технологій, які необхідні для використання при створенні даної інформаційно-довідкової системи. Початком розробки навчальної інформаційної системи став інформаційно-довідковий розділ.

Нами було створено Reference.svelte – сторінка з посиланнями на інформаційно-довідковий розділ, що містить наступні теми (рис. 3.3):

Рис. 3.3. Теми на сторінці з посиланнями Reference.svelte

Джерело: розроблено автором самостійно

3.3.2. Реалізація блоку тестування

Для формування інтерфейсу блоку тестування (Front-end), що є частиною проєкту і представляє набір спеціальних засобів, призначених для взаємодії між користувачем та функціями системи. У нашому випадку це взаємодія між програмною, апаратно-технічною складовою та людиною, для обміну даними та отримання відповідної інформації.

У Front-end увійшло: vite – система складання, svelte – компілятор; подібність react'a/vue, але не включений до кінцевого коду бібліотеки, тому що замість цього написаний розробником код перетворюється на кінцевий js-код, який виконується на сторінці (cyber-enhanced applications – за рахунок даних технологій прискорює процес розробки); tailwindcss – готовий набір CSS-класів з ідеології Atomic CSS; за фактом – це CSSframework.

Технології CSS та технології JS наведемо на рис. 3.2.

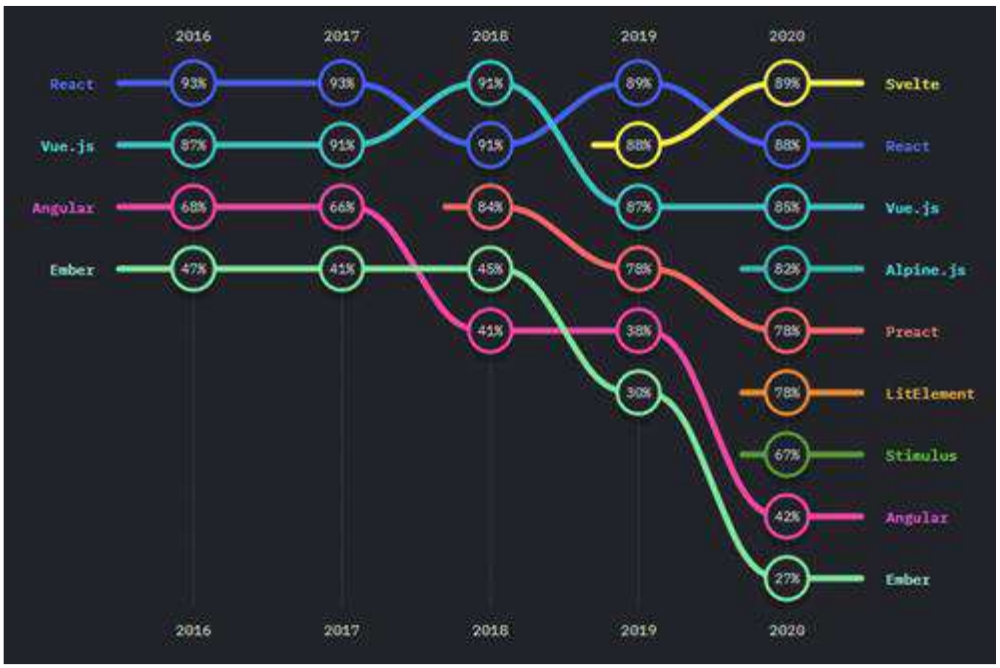

Рис. 3.2. Відсоток задоволеності, зацікавленості, використання, впізнаваності

Джерело: розроблено автором самостійно

І так основними компонентами, які наш компілятор svelte перетворює на продуктивний імперативний код є:

Menu.svelte – меню сайта;

MenuMobile.svelte – меню сайта для мобільних пристроїв;

MenuDesktop.svelte – меню сайта для ПК;

DesktopItem.svelte – елемент меню для ПК;

MobileItem.svelte – елемент меню для мобільних пристроїв;

Footer.svelte – нижня частина сайта.

Усі сторінки сайту містять Menu та Footer. Content.svelte – сторінка content.html сайту, яка містить:

1. CategoryItem.svelte – категорія навчання (пошта, акаунти тощо), паролі та облікові записи.

2. AccountsCategoryDescription.svelte – докладний опис категорії «Акаунти».

3. EmailCategoryDescription.svelte – докладний опис категорії «Пошта».

І так електронна пошта, на сьогоднішній день є у всіх користувачів для розсилки будь-якої інформації, причому особиста електронна пошта багатьма користувачами використовується замість робочої службової адреси. Тому не варто забувати, що електронна пошта, по суті, є золотим ключиком до величезної кількості інформації. І зловмисники, усвідомлюючи це в першу чергу, будуть робити різні спроби зламати поштову скриньку.

Тому при створенні цієї програми було так само поставлене це питання, що може дати компанії вивчення цієї теми. А відповідь як завжди виявлялася дуже простою, при вивченні співробітниками даної теми знизиться ризик злому поштових скриньок, а відповідно і втрати інформації, зокрема конфіденційної, а найголовніше, знизиться ризик зараження шкідливим програмним забезпеченням всієї мережі компанії. Тому була зроблена Test.svelte – сторінка test.html сайту ControlPanel.svelte – сторінка control_panel.html сайту EmailLesson1.svelte.. EmailLesson5.svelte – сторінки теорій категорії навчання «Пошта» AccountsLesson1.svelte.. AccountsLesson6.svelte – «Акаунти». Так кінцевими точками API Endpoints в нас стало /api2/register – реєстрація користувача:

Request:

```
type apiRegisterReq struct {
Email string `json:"email,omitempty"`
Pass string `json:"pass,omitempty"`
Lang string `json:"lang,omitempty"`
}
```

/api2/auth – авторизація користувача:

Request:

```
type apiAuthReq struct {
Email string `json:"email,omitempty"`
Pass string `json:"pass,omitempty"`
}
```

/api2/get_category_info – отримання інформації про категорію навчання:

Request:

type apiGetCategoryInfoRequest struct {

Name string `json:"name"`

}

Response:

type apiGetCategoryInfoRow struct {

Title string `json:"title"`

QuestionCount int `json:"questionCount"`

}

/api2/get_question_info – отримання інформації про питання тесту:

Request:

type apiGetQuestionInfoRequest struct {

QuestionNumber int `json:"questionNumber"`

CategoryName string `json:"categoryName"`

}

Response:

type apiGetQuestionInfoRow struct {

Title string `json:"title"`

CorrectCount int `json:"correctCount"`

}

/api2/get_question_variants – отримання варіантів відповіді на питання тесту:

Request:

type apiGetQuestionVariantsRequest struct {

QuestionNumber int `json:"questionNumber"`

CategoryName string `json:"categoryName"`

}

Response: масив з елементів наступного виду:

type apiGetQuestionVariantsRow struct {

Id int `json:"id"`

Text string `json:"text"`

}

/api2/answer_question – відповісти на питання:

Request:

type apiAnswerQuestionRequest struct {

CategoryName string `json:"categoryName"`

QuestionNumber int `json:"questionNumber"`

UserAnswer []int `json:"userAnswer"`

}

Response:

struct {

Success bool

}

Таблиця user – включає інформацію про користувачів сайту. Має наступний вигляд:

[id] [int] IDENTITY(1,1) NOT NULL,

[email] [nvarchar](200) NOT NULL,

[pass] [nvarchar](200) NOT NULL,

[confirmation_link] [nvarchar](200) NOT NULL,

[end_payment_date] [datetime2](7) NOT NULL,

[email_is_valid] [bit] NOT NULL,

[load_date] [datetime2](7) NOT NULL,

[update_date] [datetime2](7) NULL,

[lang] [nvarchar](10) NOT NULL,

[restore_email_link] [nvarchar](30) NOT NULL,

[restore_link_valid] [bit] NOT NULL,

[restore_link_valid_till] [datetime2](7) NULL,

Таблиця token – включає інформацію про токіни користувачів сайту. Має наступний вигляд:

[value] [nvarchar](200) NOT NULL,

[pass] [nvarchar](200) NOT NULL,

[user_id] [int] NOT NULL,

[expires_in] [datetime2](7) NULL,

[load_date] [datetime2](7) NOT NULL,

[update_date] [datetime2](7) NULL,

Таблиця test_category – категорії/теми тестів. Має вигляд:

id int identity(1,1) primary key not null,

title nvarchar(300) not null,

little_name nvarchar(300) not null

Таблиця question – зберігає питання тестів. Має наступний вигляд:

id int identity(1,1) primary key not null,

title nvarchar(2000) not null,

test_category_id int not null references test_category(id),

order_num int not null,

Таблиця question_variants – зберігає відповіді на питання до тестів. Має наступний вигляд:

id int identity(1,1) primary key not null,

question_id int not null references question(id),

[text] nvarchar(2000) not null,

is_correct bit not null

Таблиця answer – зберігає відповіді користувачівна питання до тестів. Має наступний вигляд:

id int identity(1,1) primary key not null,

[user_id] int not null references [user](id),

question_id int not null references question(id),

user_answer nvarchar(50) not null,

Основним функціоналом сайту є можливість проходження користувачем тестів.

При відкритті сторінки test.html користувач побачить (якщо встигне) напис:

«Завантаження...». Змінні компоненти Test ініціалізуються в наступні значення:

```
interface TResult {
rightAnswersCount: number;
allQuestionsCount: number;
rightAnswersPercent: number;
passLevel: number;
isPassed: boolean;
}
let categoryLittleName = getCategory();
let categoryTitle = 'Загрузка...';
let questionCount = 0;
let showResult = false;
let result: TResult
interface TQuestionInfo {
title: string;
correctCount: number;
};
interface TQuestionVariant {
id: number;
text: string;
};
48
let question: {
num: number,
info: TQuestionInfo,
variants: TQuestionVariant[],
radioAnswer: number,
checkboxAnswer: number[],
} = null;
```

Інтерфейси TResult, TQuestionInfo, TQuestionVariant описують типи даних деяких змінних. Це можливо завдяки використанню TypeScript усередині svelte компонентів. Перевагою використання статичної типізації є ретельніша перевірка коду без необхідності його виконання.

Щоб дізнатися назву тесту, який бажає пройти користувач, використовується функція getCategory():

```
function getCategory() {
const urlParams = new URLSearchParams(window.location.search);
const category = urlParams.get('category');
return category;
}
```

Як видно, ця функція зчитує значення параметра категорії з URL-адреси. А потім, за допомогою функції setCategoryInfo завантажується інформація про тему тесту та кількість питань у тесті:

```
async function setCategoryInfo(categoryLittleName) {
try {
const categoryInfo = await post('/api2/get_category_info', {
name: categoryLittleName,
});
categoryTitle = categoryInfo.title;
questionCount = categoryInfo.questionCount;
} catch (ex) {
console.log(ex);
alert(ex.message);
}
}
```

Що відразу відобразиться всередині сторінки.

Коли користувач натискає кнопку «почати тест», викликається функція start(): async function start() {

```
async function start() {
await getQuestion(categoryLittleName, 1);
}
```

Як видно, ця функція викликає функцію getQuestion(), яка отримує інформацію про питання №1 для тесту, ім’я якого вказано у параметрі категорії URL-адреси.

```
async function getQuestion(categoryLittleName, questionNumber) {
const req = {
questionNumber: questionNumber,
categoryName: categoryLittleName,
};
try {
const questionInfo: TQuestionInfo = await
post('/api2/get_question_info', req);
const questionVariants: TQuestionVariant[] = await
post('/api2/get_question_variants', req);
question = {
num: questionNumber,
info: questionInfo,
variants: questionVariants,
radioAnswer: -1,
checkboxAnswer: [],
};
} catch (ex) {
alert(ex.message);
}
}
```

Видно, що функція getQuestion() по черзі виконує 2 запити до сервера:

1. /api2/get_question_info – отримання самого питання;
2. /api2/get_question_variants – отримання варіантів відповіді на питання.

Після чого отримана інформація збирається і записується в змінну quest компонента Test і негайно відображається. У разі виникнення помилки, користувачу про неї повідомляється шляхом появи інформаційного повідомлення з описом помилки.

При натисканні «відповісти» викликається функція answer():

```
async function answer() {
let answer: number[] = [];
if (question.info.correctCount === 1) {
answer = [question.radioAnswer];
} else {
answer = question.checkboxAnswer;
}
const req = {
categoryName: categoryLittleName,
questionNumber: question.num,
userAnswer: answer,
};
try {
await post('/api2/answer_question', req);
} catch (ex) {
alert(ex.message);
return;
}
if (question.num >= questionCount) {
await getTestResult();
} else {
await getQuestion(categoryLittleName, question.num + 1);
}
}
```

Видно, що ця функція збирає відповідь користувача в змінну answer і передає цю відповідь на сервер за допомогою запиту /api2/answer_question, після чого у випадку, якщо це було останнє питання тесту, викликається функція getTestResult(), яка відображає результат проходження тесту, а якщо це не останнє питання тесту, викликається вже знайома нам функція getQuestion() для отримання наступного питання.

3.3.3. Реалізація блоку контролю результатів тестування

/api2/get_test_result – отримати результат тестування

type apiGetTestResultRequest struct {

CategoryName string `json:"categoryName"`

}

Response:

type apiGetTestResultRow struct {

RightAnswersCount int `json:"rightAnswersCount"`

AllQuestionsCount int `json:"allQuestionsCount"`

RightAnswersPercent int `json:"rightAnswersPercent"`

PassLevel int `json:"passLevel"`

IsPassed bool `json:"isPassed"`

}

Тут:

RightAnswersCount – кількість вірних відповідей при проходженні тесту;

AllQuestionsCount – загальна кількість питань у тесті;

RightAnswersPercent – кількість вірних відповідей, виражена у відсотках;

PassLevel – мінімальний прохідний бал;

IsPassed – чи пройдено тест успішно;

/api2/get_control_panel_results – отримати результати тестування всіх користувачів;

Request: порожній

Response: масив з елементами такого виду:

```
type apiGetControlPanelResultsRow struct {
Email string `json:"email"`
TestTheme string `json:"testTheme"`
RightAnswersCount int `json:"rightAnswersCount"`
AllQuestionsCount int `json:"allQuestionsCount"`
RightAnswersPercent int `json:"rightAnswersPercent"`
IsPassed bool `json:"isPassed"`
}
```

Властивості трактуються аналогічно до попереднього запиту, але на додаток містять:

Email – адреса електронної пошти тестованого;

TestTheme – найменування тесту, про яке йдеться в елементі відповіді (response'a);

Контроль результатів (рис. 3.3):

Результати

Пошта співробітника	Тема тесту	Правильних відповідей	Всього питань	Відсоток правильності відповідей	Підсумок
123@gmail.com	Електронна пошта	14	15	93	Здав
123@gmail.com	Електронна пошта	3	9	33	Не здав
123@gmail.com	Електронна пошта	15	15	100	Здав
123@gmail.com	Електронна пошта	3	9	33	Не здав

Рис. 3.3. Контроль результатів

Джерело: розроблено автором самостійно

Таким чином пройшовши тест, результат цього проходження фіксується і подальшій модифікації питань до тестів та інших подібних елементів, що не призведуть до зміни результату проходження тесту.

3.4. Практичне застосування (тестування) навчальної системи для персоналу компанії

Розроблену навчальну систему «Сігма-1» протестували на співробітниках підприємства ПрАТ «Оболонь».

Крім того, зазначено, що дана система дозволяє після навчання співробітників ПрАТ «Оболонь» мобілізувати їхню увагу і відповідно не дозволить стати жертвою соціальної інженерії. Так само було зазначено, що дана система з урахуванням проведеного дослідження дуже актуальна сьогодні і просто необхідна, у зв’язку з тим, що дуже часто, заняття проводяться в дистанційному режимі через вжиті заходи воєнного стану і співробітники відповідно передають інформацію через Інтернет, користуючись електронною поштою.

3.5. Аналіз результатів тестування, висновки

Продовжуючи це дослідження, знову звернулися до 28 осіб, які брали участь в опитуванні щодо визначення актуальних загроз та уразливостей атак методами соціальної інженерії. Всі ці співробітники пройшли тест на нашій системі.

За результатами тестування виробничий та технологічний відділи ПрАТ «Оболонь» набрали приблизно по 10 відсотків правильних відповідей.

У відділі комерції та електронних продажів 70% співробітників відповіли вірно. Це можливо пояснюється тим, що співробітники комерційного відділу регулярно стикаються з порушеннями у сфері соціальної інженерії. Звідси напрошується висновок, що систематичні заняття в галузі навчання співробітників сприятиме підвищенню рівня захищеності інформаційної безпеки від атак методами соціальної інженерії.

ВИСНОВКИ

Соціальна інженерія на підприємстві це використання психологічних та соціальних методів для впливу на співробітників або клієнтів з метою

досягнення певних цілей організації. Це може включати вплив на мотивацію співробітників, створення сприятливого робочого середовища, підвищення продуктивності або збільшення відвідуваності клієнтами. Соціальна інженерія може бути використана як у позитивних, так і у негативних цілях, тому важливо ретельно розглядати її методи та наслідки.

Соціальна інженерія – це різні способи і методи маніпуляції людьми з метою отримання якоїсь інформації, що може зацікавити шахраїв або зловмисників, з використанням знань людського стану або психіки. Основним завданням зловмисників буде отримання доступу до інформації, використовуючи не програми злому, а довірливість людей, користувачів, як правило різних сервісів.

Для впливу на людину соціальні інженери використовують численні і різноманітні техніки і методики психологічного впливу. Зупиняючись на атаках соціальної інженерії, стає ясно, що атаки впливають на рівень підсвідомості, так як в більшості злочинів потерпілі чули про такий або подібний вид шахрайства. Ці знання важливі для подальшого запобігання від дії атак соціальної інженерії.

Всі класифікації атак соціальної інженерії спрямовані на те, щоб людина, на яку впливає зловмисник, добровільно повідомила інформацію, яка буде представляти якийсь інтерес і якою можна буде користуватися. Не варто забувати, що зловмисник може видати себе за кого завгодно, попередньо зібравши інформацію про об’єкт своєї атаки – через соціальні мережі, або за допомогою результатів різних інтернет-опитувань, придбання інформації у недобросовісних компаній тощо. Такий прийом отримав назву «претекстинг», коли зловмисник заздалегідь зібрав максимальну інформацію про об’єкт, щоб не викликати у нього підозри. І тут все дії зловмисника засновані на створенні довірчих відносин і досягнення довіри у об’єкта атаки. І так як правило зловмисники представляються співробітниками, банків або ж біржовими гравцями і намагаються отримати максимальну інформацію у довірливих осіб.

З урахуванням вищесказаного, щоб не стати жертвою соціальної інженерії простим користувачам, а тим більше співробітникам компаній, необхідно дотримуватися простих правил: ніколи не слід відкривати електронні листи, від невідомих або сумнівних джерел; по закінченні робочого дня необхідно завжди відключати комп'ютерну техніку і ставити складні паролі для авторизації при включенні; мінімальним захистом комп'ютера повинна бути антивірусна програма, яка зможе убезпечити від деяких атак.

Визначення актуальних загроз та уразливостей від атак реалізованих за допомогою соціальної інженерії буде проводитися на підприємстві ПрАТ «Оболонь».

У ході проведення дослідження шляхом опитування користувачів комп'ютерних систем на підприємстві ПрАТ «Оболонь» вдалося виявити рівень компетентності користувачів та визначено актуальні уразливості та загрози від атак методами соціальної інженерії. Результати проведеного опитування дозволили зробити висновок, що найкращим захистом комп'ютерних мереж підприємства є ознайомлення співробітників з видами загроз і навчання способам протидії загрозам методами соціальної інженерії.

Для реалізації такого підходу підготовлено добре структуровані інформаційно-довідкові матеріали та певні питання, за якими передбачається проводити навчання та підготовку персоналу комп'ютерних систем. Результати опитування використано під час підготовки інформаційно-довідкових матеріалів та питань для реалізації блоку контролю результатів тестування у розробці навчальної системи протидії атакам методами соціальної інженерії.

У процесі опитування з'ясувалося, з якими загрозами соціальної інженерії стикався персонал комп'ютерних систем і проводився відбір найбільш значних ситуацій з метою використання в розробці навчальної системи. Було опитано 28 осіб, які мають доступ до комп'ютерної мережі, а також спеціалісти центру цифрового розвитку. Нижче наводиться відсоткове

співвідношення актуальності деяких загроз, що розглядаються у процесі опитування.

Найбільш високий відсоток за результатами опитування отримала загроза, у реалізації якої зловмисник є іншою особою. Це питання набрало майже 85%. З цією ситуацією співробітники стикалися у службовий час, коли дзвонили конкуренти і зверталися з деякими проханнями.

Наступним із найпоширеніших питань стало питання, з яким стикалися опитувані співробітники, було питання про отримання якоїсь шуканої інформації під час роботи у пошукових системах. Користувачі стикалися із сайтами, призначеними для розкрадання паролів з вимогами авторизації. Це питання набрало 73% з усіх опитуваних. З питанням про злам електронної пошти стикалися близько 53% опитуваних. При розгляді цього питання обговорено рекомендації про те, що можна надсилати електронною поштою, а що не можна і як поводитися при отриманні незнайомого листа.

Наступними рівними за відсотками, 45% стали питання, пов’язані з покупками в Google Play, критеріями злому особистої поштової скриньки та ціла низка інших ситуацій, які є по суті атаками методами соціальної інженерії, з якими зустрічалися співробітники.

Отже, в процесі виконання кваліфікаційної роботи була розроблена інформаційно-довідкова навчальна система «Сігма1», призначена для навчання користувачів комп’ютерних систем протидії атакам методами соціальної інженерії та контролю інформаційної безпеки компанії через спеціально підготовлені тести на проникнення.

При демонстрації роботи інформаційно-довідкової навчальної системи «Сігма1» керівництво деяких компаній висловили готовність до впровадження системи для навчання співробітників з метою підвищення інформаційної безпеки компаній.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Вітлінський В. В. Моделювання економіки : навч. посібник. Київ: КНЕУ, 2003. 408с.

2. Вітлінський В. В. Моделювання рейтингової оцінки вищого

навчального закладу. *Економічна кібернетика.* 2020. № 3-4. С. 64-73.

3. ДСТУ ISO/IEC 27032:2016. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). На заміну ДСТУ ISO/IEC 27032:2015 ; чинний від 2018-01-01. Вид. офіц. [Б. м. : б. в.], 2016.

4. Креативний менеджмент. Львів: Видавництво Львівської політехніки, 2010. 124 с.

5. Лисенко О. А. Класифікація бізнес процесів на промислових підприємствах: теоретичні аспекти. *Університетські наукові записки.* 2013. № 2. С. 190-197.

6. Мовчан Д. А. (2022), Віртуальна лабораторія для тестування співробітників організації щодо фішингових атак: пояснюв. зап. диплом. роботи магістра: 125 Кібербезпека. Київ, 64 с.

7. Національний стандарт України. Системи управління якістю. Вимоги (ISO 9001:2008, IDT). ДСТУ ISO 9001:2009. URL: http://www.plitka.kharkov.ua/certs/433_iso9001.pdf.

8. Національний стандарт України. Системи управління якістю. Основні положення та словник термінів (ISO 9000:2005, IDT). ДСТУ ISO 9000:2007. URL: http://dbn.at.ua/_ld/11/1128_432_iso9000-1-pdf

9. Офіційний сайт ПрАТ «Оболонь». URL: http://obolon.ua

10. Помазун О. М. Моделі та інформаційні технології підтримки прийняття рішень з управління бізнес-процесами підприємства: дис. на здобуття наукового ступеню к.е.н.. Київ, *Київський національний економічний університет імені Вадима Гетьмана*, 2016. С. 11-14

11. Пономаренко В. С. Теорія та практика моделювання бізнес-процесів: монографія. Харків: Вид. ХНЕУ, 2013. 244 с

12. Туранська О. С., Лисенко О. І. Захист інформації у безпроводових сенсорних мережах. «Проблеми телекомунікації»: одинадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-17) 18-21 квітня 2017 р., Київ: С. 420-422.

13. Туранська О. С., Петрова В. М. Керівні принципи та підходи до захисту інформації у безпроводових сенсорних мережах. «Проблеми телекомунікації»: дванадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-18) 16-20 квітня 2018 р., Київ: С. 383-385

14. Швиданенко Г. О. Оптимізація бізнес-процесів: навч. посіб. Київ: КНЕУ, 2012. 487 с.

15. Як здійснюються атаки з використанням соціальної інженерії? URL : https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/

16. Adam Kavon Ghazi-Tehrani & Henry N. Pontell. Phishing Evolves: Analyzing the Enduring Cybercrime, Victims & Offenders, 2021, pp. 316–342. DOI: 10.1080/15564886.2020.1829224.

17. Ankit Kumar Jane, B. B. Gupta. A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems, 2021, pp. 527–565. DOI: 10.1080/17517575.2021.1896786.

18. ARIS Express. URL: http://compress.ru/Article.aspx?id=21780.

19. Gophish – Open Source Phishing Framework. Gophish – Open Source PhishingFramework. URL : https://getgophish.com/

20. Hong J. Why have there been so mane security breaches recently? CACM. 2011. URL : https://www.researchgate.net/deref/http%3A%2F%2Fcacm.acm.org%2Fblogs%2Fblogcacm%2F107800-why-have-there-been-so-many-security-breachesrecently%2Ffulltext.

21. Introduction and Support Package: Guidelines on the Process Approach to quality management systems (ISO 9000). ISO/TC 176/SC 2/N 544R. 2015.

22. Npcap.com: офіц. сайт для встановлення утиліт. URL: https://nmap.org/npcap/

23. Oracle VM VirtualBox Oracle VM VirtualBox. URL : https://www.virtualbox.org/

24. Security Awareness Training | KnowBe4.Security Awareness Training / KnowBe4. URL: https://www.knowbe4.com.

25. Snort.org: офіц. сайт системи виявлення та запобігання вторгнень. URL: https://www.snort.org/

26. Social Engineering in Kali Linux – javatpoint. URL: https://www.javatpoint.com/social-engineering-in-kali-linux

27. Vulnerability. System Science (HICSS), 2012 45th Hawaii International Conference on At: Maui, Hawaii. pp. 2366–2373. DOI:10.1109/HICSS.2012.657.

ДОДАТКИ

Додаток А

Таблиця 1

Модель зовнішнього порушника ПрАТ «Оболонь»

№	Тип порушника	Ймовірність наявності даного типа порушника для аптеки	Потенціал порушника	Мотивація порушника	Узагальнені можливості порушника
1	Спеціальні служби іноземних держав	Низька	Високий	Завдання збитків державі, сфері охорони здоров'я за допомогою отримання інформації про вітчизняних виробників медичних препаратів з подальшим використанням для інформаційної агресії проти держави.	Можливість самостійно створювати методи нападу, готувати та проводити атаки в контрольованій зоні з фізичним доступом до обладнання. Можливість залучення професіоналів із досвідом розробки та аналізу інтегрованих систем захисту інформації (включаючи фахівців у галузі аналізу лінійних сигналів передачі та компрометації електромагнітних випромінювань та індукцій). Можливість залучення фахівців з досвідом розробки та аналізу інтегрованих систем захисту інформації (включаючи фахівців у галузі використання незадокументованих можливостей прикладного програмного забезпечення для здійснення атак); Можливість залучення фахівців із досвідом розробки та аналізу інтегрованих систем захисту інформації (включаючи фахівців у галузі використання незадокументованих можливостей апаратних та програмних компонентів для функціонування систем захисту для здійснення атак);
2	Терористичні, екстремістські угруповання	Низька	середній	Завдання збитків державі, окремим її сферам діяльності	Можливість самостійно здійснювати створення методів атаки, підготовку

				або секторам економіки. Вчинення терористичних актів. Ідеологічні або політичні мотиви.	та проведення атак поза контрольованою зоною та у контрольованій зоні, але без фізичного доступу до обладнання. Можливість залучення професіоналів із досвідом розробки та аналізу інтегрованих систем захисту інформації (включаючи фахівців у галузі аналізу лінійних сигналів передачі та компрометації електромагнітних випромінювань та індукцій).
3	Злочинні групи (кримінальні структури)	Висока	низький	Отримання інформації про постачальників з подальшим використанням для злочинних дій (переманювання, дискредитація тощо), рейдерський захват приміщення	Здатність самостійно здійснювати створення методів нападу, підготовку та проведення атак лише за межами контрольованої зони (віддалені атаки через мережу з використанням доступних шкідливих програмних продуктів або злочинних сервісів), соціальна інженерія (шантаж, запугування).
4	Конкуруючі підприємства	Висока	середній	Дискредитація аптеки, Отримання інформації про постачальників з подальшим використанням для переманювання	Можливість самостійно здійснювати створення методів атаки, підготовку та проведення атак поза контрольованою зоною та у контрольованій зоні, але без фізичного доступу до обладнання. Можливість залучення професіоналів із досвідом розробки та аналізу інтегрованих систем захисту інформації (включаючи фахівців у галузі аналізу лінійних сигналів передачі та компрометації електромагнітних

					випромінювань та індукцій)
5	Розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів	Висока	середній	Заподіяння майнової шкоди шляхом обману або зловживання довірою. Ненавмисні, необережні або некваліфіковані дії	Здатність впровадження додаткових функціональних можливостей в програмне забезпечення або програмно-технічні засоби на етапі розробки.
6	Клієнти	висока	низький	Дискредитація аптеки внаслідок внутрішніх або зовнішніх мотивів. Отримання конфіденційної інформації для подальшого продажу.	Можливість самостійно здійснювати створення методів атаки, підготовку та проведення атак поза контрольованою зоною та у контрольованій зоні, але без фізичного доступу до обладнання
7	Колишні працівники	середня	середній	Дискредитація аптеки внаслідок внутрішніх або зовнішніх мотивів. Отримання конфіденційної інформації для подальшого використання у власних цілях.	Знають інформаційну структуру та порядок захисту інформаційних ресурсів в організації. Здатність самостійно здійснювати створення методів нападу, підготовку та проведення атак лише за межами контрольованої зони (віддалені атаки через мережу з використанням доступних шкідливих програмних продуктів або злочинних сервісів)
8	Зовнішні суб'єкти (фізичні особи)	Висока	низький	Ідеологічні або політичні мотиви. Заподіяння майнової шкоди шляхом шахрайства або іншим злочинним шляхом. Цікавість або бажання самореалізації (підтвердження статусу). Виявлення вразливостей з метою їх	Мають можливість отримати інформацію про уразливість інформаційної системи, яка опублікована в загальнодоступних джерелах. Здатність самостійно здійснювати створення методів нападу, підготовку та проведення атак лише за межами контрольованої зони (віддалені атаки через мережу з використанням доступних шкідливих програмних продуктів або злочинних сервісів)

				подальшого продажу і отримання фінансової вигоди	
9	Розробники програмного та технічного захисту	Середня	Високий	Бажання нашкодити існуючій інфраструктурі ІБ з метою розповсюдження власних розробок захисту ІБ підприємства	Знають інформаційну структуру та порядок захисту інформаційних ресурсів загалом. Мають можливість отримати інформацію про уразливість інформаційної системи, яка опублікована в загальнодоступних джерелах. Здатність самостійно здійснювати створення методів нападу, підготовку та проведення атак лише за межами контрольованої зони (віддалені атаки через мережу з використанням шкідливих програмних продуктів)

Таблиця 2

Модель внутрішнього порушника ПрАТ «Оболонь»

№	Посади, працівники яких можуть бути	Можливість порушення	Потенціал порушника	Тип (Мотивація) порушника	Узагальнені можливості порушника

	потенційними порушниками				
1	Директор	низька	високий	Халатний	Повний доступ до інформаційної системи
2	Головний бухгалтер	середня	високий	Халатний Маніпульований Ображений	Повний доступ до фінансових документів. Доступ до кабінету директора в його присутності.
3	Провізори	середня	середній	Халатний Маніпульований Ображений Нелояльний Підроблюючий Введений	Доступ до інформації щодо обороту в торгівлі лікувальними засобами. Доступ до складу медичних препаратів. Доступ до кабінету директора та головного бухгалтера в їх присутності.
4	Прибиральниця	Середня	середній	Халатний Маніпульований Ображений Нелояльний Підроблюючий Введений	Доступ до кабінету директора та головного бухгалтера до початку робочого дня для прибирання та в їх присутності. Не мають доступа до комп'ютерів.
5	Охоронці	Середня	Низький	Халатний Маніпульований Ображений Нелояльний Підроблюючий Введений	Доступ до кабінету директора та головного бухгалтера до початку робочого дня та в їх присутності. Не мають доступа до комп'ютерів.

Таблиця 3

Ненавмисні загрози компанії

№	Тип загрози	Потенційна можливість загрози

1.	Землетрус	низька
2	Втрата електроживлення	середня
3	Пожежа	середня