МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____20__ р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ ТА ЗАСОБИ ЇХ ПРОТИДІЇ

СТУДЕНТ: Рожко Владислав Геннадійович _____
(підпис)

КЕРІВНИК: к.держ.упр., доц. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 20__ р.

ЗАВДАННЯ

на дипломну роботу

студенту Рожку Владиславу Геннадійовичу

Тема роботи: «ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ ТА ЗАСОБИ ЇХ ПРОТИДІЇ», затверджена наказом по університету № 170 від «11» жовтня 2021 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 20___ р.
2. **Об'єкт дослідження:** забезпечення інформаційної безпеки банку.
3. **Предмет дослідження:** загрози інформаційній безпеці банку та засоби їх протидії.
4. **Мета дослідження** полягає у вивченні загроз інформаційній безпеці банку та засобів їх протидії.
5. **Перелік питань, які мають бути розроблені:**

5.1 Проаналізувати нормативно-правове забезпечення інформаційної безпеки банку в Україні.

5.2 З’ясувати види загроз інформаційній та кібербезпеці банку.

5.3 Дослідити засоби забезпечення інформаційної безпеки банківських установ.

6. **Дата видачі завдання** «16» вересня 2021 р.

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ В.Г. Рожко
підпис

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

студентом Рожком Владиславом Геннадійовичем

Дата видачі завдання: «16» вересня 2021 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	16.09.2021	
2.	Збір та аналіз літератури.	28.09.2021	
3.	Аналіз нормативно-правового забезпечення інформаційної безпеки банку.	12.10.2021	
4.	Встановлення видів загроз інформаційній безпеці банку.	26.10.2021	
5.	Дослідження засобів забезпечення інформаційної безпеки банківських установ.	09.11.2021	
6.	Формулювання висновків до роботи.	23.11.2021	
7.	Оформлення роботи.	07.12.2021	
8.	Оформлення презентації.	14.12.2021	
9.	Отримання рецензії на роботу.	24.12.2021	
10.	Захист у ДЕК.	__.01.2022	

Студент В.Г. Рожко

(підпис)

Науковий керівник Т.М. Мужанова

(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню загроз інформаційній безпеці банків та засобів їх протидії. Робота складається зі вступу, трьох розділів, що містять 10 рисунків та 2 таблиці, висновків та списку використаних джерел із 61 найменування. Загальний обсяг роботи становить 87 аркушів, 7 з яких займає список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки банку.

Предметом дослідження є загрози інформаційній безпеці банку та засоби їх протидії.

Метою роботи є вивчення загроз інформаційній безпеці банку та засобів їх протидії.

Для цього у роботі використані методи аналізу, синтезу, класифікацій та порівняння, оцінювання ризиків, вивчення нормативно-правової бази, а також підходів до навчання персоналу у сфері інформаційної безпеки.

Як результат у роботі проаналізовано нормативно-правове забезпечення інформаційної безпеки банку; з'ясовано види загроз інформаційній та кібербезпеці банку; досліджено засоби забезпечення інформаційної безпеки банківських установ.

Галузь застосування. Розроблені підходи можуть бути використані у ході впровадження комплексу засобів забезпечення інформаційної безпеки банківської установи, зокрема виявлення, аналізу та протидії кіберзагрозам, а також для навчання персоналу банку в сфері інформаційної безпеки.

Ключові слова: ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ, ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ, АРТ-АТАКИ, БОТНЕТИ, ЗАСОБИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ.

ЗМІСТ

ВСТУП 8
Розділ 1 НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ 10
1.1 Основні засади забезпечення інформаційної безпеки банку 10
1.2 Законодавство України з питань інформаційної безпеки 15
1.3 Нормативні документи НБУ щодо забезпечення інформаційної безпеки в банківській системі України 20
Висновки до розділу 1 24
Розділ 2 ВИДИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ 26
2.1 Джерела та актуальні кіберзагрози інформаційній безпеці банку 26
2.2 APT-атаки як одна з найбільш поширених кіберзагроз ІТКС 31
2.3 Загрози для інформаційної безпеки банку з боку ботнетів 40
Висновки до розділу 2 50
Розділ 3 ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 52
БАНКІВСЬКИХ УСТАНОВ 52
3.1 Аналіз та оцінка ризиків інформаційної безпеки банку 52
3.2 Захист банківської інформації від кіберзагроз APT-атак та ботнетів 58
3.3 Навчання персоналу банку з питань інформаційної безпеки 65
Висновки до розділу 3 78
ВИСНОВКИ 79
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 81

ВСТУП

Актуальність теми. Як свідчить практика, сучасні фінансові установи є одними з лідерів у побудові комплексних систем інформаційної безпеки та використання в них передових технологій та рішень.

Діджиталізація бізнесу, зростаюча кількість змін в IT-інфраструктурі організації, кіберзагрози і кібератаки, що з'являються знову і знову, також вимагають адекватного реагування від фахівців з ІБ. У результаті сьогодні побудова комплексної системи ІБ перетворюється на безперервний процес впровадження нових методів і засобів захисту та вдосконалення вже існуючих.

З огляду на зазначене тема дипломної роботи є актуальною, а використання її результатів сприятиме покращенню підходів до виявлення та протидії загрозам інформаційній системі банків.

Мета і завдання дослідження. **Мета** роботи полягає у вивченні загроз інформаційній безпеці банку та засобів їх протидії.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати нормативно-правове забезпечення інформаційної безпеки банку.

2. З’ясувати види загроз інформаційній та кібербезпеці банку.

3. Дослідити засоби забезпечення інформаційної безпеки банківських установ.

Об’єкт дослідження — забезпечення інформаційної безпеки банку.

Предмет дослідження – загрози інформаційній безпеці банку та засоби їх протидії.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, синтезу, класифікацій та порівняння, оцінювання ризиків, вивчення нормативно-правової бази, а також підходів до навчання персоналу у сфері інформаційної безпеки.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації заходів з аналізу, виявлення та протидії загрозам інформаційній безпеці банку і забезпечення конкурентоспроможності банку.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформаційної безпеки банку, а також навчання працівників банку в сфері інформаційної безпеки.

Розділ 1

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

1.1 Основні засади забезпечення інформаційної безпеки банку

У сучасному світі банківська інформація має значну ціну й величезне значення. Саме з цієї причини до неї і виникає злочинний інтерес.

Невід'ємна частина роботи будь-якої банківської установи – це забезпечення безпеки зберігання даних, наявність регулярної зміни та перевірки паролів. Також контролюється ймовірність витоку інформації.

У банківських інформаційних системах і базах даних міститься конфіденційна інформація про банківських клієнтів, про стан їх рахунків і про те, які ними проводяться фінансові операції. Тому інформаційна безпека таких даних має бути на вищому рівні [20]. При цьому, якщо швидкий і своєчасний обмін та обробка інформації відсутні – відбудеться збій банківської системи. Тому необхідна наявність цілої структури, завдяки якій можливе забезпечення захисту банківської інформації та конфіденційності клієнтської бази.

Заходи щодо захисту даних такого типу повинні здійснюватися послідовно:

- спершу оцінюється і розробляється конфіденційна інформація;
- створюється об'єкт для здійснення захисту.
- контролюється ефективність вжитих заходів.

Банк може повністю здійснювати свою діяльність лише тоді, коли є налагоджений обмін внутрішніми даними та є надійна захисна система. Обладнання такого захисту банківських об'єктів може мати різні форми: фахівцями у сфері забезпечення інформаційної банківської безпеки можуть створюватися як різновиди локальних систем, так і централізовані захисні програми. При виборі конкретної форми захисної системи варто уточнити

наступне: потрібно продумати питання про всілякі способи злому та витоку даних. У разі грамотного та професійного підходу до забезпечення безпеки робота всіх банківських відділень буде злагодженою – а отже, фінансова організація (банк) функціонуватиме безперервно.

Комплекс захисних заходів, спрямований на запобігання порушення конфіденційності даних, має такі конкретні дії [20]:

- контроль процесу обміну даними, вони суворо регламентовані, проводиться обробка швидкості передачі, а також своєчасно знищуються залишкові відомості;

- спеціальна підготовка банківських співробітників, що користуються банківськими даними, включає різні інструктажі та стеження за виконанням необхідних регламентів, дотримання ними всіх вимог безпеки;

- ретельний облік каналів та серверів, також є заходи, спрямовані на забезпечення технічного захисту інформації та банківської безпеки – тобто захищаються резервні копії, забезпечується безперебійне живлення обладнання, що має цінну інформацію, обмежується доступ до сейфів;

- аналіз ефективності заходів.

У кожному напрямі є різні робочі етапи. Наприклад, під час контролю обміну даних, проводиться обробка швидкості передачі, також своєчасно знищуються залишкові відомості. Доступ до банківських даних захищено за допомогою ідентифікаційної системи, тобто її охороняють паролі або електронні ключі. Робота зі співробітниками, що користуються банківськими даними, включає різні інструктажі і стеження за виконанням необхідних регламентів.

Канали та сервери підлягають суворому обліку, також є заходи, спрямовані на забезпечення технічного захисту інформації та банківської безпеки – тобто захищаються резервні копії, забезпечується безперебійне живлення обладнання, що має цінну інформацію, обмежується доступ до сейфів.

Щоб аналізувати, наскільки ефективні вжиті заходи, необхідне ведення обліку або записів, завдяки яким відзначатиметься працездатність і дієвість засобів захисту інформації, що використовуються в банківській установі.

Незважаючи на те, що можливостей злому системи та несанкціонованого доступу до інформації існує досить багато, забезпечення безпеки банківських даних – процедура цілком реальна.

Завдяки наявності сучасних методів інформаційної безпеки тепер удосконалено систему криптографії, а також реалізовано такий захід, як електронний цифровий підпис (ЕЦП). Це так званий аналог і замінює власноручний підпис. Також ЕЦП має безпосередню прив'язку до електронного ключа, що зберігається у власника підпису, а також є захист – наявність спеціального коду.

Електронний підпис у найпростішому вигляді – це електронні дані, які підписант додає до інших електронних даних або логічно зв'язує з ними та використовує їх як власний підпис [1].

Традиційним способом підтвердження юридичних фактів є паперовий документ з печатко. та підписом. Практики створення паперових документів та їх обміну розвивалися століттями та стали частиною сучасної культури ділового обороту. Проте зі стрімким розвитком технологій та суспільства ця культура змінюється настільки швидко, що акти нормативного регулювання часто стають неактуальними вже у процесі підготовки. Можна стверджувати, що ця доля спіткала і Директиву ЄС про електронні підписи 1999 року. Вона дозволила країнам-учасницям розробляти свої власні політики електронного документообігу і це призвело до того, що інфраструктури країн, щодо вимог до ідентифікації та верифікації, виявилися несумісними одна з одною і, відповідно, малопридатними до умов єдиного ринку.

Директива фактично легітимізувала ті способи електронного ділового обміну, за яких ідентифікація його учасників і цілісність даних, якими вони обмінюються захищені просунутими технічними засобами. Іншими словами, навіть договір, укладений шляхом обміну простими електронними повідомленнями суд може визнати дійсним, не кажучи вже про клік-договори (натискання на віртуальну кнопку «згодний» або «підтвердити») або договори, укладені за допомогою сканованих копій.

Підлаштовуючи своє власне законодавство до європейського, Україна у 2003 році ухвалила Закон «Про електронний цифровий підпис», який вніс у наше правове поле поняття електронного підпису та ЕЦП. Подібним до ЄС чином електронний підпис, навіть не захищений криптографічно, став набирати популярності в українському діловому обороті і набувати дедалі більшого адміністративного ухвалення.

У 2016 році європейська Директива була скасована, а на заміну їй прийшов eIDAS – Регламент ЄС 2014 року про електронну ідентифікацію, верифікацію та довірчі послуги (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market). Україна здійснює аналогічне рокірування: Закон про ЕЦП втратив дію 7 листопада 2018 року, а чинності набув Закон «Про електронні довірчі послуги» (детальніше див. п. 1.2).

Очевидним чином, у Законі про ЕДУ багато чого взято за основу з eIDAS, ряд положень є прямим перекладом. Юристам слід мати на увазі факт цієї аналогії, оскільки цілком імовірно, що не лише закон, а й його тлумачення з правозастосуванням слідуватимуть за європейською практикою.

Взагалі, існують основні принципи, згідно з якими забезпечується інформаційна безпека банку:

1. Проблеми своєчасно встановлюються і виявляються.

2. Можна спрогнозувати розвиток.

3. Вжиті заходи повинні бути актуальними та ефективними.

Таким чином, система безпеки, загалом, є безперервним процесом ідентифікації, аналізу та контролю.

Також варто окремо виділити, наскільки важливою є ретельна та регулярна робота з персоналом, оскільки забезпечення безпеки інформації залежить і від того, наскільки якісно та акуратно виконуються вимоги служби безпеки.

Інформаційна безпека банку – це стан захищеності всіх його інформаційних активів. Репутація та конкурентоспроможність банку напряму залежать від його інформаційної безпеки.

Високий рівень забезпечення інформаційної безпеки банку дозволяє звести до мінімуму наступні ризики [21]:

- ризик витоку інформації, яка становить комерційну, службову та/або банківську таємницю;

- ризик втрати або знищення критичних даних;

- ризик використання неповної або спотвореної інформації в процесі діяльності банку, у тому числі при прийнятті управлінських рішень;

- ризик поширення у зовнішньому середовищі інформації, що загрожує репутації банку.

Особливості інформаційних систем банку полягають у тому, що вони:

- зберігають та оброблюють велику кількість даних про фінансовий стан та діяльність фізичних та юридичних осіб;

- включають в себе інструменти для проведення транзакцій, що ведуть до фінансових наслідків;

- не можуть бути повністю закритими, оскільки повинні відповідати сучасним вимогам щодо рівня обслуговування (мати систему онлайн-банкінгу, мережу банкоматів, підключених до публічних каналів зв'язку і т.д.).

Описані вище особливості призводять до того, що інформаційні активи кредитних організацій є бажаною ціллю зловмисників і потребують серйозного захисту.

Основними джерелами загроз інформаційній безпеці банків є:

- зовнішні зловмисні та незловмисні порушники ІБ;

- внутрішні зловмисні та незловмисні порушники інформаційної безпеки;

- збої та відмови програмних та апаратних компонентів інформаційних систем;

- катастрофи техногенного та природного характеру, що можуть порушити нормальний режим роботи інформаційних систем.

Головне завдання зловмисників (зовнішніх порушників та інсайдерів), що атакують інформаційні системи банків, – отримання контролю над інформаційними активами кредитної організації для подальшого здійснення

неправомірних транзакцій або компрометації банку на замовлення недобросовісних конкурентів.

Таким чином, система забезпечення інформаційної безпеки банку повинна відповідати наступним вимогам [21]:

- бути адекватною внутрішнім та зовнішнім загрозам;

- реалізовувати комплексний підхід до захисту – включати всі необхідні організаційні заходи та технічні рішення і захищати всі компоненти ІС (системи електронних платежів, електронного документообігу та обслуговування платіжних карток, банківські програмні та програмно-технічні комплекси, системи віддаленого обслуговування, мережі зв'язку тощо). обробляти великі обсяги інформації без погіршення швидкодії;

- бути надійною та відмово стійкою завдяки застосуванню технологій кластеризації, віртуалізації, балансування навантаження та ін.;

- мати інструменти збору, аналізу даних про інциденти та реагування на події безпеки.

1.2 Законодавство України з питань інформаційної безпеки

В України організаційні та правові основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначає Закон України «Про основні засади забезпечення кібербезпеки України» [18] (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

Закон України «Про електронні довірчі послуги» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.400) [1] визначає організаційні та правові засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов’язки суб’єктів правових відносин у сфері електронних довірчих послуг,

порядок здійснення державного контролю (нагляду) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також організаційні та правові засади здійснення електронної ідентифікації.

Метою цього Закону є врегулювання відносин у сферах електронної ідентифікації та надання електронних довірчих послуг.

Закон описує електронний підпис, удосконалений електронний підпис та кваліфікований електронний підпис.

Електронний підпис у найпростішому вигляді – це електронні дані, які підписант додає до інших електронних даних або логічно зв'язує з ними та використовує їх як власний підпис.

Удосконалений електронний підпис (УЕП) – це електронний підпис, який відповідає наступним додатковим критеріям:

- вона зроблена шляхом криптографічного перетворення даних, з якими пов'язана, за допомогою спеціального програмного забезпечення або обладнання;

– при цьому застосовувався особистий ключ, який однозначно пов'язаний із підписувачем та дає можливість його електронної ідентифікації;

– якщо відбувається втручання у цілісність даних, завірених таким підписом, таке втручання стає виявленим.

Кваліфікований електронний підпис (КЕП) – це такий підпис, що відповідає всім критеріям для УЕП, а також наступним додатковим критеріям:

– програмне забезпечення та/або обладнання, якими вона здійснюється, підлягають додатковим вимогам (наразі законодавство не уточнює, яким саме);

– вона ґрунтується на кваліфікованому сертифікаті відкритого ключа.

Слід звернути увагу на терміни «сертифікат» та «особистий ключ». Як правило, криптографічний захист електронних підписів засновується на шифруванні, що передбачає використання пари «особистий ключ – відкритий ключ». Відкритий ключ доступний як для підписувача, так і для кореспондентів, а особистий ключ повинен перебувати лише у підписувача (до речі, така асиметрія між ключами, лежить в основі терміну «асиметричне криптографічне

перетворення», яке зустрічається в Законі). Пара цих ключів при цьому створюється таким чином, що лише за допомогою особистого ключа можна підписати документ електронним підписом, але перевірити підпис можна за допомогою відкритого ключа, який відповідає особистому ключу. Отримавши документ з удосконаленим електронним підписом, кореспондент може покладатися на те, що це присвоєння зробив власник особистого ключа. Крім того, при створенні підпису відбувається співвідношення даних про документ і даних, що містяться в самому підписі, таким чином, якщо після підписання змінити щось у документі, то він перестане відповідати підпису і кореспондент зможе це виявити.

Проте використання пари ключів саме собою не вирішує питання ідентифікації підписувача. Незважаючи на те, що кореспондент бачить, що документу присвоєно конкретний підпис, він не завжди може бути впевнений у тому, що особистий ключ не був перехоплений або навіть відкритий ключ спочатку не був створений зловмисником з метою видачі себе за підписанта.

Отже, більш наочно, ніж за допомогою формальних визначень, хоч і спрощено, класи електронних підписів можна описати так.

Електронний підпис – це будь-яка електронна форма даних, яка не обов'язково захищена та використовується підписувачем як підпис. Приклад такого підпису – сканування власноручного підпису, яке прикладається до текстового файлу і конвертується, наприклад, у формат PDF.

Удосконалений електронний підпис – це підпис, сформований з використанням засобів криптографії, але при цьому не обов'язково з використанням сертифікату, а якщо і з використанням, то не обов'язково, щоб сертифікат був кваліфікованим. Прикладом існуючого протоколу, який, імовірно, можна вважати критерієм удосконаленого підпису, що підпадає під критерії, є рішення, засновані на стандарті OpenPGP.

Кваліфікований електронний підпис – має бути заснований на криптографії, і відкритий ключ має бути підтверджений сертифікатом, і сам сертифікат має бути кваліфікованим.

Крім електронного підпису, Закон вводить поняття електронної печатки. Електронна печатка також може бути вдосконаленою та кваліфікованою – критерії цих класів аналогічні відповідним критеріям класів підписів. Відмінність полягає в тому, що електронним підписом може користуватися як фізична, так і юридична особа, а електронною печаткою – лише юридична. У функціональному сенсі істотної різниці між електронною печаткою та електронним підписом немає.

Слід звернути увагу на те, що Закон передбачає встановлення вимог, яким засоби електронної ідентифікації та засоби кваліфікованого підпису та печатки мають відповідати; встановлення цих вимог доручено Кабміну. При цьому Закон встановлює принцип технологічної нейтральності – тобто невтручання державних органів у процес розробки програм та обладнання для криптографічного захисту, який не перешкоджатиме досягненню інтероперабельності між ними.

Хоча це формулювання недостатньо зрозуміле, наслідуючи європейський досвід, можна припустити, що йдеться про можливість розробників та надавачів послуг самим визначати, які схеми та рішення використовувати в рамках встановлених вимог, і з урахуванням принципу сумісності – наприклад, чи використовувати фізичні пристрої доступу чи хмарні послуги, чи використовувати двофакторну або багатофакторну автентифікацію тощо.

Закон передбачає, що електронний підпис або печатка не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки. Таким чином, правовий статус простого ЕЦП залишається незмінним – відсутність кваліфікації не робить документ з таким підписом автоматично недійсним, але ступінь довіри до нього може бути низьким. З іншого боку, кваліфікований електронний підпис, навпаки, має презумпцію автентичності (однак ця презумпція ще не означає незаперечність; навіть автентичність ручного підпису аналогічно може бути оскаржена). Удосконалений підпис

займає середню позицію: її достовірність не презумується, проте Закон надає схемам із таким підписом середній ступінь надійності.

Закон надає спеціальні вимоги до кваліфікованих надавачів довірчих електронних послуг. Щоб отримати цей статус, заявник (який може бути фізичною або юридичною особою) повинен, крім інших організаційних та технічних заходів, здійснити атестацію своєї комплектної системи захисту інформації.

Крім формування, перевірки та підтвердження дійсності кваліфікованих електронних підписів та печаток, їх сертифікатів та їх зберігання кваліфіковані надавачі можуть надавати такі послуги:

- формування, перевірка та підтвердження електронної мітки часу;

- замовлена електронна доставка.

Статус кваліфікованого надавача послуг заявники отримують з дня внесення відповідного запису до Довірчого списку. Слід зазначити, що акредитовані центри сертифікації ключів, створені згідно із Законом про ЕЦП, отримують цей статус автоматично та мають бути внесені центральним посвідчувальним органом до Довірчого списку автоматично протягом року після набрання чинності Законом.

Закон України «Про банки і банківську діяльність» (Відомості Верховної Ради України (ВВР), 2001, № 5-6, ст.30) [15] визначає структуру банківської системи, економічні, організаційні і правові засади створення, діяльності, реорганізації і ліквідації банків.

Метою цього Закону є правове забезпечення захисту законних інтересів вкладників та інших клієнтів банків, сталого розвитку і стабільності банківської системи, а також створення сприятливих умов для розвитку економіки України і належного конкурентного середовища на фінансовому ринку.

Закон України «Про Національний банк України» (Відомості Верховної Ради України (ВВР), 1999, № 29, ст.238) [11] регламентує діяльність Національного банку України (НБУ). Відповідно до Закону НБУ є центральним банком країни, одним із органів управління та особливим центральним органом

державного регулювання та нагляду, виконує роль центру емісії, проводить загальну політику у сфері обігу готівки, зміцнення національної валюти, кредитування у останній інстанції для банків, організує систему рефінансування, є головним організатором розрахунків у т.ч. між банками, встановлює правила проведення банківських операцій для банків, ліцензування банківської діяльності та операцій, в окремих випадках, передбачених цим Законом, погоджує функціонування державної банківської системи.

НБУ здійснює валютне регулювання, визначає порядок здійснення операцій в іноземній валюті, організовує та здійснює валютний контроль за банками та іншими фінансовими установами, які отримали ліцензію Нацбанку на здійснення валютних операцій. Також НБУ встановлює/оприлюднює курс національної грошової одиниці (гривні) стосовно іноземних валют, встановлює номінали, системи захисту, платіжні знаки, дизайн грошових знаків, зберігає їх резервні фонди та встановлює нормативи обов'язкового резервування коштів іншим банкам.

Також у його функції входить збереження банківських та дорогоцінних металів, каміння та інших цінностей. Банк розміщує золотовалютні резерви, виконує операції із ними. НБУ встановлює порядок визначення облікової ставки та інших процентних ставок за своїми операціями.

1.3 Нормативні документи НБУ щодо забезпечення інформаційної безпеки в банківській системі України

Відповідно до інформації, розміщеній у [22], у січні 2021 року Нацбанк посилює контроль за виконанням банківськими установами заходів щодо забезпечення інформаційної безпеки та кіберзахисту, що в умовах сучасних кіберзагроз сприятиме удосконаленню організації діяльності банків.

З цією метою регулятор впроваджує новий вид контролю за банківськими установами у вигляді безвиїзного нагляду та виїзних перевірок, які

здійснюватимуть фахівці Національного банку у сфері інформаційної безпеки та кіберзахисту.

Порядок організації та здійснення Національним банком цих заходів містить постанова Правління Національного банку України від 16 січня 2021 року № 4 «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» (далі – Постанова № 4) [29].

Цей документ ухвалений відповідно до повноважень, визначених Законом України «Про Національний банк України» [11] та з урахуванням положень Закону України «Про основні засади забезпечення кібербезпеки України» [18], Закону України «Про електронні довірчі послуги» [1], з урахуванням Директиви Європейського парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95 (далі - Положення № 95), Положення про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням Засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116 (далі - Положення № 116).

Постанова №4 встановлює:

1) порядок організації та здійснення Національним банком України (далі - Національний банк) заходів контролю за дотриманням банківськими установами вимог законодавства, що регулює відносини у сферах інформаційної безпеки, кіберзахисту та електронних довірчих послуг, а також нормативно-правових актів Національного банку, які здійснюються при виконанні наглядових функцій, покладених на Національний банк (далі - контроль);

2) вимоги щодо проведення банківською установою самооцінки стану інформаційної безпеки та кіберзахисту.

Так, банки зобов'язані щорічно проводити відповідну самооцінку, складати і подавати Національному банку щорічний звіт з питань оцінювання ризиків інформаційної безпеки/кіберризиків.

Реалізація механізмів контролю, передбачених Постановою № 4, дасть можливість регулятору ухвалювати рішення, що належать до компетенції засвідчувального центру, та здійснювати оцінку:

- ефективності функціонування системи управління інформаційною безпекою банку;

- повноти виконання банком вимог нормативно-правових актів Національного банку з питань інформаційної безпеки і кіберзахисту;

- рівня управління банком ризиками інформаційної безпеки й кіберризиками, системи внутрішнього контролю за цими напрямками.

Постанова № 4 набрала чинності з 21 січня 2021 року.

Постанова НБУ №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [27].

Це Положення було розроблено відповідно до Законів України «Про банки і банківську діяльність», «Про Національний банк України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», указів Президента України від 13 лютого 2017 року № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» та від 15 березня 2016 року №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник» (далі – ДСТУ ISO/IEC 27000:2015), ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» (далі – ДСТУ ISO/IEC 27001:2015), ДСТУ ISO/IEC

27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки» (далі – ДСТУ ISO/IEC 27002:2015), які прийняті наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року №193, та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту з метою підвищення рівня інформаційної безпеки в банківській системі України.

Це Положення встановлює:

1) мінімальні обов'язкові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту;

2) принципи управління інформаційною безпекою;

3) вимоги щодо банківських інформаційних систем, які взаємодіють з інформаційними системами Національного банку України (далі - Національний банк), з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах Національного банку.

Постанова НБУ № 95 заснована на міжнародному стандарті ISO/IEC 27001:2013 та містить 150 вимог до інформаційної безпеки. З них 132 пункти є обов’язковими до виконання починаючи з 1 березня 2018 року, і ще 18 – з 1 вересня 2019 р.

На рисунку 1.1 показано, які області ІБ охоплюють ці Вимоги.

Положення про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру (№ 116 від 19.09.2019).

Це Положення розроблене відповідно до статті 7 Закону України «Про Національний банк України», статті 9 Закону України «Про електронні довірчі послуги» і встановлює вимоги:

Рис. 1.1 Області вимог ІБ відповідно до Постановою НБУ №95

1) до надавачів електронних довірчих послуг для внесення відомостей про них до Довірчого списку за поданням засвідчувального центру;

2) до кваліфікованих надавачів електронних довірчих послуг, відомості про яких внесені до Довірчого списку за поданням засвідчувального центру (далі - кваліфіковані надавачі), та їх відокремлених пунктів реєстрації.

Висновки до розділу 1

Підсумовуючи, варто відзначити велике значення банківських систем в економіці держави, а, отже, питання забезпечення інформаційної безпеки банків має вирішуватися ефективно. Специфіка та особливості системи забезпечення ІБ є індивідуальними для кожної банківської організації, тому комплексний та професійний підхід до організації систем захисту – необхідна умова роботи всієї банківської системи.

Аналіз вітчизняного законодавства показав, що основними законами, які регулюють питання інформаційної безпеки у банківській сфері є Закони України «Про банки і банківську діяльність», «Про Національний банк України», «Про електронні довірчі послуги», «Про основні засади забезпечення кібербезпеки України» тощо.

Водночас ключову роль у нормативному регулюванні питань інформаційної безпеки вітчизняних банківських установ відіграє НБУ, який посилив контроль за виконанням банківськими установами заходів щодо забезпечення інформаційної безпеки та кіберзахисту, що в умовах сучасних кіберзагроз має сприяти удосконаленню організації діяльності банків.

Так, НБУ впровадив новий вид контролю за банківськими установами у вигляді безвиїзного нагляду та виїзних перевірок, які здійснюватимуть фахівці регулятора у сфері інформаційної безпеки та кіберзахисту. Крім цього, банки зобов’язані проводити самооцінку стану власної інформаційної безпеки та кіберзахисту. Також НБУ ухвалив мінімальні обов'язкові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків; принципи управління інформаційною безпекою; вимоги щодо банківських інформаційних систем, які взаємодіють з інформаційними системами НБУ.

Розділ 2
ВИДИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ

2.1 Джерела та актуальні кіберзагрози інформаційній безпеці банку

Проблема безпеки у фінансовому секторі багато разів обговорювалася з різних боків, оскільки платіжні та банківські системи є досить вразливими. Поки фінансові інститути вибудовують системи захисту, застосовуючи більш витончені технології, шахраї навчаються обходити їх.

Шахрайство у фінансовій сфері – це зворотний бік процесу розвитку технологій. Повністю виключити вразливість платіжних та банківських систем неможливо. Тому основні зусилля регуляторів, фінансових компаній та експертів з безпеки витрачаються на те, щоб звести до мінімуму ризики. У той же час кіберзлочинці намагаються знайти спосіб обійти нові методи захисту – в результаті створюється замкнене коло постійного протистояння атакуючих і захисників.

Щойно виникли перші електронні платіжні послуги та системи дистанційного банківського обслуговування, з'явилися люди, готові скористатися цими недоліками в корисливих цілях.

У цьому плані примітна історія PayPal. При виході обсягів операцій у сотні переказів за хвилину відстежувати їх фізично стає неможливо. Через хакерські атаки, компанія спочатку втрачала 10 млн. доларів щомісяця, розповідає один із засновників PayPal Пітер Тіль [25]. До автоматизованої системи захисту шахраї швидко пристосовувалися і знаходили варіанти обходу. Довелося створити гібрид людини і програми – систему «Ігор», на ім'я найактивнішого зломщика з Росії.

Сьогодні PayPal надає гарантії безпеки як покупцю, так і продавцю. Це не означає, що шахрайство у платіжному сервісі виключено. Просто компанія в плюсі і може собі дозволити оплачувати ризики.

У певному сенсі безпека ґрунтується на вірі в захищеність тієї чи іншої системи. Так, з’явилась нова технологія токенізації, яку платіжні системи Visa та MasterCard активно просувають у світі, починаючи з 2014 року. Багато хто впевнений, що на сьогоднішній день це ідеальний захист від шахраїв. Такою вона і вважатиметься, доки не з'явиться статистика, що доводить протилежне.

Один із небезпечних трендів останніх років – атаки на процесингові центри банків із виведенням коштів через банкомати. Ці атаки умовно можна поділити на дві категорії. Перша – це зараження підсистеми управління банкоматами чи через неї – самих банкоматів, з наступним поданням команди на видачу готівки. Зловмисникам залишається лише у потрібний момент підійти до банкомату та прийняти купюри. Другий спосіб – це зламування процесингу з наступним зарахуванням на заздалегідь отримані карти дуже значних сум. Далі відбувається переведення в готівку цих коштів через банкомати різних банків.

Також продовжуються атаки зловмисників на системи дистанційного банківського обслуговування (ДБО) клієнтів. В основному вони реалізуються через зараження пристроїв, з яких клієнти керують дистанційно своїми рахунками. З урахуванням того, що багато банків впровадили технології підтвердження переказів (операцій) одноразовими кодами, які клієнти отримують, наприклад, через служби повідомлень SMS (Short Message Service), зловмисники використовують різні методи соціальної інженерії для виманювання у клієнтів цих кодів.

Взагалі шахрайство з використанням методів соціальної інженерії, а простіше кажучи обман клієнта, – це ще один із трендів останніх двох років. Особливо часто він використовується для виманювання у людей даних їх платіжних карток і одноразових кодів підтвердження операцій. Зловмисники навіть частково автоматизували сам процес «виманювання»: початковий дзвінок здійснюється зазвичай програмно, далі як правило спрацьовує автоінформатор, який повідомляє, що на карті відбулася так звана «транзакція». Для нібито скасування такої «транзакції» на телефоні необхідно натиснути будь-яку клавішу. Якщо клієнт натискає клавішу, автоінформатор нібито переводить

дзвінок на службу технічної підтримки банку (при цьому все виглядає дуже натурально). Насправді у клієнта перемикають на «фахівця» з використання даних платіжних карток. Діють зловмисники дуже професійно, і непідготовлені люди, особливо похилого віку, найчастіше стають жертвами цієї омани.

І останній різновид зовнішніх атак, на який варто звернути увагу, – це здирство. Хакери проникають в систему і шифрують якісь важливі файли, а потім звертаються до власників компанії з пропозицією купити пароль на архів. На загальний e-mail банку приходить лист із загрозою та пропозицією перерахувати необхідну суму на вказаний електронний гаманець. Варіанти загроз можуть бути зовсім різними. Наприклад, що всі комп'ютери мережі заражені невідомим вірусом, який не виявляє ще жоден антивірус, або, що процесинг банку зламаний і якщо не перерахувати необхідну суму, то втрати стануть в десятки разів більше. Можуть шантажувати тим, що корпоративна мережа зламана і їм вдалося завантажити якусь важливу інформацію, і якщо гроші не будуть перераховані, то ця інформація буде опублікована у відкритих джерелах [8].

Рис. 2.1 Актуальні кіберзагрози в банківській сфері

У червні 2021 року офіс генпрокурора України повідомив, що в Україні викрили групу хакерів-криптовимагачів, які завдали збитків іноземним компаніям на суму близько $500 млн. Українські правоохоронці провели спільну

роботу з колегами з Південної Кореї та США. Слідство встановило, що група осіб у 2019 році атакувала вірусом-шифрувальником Clop чотири корейські компанії. Було заблоковано 810 внутрішніх серверів та персональних комп'ютерів їхніх співробітників. А у 2021 році ці ж хакери здійснили атаку із шифруванням даних на співробітників та фінансові звіти Медичної школи університету Стенфорда, Університету Меріленду та Університету Каліфорнії в США. Вони погрожували опублікувати конфіденційну інформацію та отримали викуп у криптовалюті [30].

У результаті в Києві та Київській області пройшли 24 обшуки за місцем проживання шести членів групи. У них вилучили комп'ютерну техніку, вісім автомобілів, близько $58 тисяч, €3 тисячі, понад 1,5 млн. грн. готівки, а також документацію, яка підтверджує, що хакери займалися протиправною діяльністю. Порушено кримінальну справу за ч. 2 ст. 361 (несанкціоноване втручання у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ч. 2 ст. 209 (легалізація (відмивання) доходів, одержаних злочинним шляхом) КК України. Максимальне покарання за цими статтями становить 12 років ув'язнення.

Але справжні професіонали не займаються цим на постійній основі, тому що здирство надто ризиковане – воно вимагає прямого фінансового переводу коштів від жертви до злочинця. Набагато безпечніше продати викрадену інформацію на чорному ринку. В Інтернеті можна знайти сайти, де продаються та купуються кредитні картки з кодами верифікації [23]. Купівля-продаж кредиток відбувається в IRC-чатах, а також на закритих та відкритих форумах, таких як CardersMarket та Carder.info, а іноді лоти спливають навіть на офіційних аукціонах. Найдосвідченіші хакери заходять лише в приватні, зашифровані, захищені паролем IRC-чати.

На одному з кардингових торгових форумів CardingWorld.cc вже накопичилося понад 100 000 опублікованих повідомлень від 13 000 зареєстрованих користувачів, більшість з яких розмовляють російською мовою [23]. На цьому сайті можна купити інформацію з серверів Bank of America та

Fidelity Bank, а також акаунти PayPal та послуги з безпечного переказу/переведення в готівку великих сум грошей. На сайті TalkCash.net ведеться список «злочинців» та «чесних торговців».

Незважаючи на вищесказане, варто відмітити людський фактор – основна та головна загроза інформаційної безпеки, що прямо залежить від людських відносин. Витік інформації найчастіше відбувається з провини банківського персоналу.

За даними статистики [19], приблизно 80% правопорушень відбувається через банківських співробітників – через тих, хто має доступ до даних.

При цьому забезпечення внутрішньої інформаційної безпеки банку є вкрай необхідним заходом як для того, щоб захистити конфіденційність даних від звичайної недбалості, так і для того, щоб виключити навмисний злам баз даних.

Є не лише внутрішній чинник – але й наявність технічної загрози інформаційній безпеці банківських організацій. Технічні загрози – це зламування інформаційних систем особами, які не мають прямого доступу до системи. Це можуть бути кримінальні чи конкуруючі організації. Знімають та одержують інформацію в цьому випадку за допомогою особливої аудіо- або відеоапаратури. Сучасна популярна форма злому – коли застосовуються електричні та електромагнітні випромінювання. Зловмисники за цей час одержують конфіденційну інформацію.

Небезпека та загроза для програмного забезпечення походить від різних шкідливих для носія інформації комп'ютерних вірусів, програмних закладок, здатних призвести до руйнування введених кодів.

Ще один ліквідний товар у хакерській економіці – шкідливий софт, у тому числі віруси, черв'яки, трояни. Так звані експлойти дозволяють використовувати дірки в програмному забезпеченні та проникати у чужі системи. На думку експертів, індустрія експлойтів працює так само чітко, як індустрія офіційного програмного забезпечення. «Провайдери» експлойтів купують код експлойтів у представників андеграунду, зашифровують його, щоб захистити від піратів, і

продають «упакований» експлойт. Він потім може використовуватися для створення нового або розширення існуючого ботнета.

Шкідливий софт останнім часом стає все складнішим і досконалішим. За даними Антифішингової робочої групи (Anti-Phishing Working Group), лише у грудні 2005 року було виявлено 340 нових варіантів кейлоггерів та троянів: це абсолютний рекорд за весь час спостереження.

У грудні 2006 р. експлойт для операційної системи Windows Vista продавався на румунському форумі за $50 000 [23]. Це нормальна ціна для експлойту типу «zero day», який використовує слабкі місця, ще не відомі фахівцям з комп'ютерної безпеки. Хакери йдуть на крок попереду офіційних фахівців – це й не дивно. На думку деяких експертів, загальний оборот хакерської економіки перевищує сумарні доходи всіх компаній, що займаються комп'ютерною безпекою, разом узятих.

2.2 APT-атаки як одна з найбільш поширених кіберзагроз ІТКС

Однією з найбільш поширених кіберзагроз ІТКС банків дійсно можна вважати постійні серйозні загрози (англ. Advanced Persistent Threat, APT).

Особливість цілеспрямованих APT-атак у тому, що зловмисники націлені на конкретну державну установу або приватну компанію. Це є відмінністю цієї загрози від масових атак хакерів – коли одночасно атакується велика кількість цілей і жертвою стають найменш захищені користувачі стають.

Ці атаки є цілеспрямовані, добре сплановані і включають в себе кілька етапів – починаючи від розвідки та впровадження та закінчуючи знищення слідів присутності (таблиця 2.1). В результаті, внаслідок атак типу APT зловмисники отримують доступ до інфраструктури жертви та, як правило, залишаються непомітними впродовж декількох місяців або навіть років – протягом усього цього часу вони мають доступ до всієї корпоративної інформації.

Таблиця 2.1

Етапи цільової атаки

Назва етапу	Зміст
Підготовка	Виявлення мети Збір інформації Розробка стратегії Створення стенду Розробка інструментів
Проникнення	Техніки обходу стандартних засобів захисту Експлуатація вразливостей Соціальна інженерія Комбіновані техніки Інвентаризація мережі
Розповсюдження	Закріплення Розповсюдження Оновлення Пошук ключової інформації та методів досягнення цілей
Досягнення цілей	Викрадення ключової інформації Зміна даних Маніпуляції з бізнес процесами Приховування слідів Точка виходу/повернення

Зловмисниками вивчаються інформаційні системи об'єкта атаки, щоб визначити, яке програмне забезпечення використати для тих чи інших цілей. Об'єктами атаки виступають конкретні інформаційні системи та/або люди. Шкідливе програмне забезпечення розробляється спеціально для кожної конкретної атаки, щоб системи захисту та штатні антивіруси, які використовує об'єкт атаки і які зловмисники досить добре дослідили, не змогли виявити загрозу. Найчастіше це вразливість «0-day» (нульового дня) та особливі алгоритми зв'язку з виконавцями/замовниками атаки.

Розрахувати навіть приблизну кількість APT-атак практично неможливо через складнощі при кваліфікації таких атак та їх комплексність.

Більшість фахівців сходиться на думці щодо наступних особливостей цільових атак [1]:

- Ці атаки, направлені на конкретні комерційні організації, галузі виробництва, фінансові установи або державні відомства.

- Об'єктами атаки є дуже обмежені будь-якими рамками або цілями конкретні інформаційні системи.

- Ці атаки не носять масовий характер і на їх підготовку витрачається досить багато часу та ресурсів.

- Шкідливе програмне забезпечення, яке зловмисники використовують при реалізації атаки, спеціально розробляється для конкретної атаки, щоб штатні системи захисту, не змогли виявити її реалізацію.

- Для реалізації атаки можуть використовуватися вразливості «нульового дня».

- APT-атаки, як правило, використовуються для викрадення інформації, яку можна продати, або для порушення доступності до критично важливої інформації.

- При здійсненні цільових атак використовуються ті ж самі механізми злому, як і за масових атак, зокрема фішинг. Відмінність полягає у підготовці атаки з метою запобігання можливості її виявлення системами захисту. Саме стосовно цільових атак фішинг стає дуже актуальною загрозою, оскільки атака в цьому випадку здійснюється не на абстрактні, а на конкретні фізичні особи, що може бути досягнуто методами соціальної інженерії.

- Вже після виявлення та ідентифікації цільової атаки, за підсумками її здійснення, коли про загрозу цієї атаки стає відомо, вона переходить у категорію «масових» – може масово використовуватися зловмисниками. При цьому як ідентифікована загроза цієї атаки вже може виявлятися системами захисту, одним із завдань яких є забезпечення мінімальної тривалості переходу загрози атаки з категорії цільових у масові.

Що стосується фінансової сфери, то тут спроби злому мають типові особливості:

- атаки є цільовими та враховують особливості процесів відправлення та обробки повідомлень у певній платіжній системі;

- шкідливий код доволі часто не виявляється стандартними засобами антивірусного захисту, незважаючи на актуальність антивірусних баз;

- зафіксовано також факти проникнення хакерів у локальні мережі банків для впровадження шкідливого коду через корпоративну електронну пошту.

Представники банків відзначають: якщо раніше шахраї намагалися грабувати клієнтів, то тепер перейшли на більший видобуток, а саме – на фінансово-кредитні установи.

Публічно доступна інформація щодо засобів проведення атак типу APT та розслідування інцидентів (які мають ознаки таких атак) дозволяють говорити про різноманітність методів. Наприклад, можуть використовуватися як телефонні дзвінки, так і автоматизовані методи.

Зловмисники в ході атаки досліджують різні можливості, щоб отримати доступ до необхідної інформації. Може здійснюватися прямий фізичний доступ або атакуватись пристрої співробітників банку та їх облікові записи в інтернет-сервісах.

Жертві навряд чи вдасться уникнути спроб націлених атак. Наприклад, зловмисник прагне отримати доступ до внутрішніх ресурсів компанії, що його цікавлять. З цією метою він може ініціювати безліч направлених атак протягом декількох місяців або років. Всі елементи атаки (мережеві атаки, шкідливе програмне забезпечення) можуть бути попередньо перевірені на «помітність» для поширених методів та систем виявлення. У разі неефективності, такі елементи проходять глибоку модифікацію. Засоби вторгнення, у тому числі й ті, що вже функціонують у захопленій системі, можуть отримувати оновлення так само як оновлення антивірусних баз.

Більшість APT-атак виявляється постфактум. Атрибуція залишається найбільшою проблемою – встановлення організаторів та виконавців таких атак.

Визначення винуватця – це надзвичайно складне завдання. У цьому процесі необхідно зібрати максимальну кількість чинників, які вказували б на

причетність хакерської групи певної національності чи організації до скоєння злочину. Для цього потрібна тісна співпраця між компаніями, які працюють у сфері інформаційної безпеки, жертвами, правоохоронними органами різних країн тощо. Але і в цьому випадку встановлюються лише одиниці винуватців, найчастіше через грубі помилки зловмисників.

На даний час спрямовані атаки перестають бути долею обраних: зловмисники постійно оптимізують та вдосконалюють свої техніки та інструменти, і це здешевлює і спрощує організацію шкідливої кампанії, що, у свою чергу, сприяє появі нових гравців.

Основне завдання атаки класу APT — крадіжка конфіденційної інформації, яку згодом можна використати для отримання геополітичної переваги або продажу заінтересованим особам. Найбільший ризик стати жертвою цільової атаки мають урядові та дипломатичні організації, банківські установи, компанії, що працюють в енергетичній та аеро-космічній галузях, організації у сфері охорони здоров'я та освіти і науки, телекомунікаційні та IT-компанії, постачальники для збройних сил, а також громадські та політичні активісти. Згідно [1] наведемо перелік основних цілей таргетованих атак:

- Офіс правління компанії. Часто апаратура неналежно захищена від фізичного пошкодження (наприклад, з боку персоналу з прибирання або технічного обслуговування приміщень).

- Центри обробки даних є надійним середовищем для розміщення приватної хмари. Проблемою є забезпечення безпечного функціонування численних серверів, а також програм, що працюють на цих серверах.

- Мережа постачальників. Через застосування мережевих рішень, що розширюється, при роботі з постачальниками виникають ризики, пов'язані з тим, що відносно невеликі компанії-постачальники, як правило, гірше захищені.

- Хмарні обчислення. В основі своєї використання зовнішньої хмари безпечно. Проблеми пов'язані з тим, що рівень захисту даних залежить від законодавства та можливий доступ з боку спецслужб.

- Виробництво. Безліч застарілих спеціалізованих систем все частіше об'єднується в мережі, і їхню роботу важко відстежувати та контролювати. Атаки зловмисників у цьому випадку можуть призвести до виробничих та репутаційних втрат або навіть краху компанії.

- Бази даних забезпечують безпечне збереження важливої інформації. Головна слабкість в тому, що в якості «інструментів» для проникнення в бази даних зломщики можуть використовувати адміністраторів.

- Кінцева продукція активується за допомогою інформаційних технологій. Зростання використання мережних рішень для забезпечення функціонування кінцевої продукції полегшує проведення кібератак. Дистанційно контролюючи пристрої користувачів з метою провокування поломок, хакери мають можливість незаконно отримувати конфіденційну інформацію через ці пристрої. У зв'язку з цим компанії може загрожувати втрата репутації та отримання позовів від користувачів, які стали жертвами шахрайства.

- Офісні мережі. Зростаючий рівень мережевої взаємодії, що передбачає об'єднання багатьох систем, надає хакеру багаті можливості, якщо він зможе проникнути в мережу

- Продаж. Витік маркетингових планів, інформації про ціни та клієнтів підриває репутацію компанії та позбавляє її конкурентних переваг.

- Мобільні пристрої. Купуючи доступні на комерційному ринку смартфони, користувачі часто зберігають у пам'яті пристрою конфіденційні дані, які, як правило, легко можуть бути викрадені зловмисниками. Найбільш випробувані та надійні концепції безпеки можуть виявитися марними, якщо співробітниками компанії використовуються особисті мобільні пристрої для вирішення робочих завдань.

Наслідки вдалої спрямованої атаки можуть бути доволі різноманітними:

- компрометація даних ключових персон;

- втрата критичних даних;

- викрадення комерційної таємниці;

- знищення IT-інфраструктури;

- переривання бізнес-процесів;
- недоступність сервісів, що надаються компанією;
- викрадення грошових коштів;
- погіршення репутації;
- втрата конкурентної переваги;
- втрата довіри клієнтів;
- зменшення долі на ринку;
- прямі та непрямі грошові втрати.

Причому втрати можуть носити так званий «характер з післядією», тобто умовно розділити можна їх на прямі та непрямі.

До прямих віднести можна втрачені можливості компанії (втрачені контракти, втрачений прибуток), відновлення системи (IT-консалтинг, аудиторії, юристи та PR-активності), простої виробництва (скорочення доходів).

До непрямих відносяться подальші витрати, які спрямовані на вирішення наступних питань для запобігання повторних інцидентів:

- закриття наявних вразливостей в інфраструктурі;
- зміна систем захисту;
- закупка додаткових засобів ІБ;
- наймання додаткових штатних спеціалістів з ІБ;
- перегляд бізнес-процесів;
- підвищення обізнаності працівників в питаннях ІБ;
- поліпшення експертизи служб ІБ.

Взагалі підрахувати реальні збитки від атак класу APT практично неможливо: за даними компанії ESET, 66% інцидентів системи безпеки залишаються непоміченими багато місяців. Саме під це і розроблюється складне шкідливе ПЗ для цільових атак: крадіжка даних відбувається непомітно, у «фоновому» режимі. Велика кількість атак залишається непоміченими. При виявленні багато організацій намагаються приховати факт інциденту і не розголошувати його. У «Лабораторії Касперського» вважають, що щотижня у

світі стає відомо як мінімум про одну гучну цільову атаку. Насправді таких гучних атак на тиждень може відбуватися понад сто.

Стосовно джерел таргетованих атак, то в цьому питанні для досягнення своїх цілей злочинці використовують усі доступні засоби. Можна виділити кілька основних векторів таргетованих атак:

1. Несанкціонований доступ до офісної техніки та іншого обладнання, яке можна проникнути або впровадити шкідливий код. Хоча центри обробки даних в основному забезпечують прийнятний рівень безпеки, їх уразливі місця пов'язані з функціонуванням серверного обладнання та встановленого на ньому програмного забезпечення.

2. Розгалужені локальні мережі, завдяки розвитку технологій, дозволяють зловмисникам у разі підключення до одного з пристроїв (це може бути комп'ютер, факс, принтер або МФУ) спокійно переміщатися всередині корпоративної мережі.

3. Використання смартфонів та іншої персональної електроніки в робочих цілях та всередині корпоративної мережі може стати слабкою ланкою у захисті та відправною точкою у розвитку атаки.

Малоймовірно, що цільову атаку буде застосовано проти рядових користувачів ПК, якщо вони не є співробітниками компаній. Метою атаки може стати будь-яка інформація, яка становить цінність. Найчастіше такі напади здійснюються для отримання промислових секретів, персональних та платіжних даних. Багато великих бізнесменів та керівників підприємств припускають, що одного разу подібна атака може бути проведена і проти їх організації.

Сьогодні відомо про більш ніж 100 хакерських угруповань, які проводять цільові атаки. Від їхніх дій страждають державні та комерційні структури у 85 країнах. Таке широке поширення пояснюється оптимізацією засобів злому, що призводить до спрощення та здешевлення шкідливих операцій.

Виробники засобів та систем забезпечення інформаційної безпеки регулярно вдосконалюють засоби протидії APT-атакам. Розробляються спеціалізовані комплексні продукти, створені не тільки для пошук невідомих

зразків шкідливого коду, але і для виявлення підозрілої активності в системі. Це пояснюється тим, що під час атак шкідливе програмне забезпечення використовується не завжди: зловмисники можуть використовувати і цілком легальні засоби. Окремі модулі аналізують файли, що завантажуються з Інтернету, мережеву активність і поведінку користувачів на робочих станціях. Найбільш ефективними є комплексні рішення, окремі компоненти яких надають зловмисникам хибні набори цілей та даних, таким чином відволікаючи їх від критично важливих даних та ресурсів.

Повністю захиститись від APT-атак неможливо. Так, якщо злочинець планує отримати доступ до даних компанії, він може безперервно вести атаки протягом багатьох місяців або навіть років, іноді паралельно починаючи кілька шкідливих кампаній. Не маючи обмежень у часі, він ретельно перевіряє можливість виявлення з боку антивірусу та системи захисту шкідливого програмного забезпечення і за необхідності модифікує та оптимізує його. Основні витрати часу припадають на підготовчих етап, а ось сама атака займає лічені хвилини. Ймовірність її успішної реалізації дуже велика.

Під час підготовки вивчається об'єкт атаки, збирається повна інформація, проводяться розвідувальні заходи, визначаються слабкі місця в системі захисту. Для моніторингу використовуються спам-розсилки, офіційні сайти та облікові записи в соціальних мережах, профільні форуми. За допомогою програм-аналізаторів проводиться вивчення мережевої інфраструктури та програмного забезпечення організації. Для отримання даних можуть застосовуватись автоматизовані методи або індивідуальні форми впливу, наприклад, телефонні дзвінки. Прикладом є кібершпигунська група Poseidon, яка розробляє інструменти атаки ще з 2005 року.

Виявлення APT-атаки – комплексне та дуже складне завдання. Факт проникнення в систему може бути непомітним впродовж досить довгого часу. В результаті цього, визначити загальну кількість атак класу APT, які реалізуються по всьому світу, надзвичайно складно.

2.3 Загрози для інформаційної безпеки банку з боку ботнетів

Термін Botnet (ботнет) утворено від слів robot (робот) і network (мережа). Кіберзлочинці використовують спеціальні троянські програми, щоб обійти систему захисту комп'ютерів, отримати контроль над ними та об'єднати їх у єдину мережу (ботнет), якою можна керувати віддалено.

Часто кіберзлочинці прагнуть заразити шкідливими програмами та взяти під контроль тисячі, десятки тисяч і навіть мільйони комп'ютерів і таким чином вільно керувати великою зомбі-мережею. Такі мережі можна використовувати для здійснення атак типу «відмова в обслуговуванні» (Distributed Denial of Service, DDoS), великомасштабних кампаній розсилки спаму та інших типів кібератак.

У деяких випадках кіберзлочинці створюють велику мережу зомбі-комп'ютерів, а потім продають доступ до цієї зомбі-мережі іншим злочинцям або здають її в оренду. Спамери орендують або купують такі мережі для проведення великомасштабних кампаній поширення спаму.

Зловмисники досить швидко здогадалися використовувати ботнети для запуску складного шкідливого програмного забезпечення, що дозволило їм створити цілі інфраструктури із заражених комп'ютерів та інших пристроїв із виходом до Інтернету для отримання незаконного прибутку у величезних масштабах.

Обчислювальна потужність одного ботнета дозволяє здійснювати шкідливі дії швидко та часто без виявлення. Наприклад, у 2016 році ботнет був використаний для створення найбільшої DDoS-атаки в історії, яка викликала збої у роботі таких сайтів як Twitter, Amazon та Netflix.

Правоохоронні органи в останні роки змогли досягли значних успіхів у боротьбі зі злочинною діяльністю, пов'язаною з використанням ботнетів, але поки що цих зусиль недостатньо, щоб нанести удар по ботнетах під керівництвом кіберзлочинців. Ось декілька відомих прикладів [11]:

1. Міністерство юстиції США звинуватило двох молодих людей у їх причетності до розробки та використання ботнета Mirai: 21-річному Парасу Джа (Paras Jha) та 20-річному Джошуа Уайту (Josiah White). Їх звинувачують в організації та проведенні чисельних DDoS-атак на установи, а потім вимаганні викупу за їх зупинку, а також з продажу цим організаціям «послуг» щодо запобігання у майбутньому подібним атакам.

2. В рамках транскордонної операції іспанська влада затримала жителя Санкт-Петербурга Петра Левашова, більш відомого в кіберзлочинних колах як Peter Severa. Він керував один із ботнетів під назвою Kelihos, який довго існували в Інтернеті та за приблизними оцінками, заразив понад 100 тис. комп'ютерів. Крім здирства, Петро Левашов активно використовував Kelihos для організації розсилки спам-листів, беручи за мільйон повідомлень по 200-500 доларів США.

3. Двох ізраїльських тинейджерів було заарештовано за звинуваченням в організації DDoS-атак на замовлення. Вони встигли провести близько 150 тис. DDoS-атак та заробити близько $600 тис.

Ботнети (рисунок 2.2) є комп'ютерними мережами, які складаються з великої кількості комп'ютерів або інших пристроїв, підключених до Інтернету, на яких завантажено та запущено, звісно без відома їх власників, шкідливе автономне програмне забезпечення – боти.

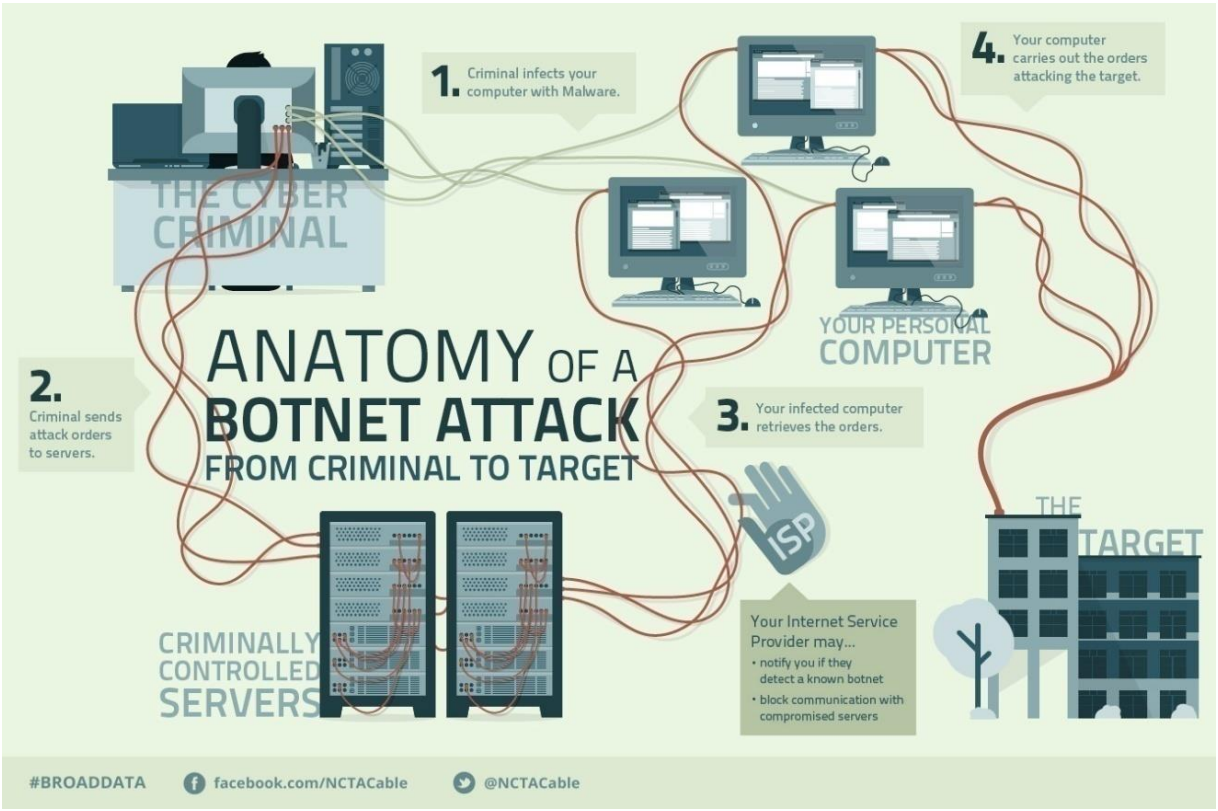

Рис. 2.2 Схема роботи ботнетів

З самого початку свого створення боти розроблялись з метою автоматизації повторюваних та одноманітних завдань, ніяк не пов'язаних з криміналом. Цікавим ще є той факт, що мета одного із перших успішних ботів, який має назву Eggdrop та був розроблений у 1993 році, полягала в управлінні та захисту IRC (Internet Relay Chat) каналів від спроб втручання сторонніх осіб та перехоплення керування ними. Але зловмисники дуже швидко побачили потенціал ботнетів та навчилися використовувати їх як глобальні, практично автоматичні системи, які дають прибуток.

За останній час ботнети та пов'язане з ними шкідливе програмне забезпечення значно розвинулися, і на сьогоднішній день можуть використовувати різноманітні методики атак, що можуть одночасно реалізовуватись в кількох напрямках. Крім того, з погляду кіберзлочинців так звана «ботекономіка», виглядає надзвичайно привабливо. Перш за все практично відсутні будь-які витрати на інфраструктуру, оскільки для організації мережі із заражених машин злочинці використовують скомпрометовані комп'ютери та інші пристрої і обладнання з можливістю виходу в Інтернет, природно, без згоди

та відома користувачів цих пристроїв. Відсутність будь-яких вкладень в інфраструктуру означає, що прибуток злочинців фактично дорівнює їх доходу від незаконної діяльності. Не зважаючи на широкі можливості та вигоду від використання такої інфраструктури, зловмисники дуже серйозно підходять до питання власної анонімності. З цією метою, вимагаючи викуп, вони, зазвичай, використовують такі криптовалюти, які неможливо відслідкувати, наприклад, Bitcoin (BTC). Саме із зазначених вище причин ботнети стали найбільш пріоритетної та бажаною платформою для кіберзлочинців.

Ботнети з точки зору реалізації різноманітних бізнес-моделей є надзвичайно гарною платформою для запуску різного роду шкідливих функцій, що приносить зловмисникам великий дохід:

1. Швидке та масштабне поширення заражених електронних листів, що містять в собі програми-вимагачі, що вимагають викуп.

2. Як платформа, метою якої є «накручування» кількості кліків за посиланням.

3. Відкриття проксі-серверів для анонімізації доступу до мережі Інтернет.

4. Проведення масових спам-розсилок електронних листів та хостинг фішингових (підроблених) сайтів.

5. Виведення ліцензійних даних на програмне забезпечення або CD-ключів.

6. Викрадення персональної ідентифікаційної інформації.

7. Викрадення даних кредитних карток та іншої інформацію щодо банківського рахунку, включаючи PIN-коди та/або «таємні» паролі.

8. Установка кейлоггерів для перехоплення всієї інформації, яку користувач вводить в систему.

9. Здійснення спроб злому інтернет-систем методом брутфорсу (прямий перебір або метод «грубою сили»)

Простота, з якою можна створити, змінити та кастомізувати різноманітні компоненти шкідливого програмного забезпечення ботнету - важливий фактор, який сприяє популяризації використання ботнетів у кіберзлочинних колах. Ще в 2015 році, коли у відкритому доступі виявили вихідний код LizardStresser,

інструментарію для проведення DDoS-атак, створеного відомою хакерською групою Lizard Squad, з'явилась можливість швидкого створення ботнетів. На сьогоднішній день навіть дитина з базовими комп'ютерними знаннями може налаштувати ботнет для проведення DDoS-атак.

Незважаючи на доступність і простий у використанні код LizardStresser, він також містить деякі складні методи для проведення DDoS-атак: тримати відкритим з'єднання за протоколом TCP, посилати випадкові рядки зі змістом символів на TCP-порт або UDP-порт і так далі, Шкідливе програмне забезпечення також включало в себе механізм, який дозволяє завантажувати та встановлювати оновлення LizardStresser, які включали нові команди та оновлений список заражених пристроїв, а також встановлення додаткового шкідливого програмного забезпечення. З того часу були опубліковані вихідні коди інших шкідливих програм для організації та контролю ботнетів, включаючи, в першу чергу, програмне забезпечення Mirai, що суттєво зменшило «високотехнологічний бар'єр» для початку кримінальної активності і, в той же час, збільшило гнучкість застосування ботнетів та можливості для отримання прибутку.

До появи колосальних за своїм масштабом ботнетів призвело масове використання незахищених IoT-пристроїв (рисунок 2.3). Це мало вибухоподібний ефект з точки зору кількості заражених пристроїв та трафіку, який вони генерували під час атак. Таким чином, наприклад, влітку 2016 року під час проведення у Ріо-де-Жанейро Олімпійських Ігор один із ботнетів, створений на основі LizardStresser, в основному використав близько 10 тис. заражених IoT-пристроїв (насамперед — веб-камери) для здійснення численних і тривалих у часі DDoS-атак зі стійкою потужністю понад 400 Гбіт/с, що під час свого піку досягла значення 540 Гбіт/с. Відзначимо, що, згідно з приблизними оцінками, оригінальний ботнет Mirai зміг скомпрометувати близько 500 тис. IoT-пристроїв по всьому світу.

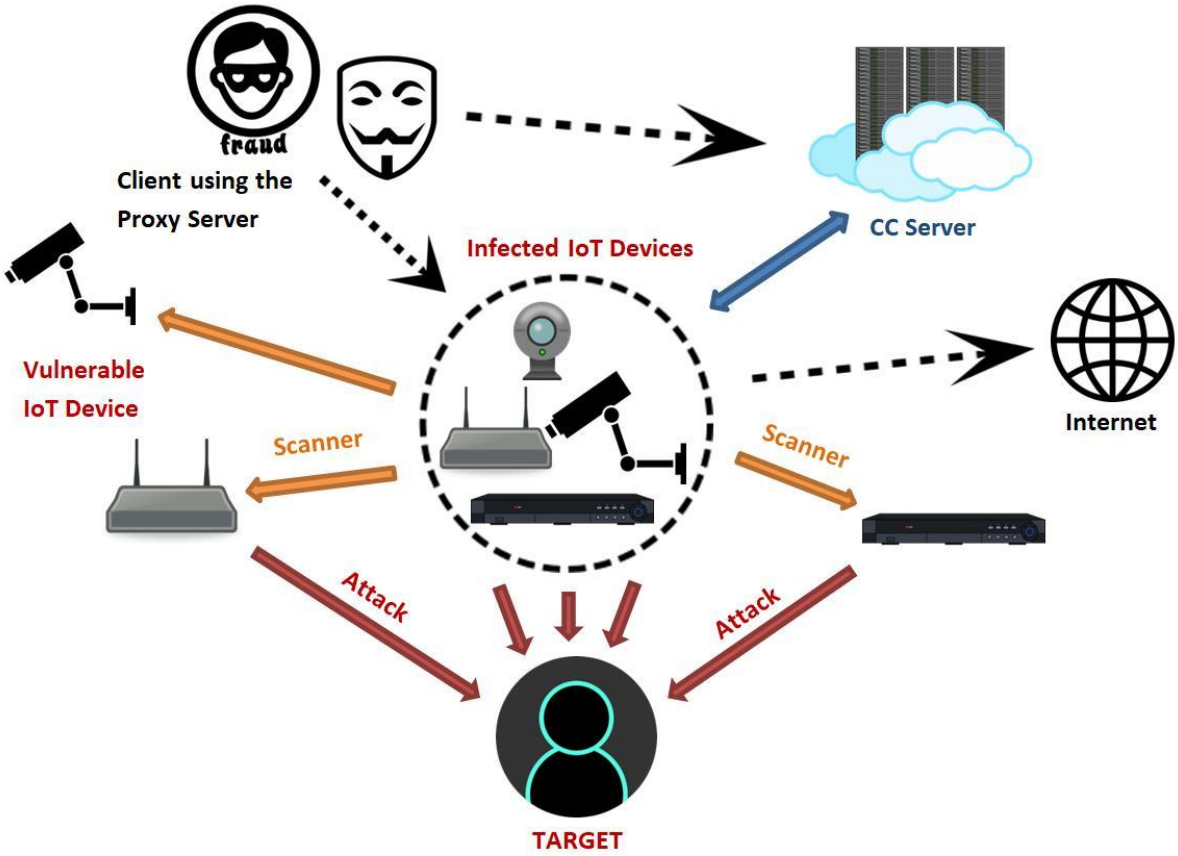

Рис. 2.3 Використання IoT-пристроїв в схемах ботнетів

Після подібних атак багато виробників почали вносити деякі зміни до своїх пристроїв. Але незважаючи на це, більшість IoT-пристроїв досі поставляються з відомими вразливостями безпеки або із заводськими налаштуваннями логіна та пароля. Більш того, з метою економії грошей та часу, деякі виробники з певною періодичністю дублюють програмне та апаратне забезпечення для пристроїв різного класу. Це в свою чергу призводить до того, що паролі за замовченням від одного пристрою можуть бути використані для безлічі інших IoT-пристроїв. Таким чином, у використанні вже мільярди незахищених IoT-пристроїв. Не зважаючи на те, що прогнозується зменшення їхньої кількості, очікуване в найближчому майбутньому розширення списку «потенційно небезпечних» IoT-пристроїв не може не вражати (див. рис. 2.4).

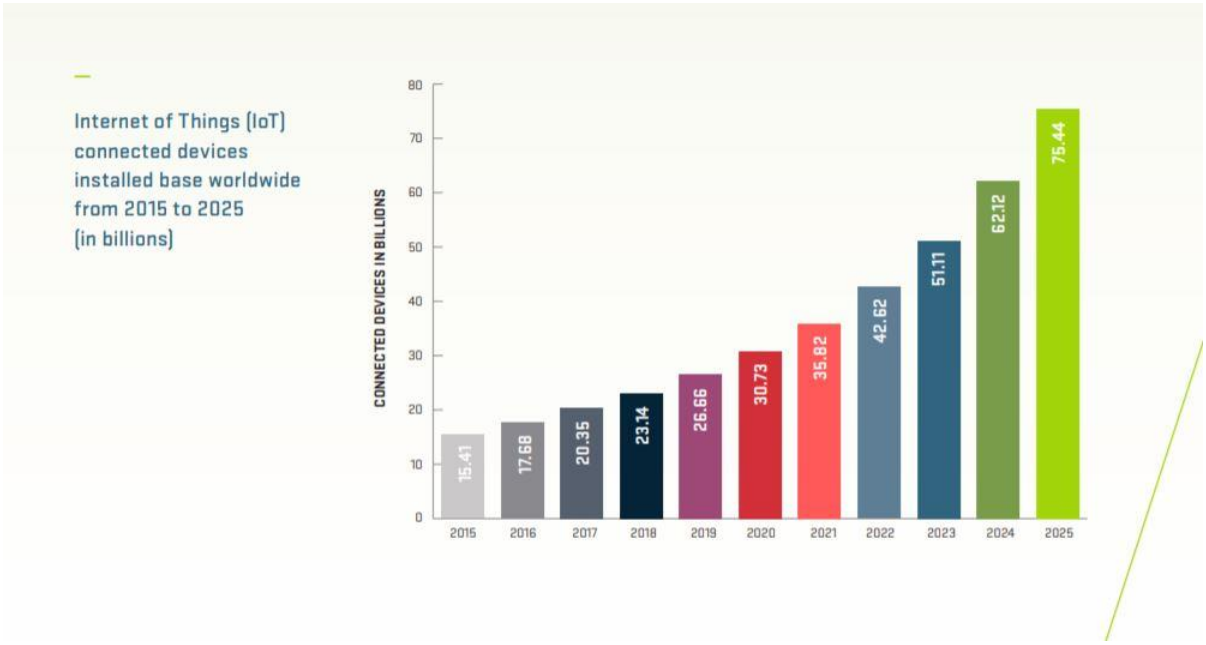

Рис. 2.4 Гістограма зростання кількості IoT-пристроїв

Багато IoT-пристроїв чудово підходять для неправомірного використання у складі злочинних ботнетів, так як:

- У більшості своїй вони некеровані, іншими словами, працюють без належного контролю з боку системного адміністратора, що робить їх застосування як анонімних проксі надзвичайно ефективним.

- Зазвичай вони знаходяться онлайн 24×7, а значить – вони доступні для здійснення атак у будь-який час, причому, як правило, без будь-яких обмежень за пропускною здатністю або фільтрацією трафіку.

- Вони часто використовують урізану версію операційної системи, реалізовану з урахуванням сімейства Linux. А шкідливе програмне забезпечення ботнетів може бути легко скомпільовано для широко використовуваних архітектур, в основному – ARM/MIPS/x86. цих пристроїв.

- Урізана операційна система автоматично означає менше можливостей для реалізації функцій безпеки, включаючи формування звітності, тому більшість загроз залишаються непоміченими власниками цих пристроїв.

Ось ще один приклад [11], який допоможе усвідомити ту міць, яку можуть мати сучасні кримінальні інфраструктури ботнету: у листопаді 2017 року ботнет Necurs здійснив розсилку нового штаму вірусу-шифрувальника Scarab. В результаті масової компанії було відправлено близько 12,5 млн. інфікованих

електронних листів, тобто швидкість розсилки склала більш ніж 2 млн. листів на годину. До речі, цей же ботнет був помічений у поширенні банківських троянів Dridex та Trickbot, а також вірусів-здирників Locky та Jans.

У квітні 2020 року Microsoft заявила, що спонсорована нею група міжнародних експертів у галузі права та інтернет-безпеки Digital Crimes Unit (DCU) виявила та допомогла правоохоронним органам знищити ботнет із 400 000 скомпрометованих пристроїв, керованих за допомогою світлодіодної консолі.

Ботнет використовувався для різних цілей: від фішингових кампаній, поширення шкідливих програм, передачі даних здирникам і до запуску розподілених атак типу DDoS.

В Microsoft зазначили, що ці дії пов'язані з цілим терабайтом (ТБ) шкідливого контенту, що відправляється щотижня. Спочатку DCU вивчила понад 400 000 скомпрометованих IP-адрес і в результаті скоротила список до 90 підозрілих IP. Наступний аналіз показав, що один з них був пов'язаний з десятками дій з поширення шкідливих програм, фішингових листів і DDoS-атак.

Агенти Бюро розслідувань Міністерства юстиції (Ministry of Justice Investigation Bureau, MJIB) змогли відстежити IP-адресу, що стоїть за цими атаками, і виявили, що кілька облікових записів, прихованих VPN-мережею, що використовує IP, знаходилися в офісній будівлі на півночі Тайваню.

В Microsoft пояснили, що зазвичай кіберзлочинці використовують скомпрометовані ПК для запуску кібератак, але цього разу джерело було ідентифіковано як консоль керування світлодіодним освітленням, що на перший погляд є незначним пристроєм IoT.

Ботнет виявили після того, як аналітик DCU з Тайваню помітив дивний сплеск сигналу, який збільшився більш ніж у 100 разів за один місяць. За словами Фу-Мей Ву, директора відділу інформаційної та комунікаційної безпеки MJIB, вони змогли нейтралізувати пристрій IoT та зафіксувати злом на обмеженому діапазоні для скомпрометованих комп'ютерів у Тайвані, що дуже відрізняється від попередніх випадків глобальної співпраці.

У березні 2020 року Microsoft та галузеві партнери скоординували знищення Necurs, одного з найбільших спам-ботнетів, відомого тим, що він з 2012 року розповсюджував шкідливі програми, які використовуються для зараження мільйонів комп'ютерів. Один заражений Necurs пристрій відправив приблизно 3,8 мільйона спам-повідомлень на більш ніж 40,6 мільйонів цілей протягом 58 днів. Відключило комп'ютерну мережу однієї з організацій після того, як співробітник компанії відкрив лист із фішинговим посиланням. Збій в роботі мережі стався через зростання максимального навантаження на ЦП під керуванням Windows і відключення інтернет-з'єднань. через вісім днів вся мережа вийшла з ладу через перегрівання, зависання та перезавантаження ПК. У Microsoft впоралися з поширенням шкідливих даних, застосувавши елементи управління ресурсами та буферні зони, призначені для ізоляції активів з правами адміністратора.

Усього з 2010 року команда Microsoft DCU [5] виявила 22 ботнети за допомогою інтернет-провайдерів, реєстрів доменів, урядових CERT та правоохоронних органів всього світу.

Що стосовно України, то у 2009 році фахівці з безпеки компанії Finjan виявили новий гігантський ботнет [31]. Число ПК-зомбі зростало щогодини. За добу лічильник показував 1.953.448 заражених машин (див. рисунок 2.5). Серед заражених - корпоративні мережі, великі банки та 77 державних організацій різних країн. За першими оцінками, ця мережа перевершує навіть знаменитий ботнет Storm.

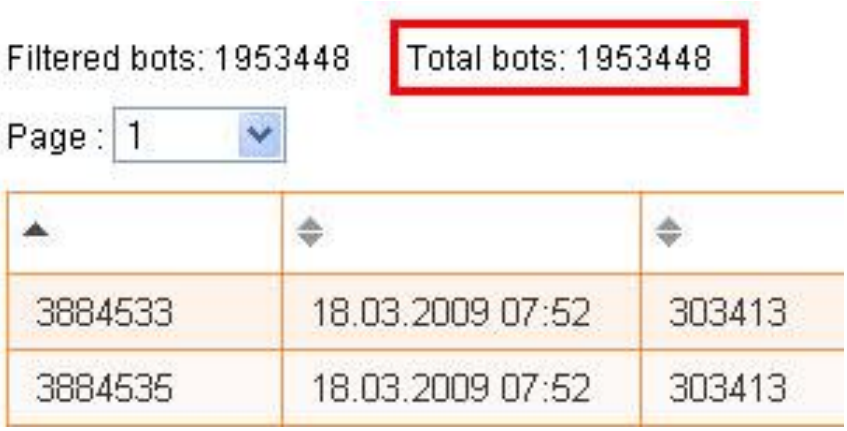

Рис. 2.5 Динаміка зараження ПК ботнетом, керованим із України (2009)

Що найцікавіше, управління ботнетом здійснювалося з України. Було ідентифіковано шістьох осіб, які брали участь у цьому. На одному з російських хакерських форумів виявлено комерційну пропозицію з оренди ботнета. Тільки 4 з 39 популярних антивірусних пакетів були здатні виявити троян, через який здійснювалося управління інфікованою системою. Це AVG, DrWeb, NOD32 та Panda.

Ще один приклад українського походження розкрито у жовтні цього року. Служба безпеки України (СБУ) повідомила про арешт оператора, який керував великим ботнетом, що налічує понад 100 тис. заражених пристроїв.

За заявою правоохоронних органів, зловмисник використав ботнет для проведення різноманітних атак, включаючи DDoS, спам, брутфорс поштових скриньок користувачів, пошук вразливостей веб-сайтів та їх зламування, а також іншу незаконну діяльність.

У поясненні СБУ зазначено, що деякі клієнти ботнету задіяли його для проведення «пентестів» у своїх організаціях і не лише.

Власник ботнета розповів на допиті, що розміщував оголошення про оренду ботнета на хакерських форумах та у спеціальних закритих чатах Telegram. Клієнти з ним зв'язувалися анонімно і використовували для оплати різні електронні платіжні системи, включаючи Webmoney. Саме через цю хакерську систему його знайшла СБУ. Він зареєстрував обліковий запис на Webmoney із зазначенням своєї реальної адреси проживання, що дозволило українській поліції дізнатися, де він знаходиться та провести затримання.

СБУ пояснила, що під час обшуків вилучило у підозрюваного комп'ютерне обладнання із доказами протиправної діяльності. Хакеру загрожує кримінальне покарання за правопорушення, згідно з ч. 2 ст. 361-1 (створення з метою використання, розповсюдження чи збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження чи збут) та ст. 363-1 (запобігання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку шляхом масового поширення повідомлень електрозв'язку) КК України.

Завдавати шкоди та приносити збитки ботнети можуть не тільки у комп'ютерному середовищі та мережах. Так у липні цього року українські силовики за несплату електроенергії закрили велику ботоферму із приставками в одному із колишніх приміщень «Вінницяобленерго».

СБУ оголосила про припинення роботи найбільшої у країні нелегальної крипто ферми. Близько 5 тисяч пристроїв для майнінгу розташовувалися в одному з колишніх приміщень «Вінницяобленерго». Їх незаконно живили енергією від мереж компанії.

Як встановили у СБУ, власниками незаконної криптоферми були мешканці Києва та Вінниці. За попередніми підрахунками, щомісячна сума збитків від діяльності нелегальних майнерів становила від 5 до 7 млн. гривень.

При цьому, як стверджують силовики, незаконний відбір електроенергії загрожував залишити без світла цілі квартали у Вінниці.

За місцем розташування криптоферми та за адресами проживання підозрюваних вилучили 3,5 тисячі ігрових приставок, понад 500 відеокарт, 50 процесорів, а також документацію з обліку споживання електроенергії, блокноти, телефони та флеш-накопичувачі.

Висновки до розділу 2

Таким чином, до основних актуальних загроз інформаційній безпеці банків можна віднести атаки на процесингові центри банків із виведенням коштів через банкомати, атаки зловмисників на системи дистанційного банківського обслуговування (ДБО) клієнтів, шахрайство з використанням методів соціальної інженерії та здирство. Також варто відмітити людський фактор – основна та головна загроза інформаційної безпеки, що прямо залежить від людських відносин. Витік інформації найчастіше відбувається з провини банківського персоналу.

Атаки типу APT досі залишаються одними з найбільш поширених та небезпечних для банківської сфери. Такі атаки добре сплановані та при

належному фінансуванні можуть тривати багато місяців. До основних етапів APT-атак відносять: підготовка, проникнення, розповсюдження, досягнення цілей.

Сприятлива ситуація для кіберзлочинців, яка створилась в останні роки, пов'язана з високою доступністю та простотою використання більш складного та гнучкого шкідливого програмного забезпечення для ботнетів у поєднанні зі значним приростом кількості незахищених IoT-пристроїв. Це зробило кримінальні ботнети основним компонентом зростаючої цифрової підпільної економіки.

Розділ 3
ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

3.1 Аналіз та оцінка ризиків інформаційної безпеки банку

З погляду інформаційної безпеки у банках можна виділити п'ять головних передумов нових ризиків інформаційної безпеки:

1. віддалена інфраструктура та пов'язані з цим атаки (наприклад, атака на новозеландську біржу, що призвела до тривалого простою);

2. масові ризики використання особистих пристроїв (багато кейсів, коли зловмисник проникав на кінцеві устрою);

3. зниження уважності на віддаленій роботі, у результаті користувач стає більш вразливим для фішингу;

4. втрата логінів та паролів;

5. загальний спад економіки.

А тепер приходить усвідомлення того, що в Україні в нашій поточній дійсності ми опинилися в іншій реальності. І за останній рік виникли передумови для формування нового порядку денного ІБ у фінансовому секторі. Одна з передумов – зростання цифрового бізнесу, причому не тільки в технологічному секторі, а й у реальному, виробничому, де компанії починають розвивати свій бізнес з допомогою технологічних продуктів.

Ще одна передумова – зростання кількості вразливостей, зокрема вразливостей нульового дня. Минулого року було поставлено абсолютний рекорд за кількістю виявлених вразливостей. Гонка за прибутком тепер починається в цифровому світі, швидко з'являються нові технології, але не встигають опрацьовувати повний цикл пошуку вразливостей, відповідно останніх з'являється все більше.

Окремим пунктом можна визначити підвищення регуляторного навантаження (див. розділ 1 пп. 1.2-1.3). Регуляторних вимог стає дедалі більше,

бо регулятори бачать цю гонку, розуміють, що громадян треба захищати від цілого валу вразливостей.

У фінсекторі тепер регулятор проникає у всі процеси. Раніше такого не було. Раніше була вимога щодо захисту систем, потім з'явилися регуляторні вимоги, пов'язані з продуктами, а тепер уже є вимоги, пов'язані з процесами розробки та експлуатації програмних продуктів.

До списку можна додати і кадровий голод: згідно з офіційною статистикою в Україні щороку не вистачає близько 10 000 фахівців з ІБ. У країні немає таких потужностей, щоби цей кадровий голод закрити.

Отже, з одного боку, йде прискорення цифровізації та є необхідність допомагати бізнесу заробляти, а з іншого – є величезна кількість формальних вимог та нові перевірки Нацбанку України, які більшою мірою перевіряють на формальну відповідність вимогам щодо захисту інформації.

У цій ситуації незрозуміло, що робити фахівцеві з ІБ: з одного боку, він живе в страху, що його можуть вигнати, оскільки він порушив вимоги НБ, а з іншого – він розуміє, що загрози, ймовірно, не там і робити треба не те. Частково розвантажити ситуацію можна, винісши частину формальних та реальних ІБ-ризиків на обробку до ІТ-департаменту та синхронізуючи стратегії ІТ та ІБ компанії.

Необхідна синергія ІТ та ІБ. У ІТ теж кадровий голод, і треба взаємодіяти, щоб синхронізувати роботу, стратегії розвитку ІТ та ІБ. Крім того, потрібна взаємодія з держорганами у питаннях політик та стандартів інформаційної безпеки.

Якийсь час тому систему інформаційної безпеки зазвичай розділяли на дві частини: захист периметра обчислювальної мережі організації та захист внутрішніх хостів [7]. В якості периметрових засобів захисту використовувалися:

- системи міжмережевого екранування (МСЕ);
- системи виявлення/запобігання атак (IDS/IPS);
- модулі DLP-систем для контролю поштового та Web-трафіку;

- системи контентної фільтрації при доступі працівників організації в мережу Інтернет;

- антивірусні засоби на поштовому сервері та на проксі-сервері доступу до мережі Інтернет та ін.

В якості захисту хостів, як правило, застосовувалися:

- антивірусні засоби;

- персональні МСЕ;

- хостові модулі систем IDS/IPS;

- хостові модулі DLP-систем;

- засоби контролю використання працівником периферійних пристроїв, насамперед USB-накопичувачів.

Багато рішень захисту кінцевих пристроїв (Endpoint) останнім часом стали поєднувати у собі значну частину перерахованого функціоналу.

Більше того, останнім часом і в периметрову, і в хостову частини стали додавати засоби захисту від атак, що таргетують (засоби класу APT, EDR). Крім того, розробники приділяють увагу взаємодії периметрових та хостових засобів захисту для підвищення ефективності виявлення та протидії сучасним кібератакам. Тому найчастіше використання периметрових та хостових засобів захисту одного виробника має додаткові бонуси щодо більш тісної взаємодії цих засобів між собою.

Конкретний засіб захисту – це лише інструмент, який є найефективнішим буде тільки в руках професіонала. Тому запорукою ефективності використання того чи іншого засобу захисту є правильно збудований процес та кваліфікація персоналу, що його здійснює. Можна виділити такі процеси верхнього рівня:

- захист від шкідливого ПЗ;

- захист від витоку даних;

- захист систем електронного документообігу;

- захист обчислювальних мереж ;

- захист інформації у мобільних користувачів;

- управління правами доступу;

- управління вразливістю;
- моніторинг і реагування на інциденти ІБ;
- управління інформаційними активами;
- управління ризиками ІБ;
- управління відповідністю (комплайнсом);
- безпечна розробка ПЗ;
- підвищення обізнаності співробітників з питань ІБ.

На відміну від інших компаній, у фінансових установах системи забезпечення інформаційної безпеки охоплюють сферу захисту платіжних процесів та платіжної інфраструктури. Цій складовій у банках приділяється особлива увага.

В останні роки з'явилася тенденція ділити сферу інформаційної безпеки на класичну інформаційну безпеку та кіберзахист. Справа в тому, що сучасні кіберзагрози не завжди вкладаються в парадигму забезпечення конфіденційності, цілісності та доступності інформації, яку сповідує класична ІБ. Наприклад, незрозуміло, як у цій парадигмі розглядати атаки на пристрої та на людину, чи проведення інформаційних атак, заснованих на споконвічно недостовірній інформації, сфабрикованих даних (маніпуляція суспільною свідомістю). Але якоїсь загальноприйнятої практики щодо подібного поділу в Україні поки що відбулося.

Особливості систем ІБ у банках пов'язані передусім із тим, що у них обробляється інформація про реальні кошти, розрахункові рахунки, грошові перекази, і навіть з тим, що з цих автоматизованих систем здійснюється управління пристроями видачі грошей – банкоматами. Тому значні зусилля фахівців із ІБ у фінансових організаціях спрямовані на захист платіжної інфраструктури та платіжних процесів.

На відміну від інших організацій, у банках існує поняття банківської таємниці – це інформація про операції, рахунки та вклади клієнтів та кореспондентів банку. Так як більшість банківських операцій і більшість оброблюваної в банку інформації відносяться до банківської таємниці, завдання

забезпечення її захисту може бути вирішена тільки шляхом побудови складної комплексної системи захисту. Така сама ситуація складається і з захистом персональних даних. У банках вони обробляються у значних обсягах, тому їх необхідно захищати відповідно до закону України «про персональні дані».

Вимоги до постачальників і виробників обладнання для інформаційної безпеки досить стандартні: функціональність, надійність, простота та зручність експлуатації при прийнятній вартості.

В даний час зростає роль ефективної взаємодії засобів захисту між собою та з системами управління інформаційною безпекою. Добре, коли різні продукти одного виробника ефективно інтегруються одне з одним, але така ж ефективна взаємодія необхідна і від рішень різних виробників.

Дуже бажано, щоб провідними гравцями в IT- та ІБ-секторах вкладалися кошти в перспективні дослідження та розробки і щоб системи інформаційної безпеки вдосконалювалися не у зв'язку з злочинами, а дозволяли запобігти в тому числі абсолютно нові, ще раніше невідомі типи атак.

Будь-які рішення та послуги у сфері ІБ вимагають постійного вдосконалення та розвитку. Вони повинні бути адекватні сучасним загрозам, які, у свою чергу, теж постійно розвиваються і вдосконалюються.

І, безумовно, завдання виробників і постачальників рішень з ІБ не в тому, щоб продати ці рішення, а у тому, щоб ці рішення ефективно функціонували і приносили організаціям, де вони працюють, реальну користь. Тому потрібна активна їхня участь на етапі як впровадження продукту, так і його експлуатації.

Сучасні системи ІБ намагаються максимально використовувати нові технології. Насамперед це BigData, машинне навчання, нейронні мережі, штучний інтелект.

На даний момент ці технології активно використовуються в системах фрод-аналізу, тобто для боротьби із зовнішнім та внутрішнім шахрайством.

Досить перспективними є системи, які самонавчаються. Фахівцям з ІБ все складніше наздогнати мільйони змін у сучасних цифрових технологіях і сервісах, кожна з яких може нести певні загрози. Тому все частіше використовуються

системи, що ґрунтуються на виявленні аномалій. Вони будують і постійно актуалізують «нормальну» поведінку об'єкта або людини і реагують на суттєві відхилення від цієї «нормальної» поведінки.

Жодна сучасна система ІБ не обходиться без використання хмарних сервісів. Більшість провідних виробників в області ІБ збирають інформацію зі своїх рішень, встановлених у всьому світі, в онлайн-режимі та агрегують цю інформацію у себе в хмарних сервісах. Підключаючи до системи ІБ такий хмарний сервіс, ви отримуєте можливість використовувати всю цю інформацію.

Єдина система ідентифікації та аутентифікації (ЄСІА).

Ідея єдиної системи віддаленої ідентифікації цікава та актуальна. Наявність у державі єдиної централізованої довіреної системи ідентифікації та аутентифікації громадян дозволило б вирішити низку серйозних проблем. Використання даної системи покликане суттєво спростити для банків завдання ідентифікації клієнтів відповідно до дійсного законодавства «про протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом, та фінансуванню тероризму» та просування своїх продуктів та послуг, у тому числі в регіонах, де немає фізичної присутності конкретної фінансової організації.

Але реальну користь система ЄСІА принесе лише в тому випадку, якщо в ній зберігатимуться біометричні дані значної кількості жителів України. На даний момент не зовсім зрозуміло, що спонукає людину реєструвати у системі ЄСІА свої біометричні дані. Якщо її наповненість незначна, то вона себе не виправдає.

Спеціалісти з ІБ мають серйозні питання до обраної біометричної аутентифікації. Зрозуміло, чому в якості технології ідентифікації в ЄСІА вибрано зображення обличчя та голос. Це єдині технології біометричної аутентифікації, якими можна охопити значну кількість громадян України, оскільки вони можуть бути реалізовані за допомогою мобільного телефону. Але вони мають серйозні недоліки. Тому, на мою думку, впровадження ЄСІА не зможе стати проривом у системі ІБ банків.

3.2 Захист банківської інформації від кіберзагроз APT-атак та ботнетів

Основними засобами захисту від цільових атак сьогодні є засоби детектування різноманітних аномалій (коду, команд, поведінки тощо). При цьому детектування аномалій в рамках окремо взятого комп'ютера, або корпоративної ІС в цілому, здійснюється з метою виявлення реалізованих, а також частково, або повністю реалізованих атак.

Крім того забезпечується можливість нейтралізації відомих атак на ранніх стадіях їх здійснення – вирішується завдання захисту інформації, що забезпечується можливістю однозначної ідентифікації виявленої аномалії як події реалізації атаки, як наслідок, здійснення автоматичної реакції на зафіксовану аномальну подію.

Щодо невідомих загроз атак, до яких належать загрози цільових атак, детектування аномалій неминуче пов'язане з помилками першого (при поверхневому аналізі подій) та другого (при глибокому аналізі) роду. В даному випадку, особливо при глибокому аналізі, а інакше будь-якого сенсу детектування аномалій не має, технологічно неможлива однозначна ідентифікація виявленої аномалії як події реалізації атаки, внаслідок чого неможлива і автоматична реакція на зареєстровану подію, яка лише з певною ймовірністю може бути атакою. Завдання детектування аномалій в даному випадку зводиться не до захисту інформації, а до проведення відповідного подальшого дослідження щодо зареєстрованого факту реалізації атаки з метою максимально оперативної однозначної ідентифікації атаки.

Після однозначної ідентифікації аномалії, як атаки (атака стає відомою, та її загроза не загроза цільової, а загроза масової атаки), щодо цієї атаки детектором аномалій вже реалізується захист інформації.

Практично всі вендори мають у своїй лінійці продукт, який позиціонується як засіб захисту від таргетованих атак. До них можна віднести FireEye, CheckPoint, McAfee і т. ін. Ефективність захисту від таргетованих атак

неспроможна повністю визначатися лише технічними засобами, які використовуються.

Технології захисту від націлених атак були і раніше, але зараз вони виходять на новий рівень. У першу чергу йдеться про різні інструменти виявлення аномалій – як на локальних комп'ютерах, так і на рівні мережевої активності рисунок 3.1).

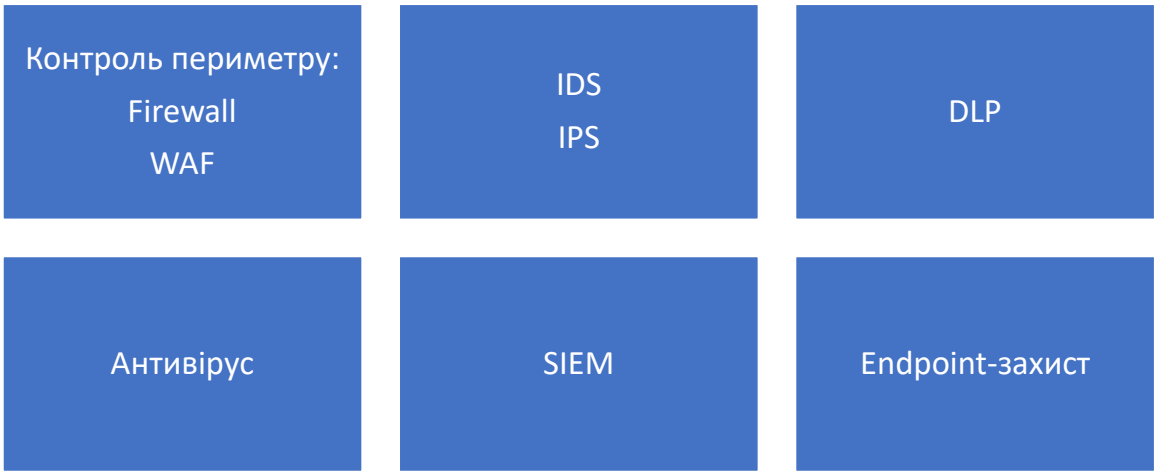

Рис. 3.1 Інструменти виявлення аномалій

Завданням таких систем є пошук всього незвичайного, що відбувається, а не пошук шкідливого коду. Це пояснюється тим, що у багатьох випадках атакуючі можуть взагалі не використовувати шкідливі програми.

Останнім часом традиційних систем захисту стає недостатньо. Це відбувається внаслідок специфіки цілеспрямованих атак і підготовки до них, а також внаслідок технологічних обмежень, що властиві традиційним засобам захисту.

Через специфіки цілеспрямованих атак і підготовки до них, таких як:

- детальне вивчення засобів захисту з метою їх обходу;

- написання унікального ПЗ і закріплення його в інфраструктурі мети;

- використання в атаках довірених, але скомпрометованих об'єктів, що не створюють негативний фон;

- застосування мультивекторного підходу до проникнення;

- прихованість та ін.

Через властиві традиційним засобам захисту технологічні обмеження:

- виявлення спрямоване лише на поширені (нескладні) загрози, вже відомі вразливості та методи;

- немає вбудованого зіставлення та кореляції детектів в єдиний ланцюжок подій;

- немає технологій виявлення відхилень у нормальних активностях та аналізу роботи легітимного ПЗ.

Етапи з вирішення задач інформаційної безпеки зображено на рис. 3.2.

Рис. 3.2 Етапи вирішення задач інформаційної безпеки

Традиційні засоби захисту (антивіруси, файєрволи тощо) на сьогоднішній день не здатні ефективно протистояти сучасним кіберзлочинцям. Для захисту інформаційної системи організації потрібен комплексний підхід, який поєднує кілька кордонів захисту із застосуванням різних технологій безпеки (таблиця 3.1)

При чому використання традиційних рішень ешелонованого захисту (NGFW, EPP) містить:

- ефективна боротьба проти класифікованих типів (нескладних) загроз;

- автоматичне блокування, без необхідності розслідування інцидентів;

- виключення зі спектра аналізу розповсюджених загроз;

- скорочення обсягу пошуку, допомога в аналізі просунутих загроз.

Таблиця 3.1

Комплексний підхід до захисту інформаційної системи банку

Вид загроз	Характеристики	Дія	Вид рішення
Поширені загрози	Відомі	Запобігання	Використання традиційних рішень ешелонованого захисту (NGFW, EPP):
	Нескладні нові		
	Атаки нульового дня		
	Невідомі, що базується на фундаменті вже відомих шкідливих об’єктів		
Просунуті загрози	Складні нові, раніше невідомі	Визначення + Реагування	Використання спеціалізованих рішень
	Атаки з використанням скомпрометованих об’єктів, які не створюють негативний фон		
	Комплексні загрози		
	Загрози рівня APT		

А використання спеціалізованих рішень передбачає:

- визначення складних атак із зіставленням різних подій в єдиний інцидент;

- ретроспективний аналіз;

- багаторівневі механізми визначення на базі динамічного машинного навчання та поведінкового аналізу;

- відправка вердиктів у NGFW та EPP.

Загалом, у комплексному проекті треба враховувати багато чинників. Наприклад, з боку сервісів, це будуть наступні елементи:

- навчання IT-адміністратора;

- тренінг по роботі із системами;

- навчання розслідуванню інцидентів;

- тренінги з Yara-правилами;

- сервіси з активного пошуку загроз;

- цифрова криміналістика;

- портал аналітичних звітів про загрози;

- аналітика подій ІБ та реагування на інциденти.

З боку підтримки:

- професійні сервіси;
- виділений експерт з ІБ;
- розширена технічна підтримка.

З боку рішень:

- мережеві рішення захисту;
- захист робочих місць;
- спеціалізоване рішення з визначення загроз;
- спеціалізоване рішення з реагування;
- локальна репутаційна база загроз для ізольованих середовищ.

При чому варто відзначити ще ті моменти, які враховуються при виборі рішень:

- цілісний підхід до визначення складних загроз;
- автоматизована протидія знайденим загрозам;
- відповідність вимогам ізоляції, реєстр з ПЗ України, сертифікація;
- автоматизовані засоби розслідування інцидентів;
- експертна допомога у виявленні загроз;
- багаторівневі детектуючі технології.

Для захисту від зовнішніх Інтернет загроз інформаційній безпеці відмінно зарекомендували себе системи запобігання вторгненням на рівні хоста (HIPS). Правильно налаштована система дає безпрецедентний рівень захищеності, близький до 100%. Грамотно вироблена політика безпеки, застосування спільно з HIPS інших програмних засобів захисту (наприклад, антивірусного пакета) надають дуже високий рівень безпеки. Організація отримує захист практично від усіх типів шкідливого ПЗ, значно ускладнює роботу хакера, який вирішив спробувати пробити інформаційний захист підприємства, зберігає інтелектуальну власність та важливі дані організації.

Захист від внутрішніх загроз також потребує комплексного підходу. Він виявляється у виробленні належних політик інформаційної безпеки,

запровадженням чіткої організаційної структури відповідальних за інформаційну безпеку співробітників, контролю документообігу, контролю та моніторингу користувачів, запровадження просунутих механізмів аутентифікації для доступу до інформації різного ступеня важливості. Ступінь такого захисту залежить від об'єктивних потреб організації захисту інформації. Далеко не всім об'єктам потрібна дорога DLP-система, що дає непогані результати захисту даних підприємства від витоків, але вимагає найскладнішої процедури впровадження та перегляду поточних механізмів документообігу. Оптимальним вибором для більшості компаній стане запровадження функціоналу захисту від витоків даних, контролю документообігу та моніторингу дій користувачів локальної мережі організації. Таке рішення є недорогим, простим у розгортанні та експлуатації, але дуже ефективним інструментом інформаційної безпеки.

Нові засоби з'явилися і продовжують з'являтися. Однак їх ефективність безпосередньо залежить від якості їх налаштування (рисунок 3.3).

Основними технологічними напрямками засобів захисту є:

- пісочниці, які імітують робочі станції організації. У пісочницях файли, одержувані з Інтернету, запускаються та аналізуються. Якщо файл, що запускається, тягне за собою деструктивну дію, то такий файл визначається як заражений;

- аналіз аномальної мережевої активності (наприклад, на базі NetFlow), який здійснюється шляхом порівняння поточної мережної активності з побудованою еталонною моделлю мережевої поведінки. Наприклад, комп'ютер або сервер, який завжди комунікує з деяким набором певних мережевих ресурсів за певними протоколами, раптом несподівано починає пробувати звертатися безпосередньо до баз даних;

- поведінковий аналіз робочих станцій, також заснований на порівнянні активності робочих станцій із еталонною моделлю. Різниця в тому, що цей аналіз здійснюється не на рівні мережі, але в рівні самої робочої станції з допомогою агентів. Нещодавно з'явилася цікава технологія, яка відстежує процеси Windows.

У разі відхилення від еталонної моделі процес Windows блокується, тим самим не даючи експлойту виконати деструктивну дію.

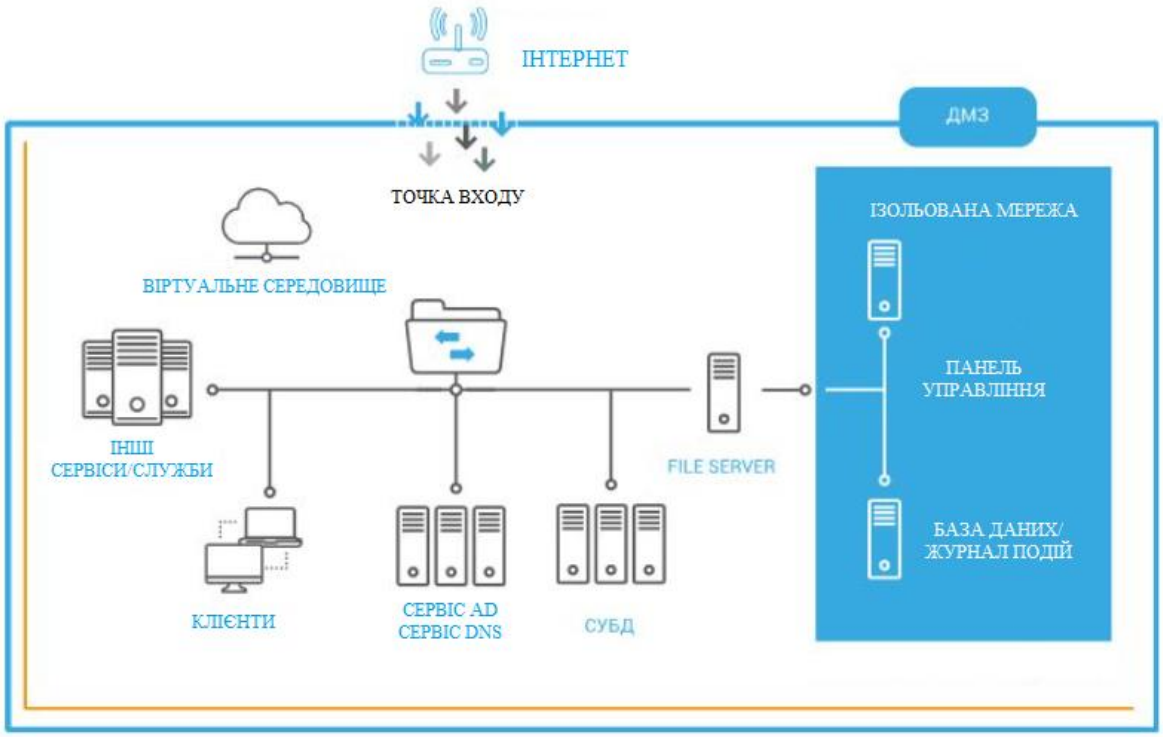

Рис. 3.3 Компоненти захисту від атак

Deception – мережа замаскованих мережевих пасток та приманок, які розкидані по всій IT-інфраструктурі та забезпечує:

- виявлення в режимі реального часу цілеспрямованих атак та атак нульового дня;

- захист реальних IT-активів за рахунок перемикання активності атакуючих на «пастки»;

- захист цінних даних від «шифрувальників»;

- збір доказів комп'ютерної криміналістики про дії зловмисників;

- відсутність помилкових спрацьовувань;

- не використовує агентів і не впливає на роботу користувачів та IT-сервісів.

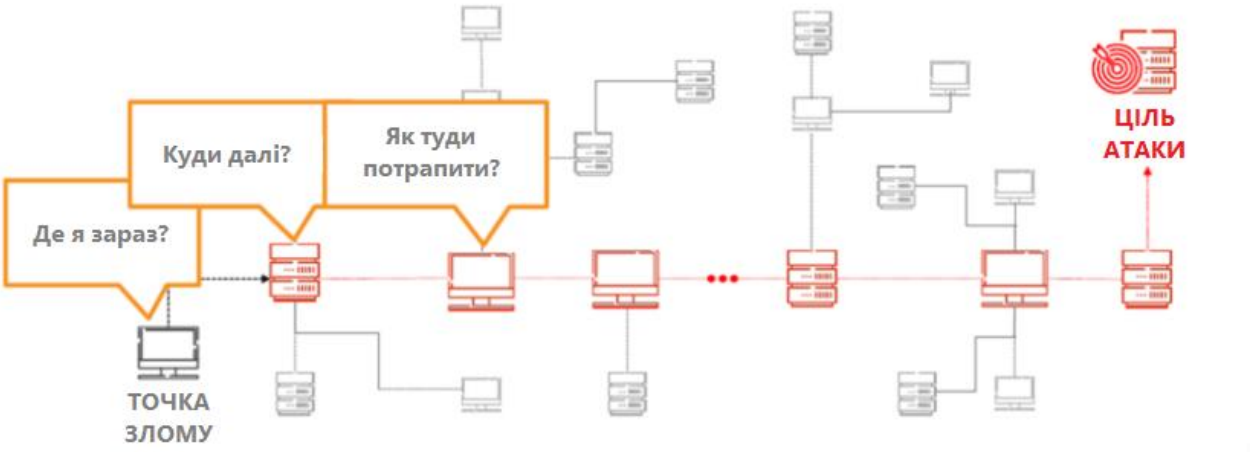

Рис. 3.4 Алгоритм дії хакера

Результати:

- Профіль зловмисника;
- Деталізовані методи та інструменти, що використовуються під час атаки;
- Поглиблений аналіз (які цілі переслідують хакери, яку інформацію вони шукають);
- Історія та хронологія злому;
- Джерела походження зловмисників на основі їх IP-адрес та даних DNS.

3.3 Навчання персоналу банку з питань інформаційної безпеки

Сучасна людина має багато знати та вміти в галузі інформаційних технологій. Розвиток технологій та впровадження нових засобів обробки інформації потребують впевненого володіння комп'ютером (ноутбуком, планшетом, смартфоном тощо), знань великої кількості програмних продуктів та правил роботи з електронною поштою, носіями інформації, Інтернетом тощо.

При роботі використовується величезний обсяг інформації, що зберігається на різних ресурсах і становить значну цінність для компанії в цілому або для когось особисто. При цьому не важливо, де використовується комп'ютер – в офісі чи у відрядженні, на відпочинку чи вдома: з розвитком мережевих технологій рівень доступу до ресурсів зростає, як і кількість різноманітних атак на ці ресурси.

У сучасних умовах поряд зі знанням основних виробничих технологій від працівника потрібно знання специфічних питань, пов'язаних із забезпеченням ІБ, що обумовлено не лише вимогами законодавства України, міжнародними та російськими стандартами та нормативними документами компанії, а й елементарними вимогами безпеки та необхідністю збереження конфіденційної інформації у таємниці.

На жаль, багато працівників дуже далекі від питань захисту інформації і тому значна кількість інцидентів ІБ, пов'язаних насамперед з витоками конфіденційної інформації, вірусними зараженнями або знищенням/ спотворенням інформації, відбувається з вини працівників, які свідомо чи ні порушують вимоги щодо забезпечення ІБ, або просто не знають цих вимог. Більшість фахівців в області ІБ сходяться на думці, що значна частина інцидентів відбувається внаслідок ненавмисних дій: через недбалість, неуважність або просто незнання.

Отже, одним з основних факторів, які суттєво впливають на стан ІБ у компанії, є обізнаність користувачів у галузі ІБ та їх уміння застосовувати отримані знання у повсякденній діяльності, тому одне з найважливіших завдань, яке доводиться вирішувати службі ІБ, – організація навчання користувачів, причому всіх, без винятків, з питань забезпечення ІБ в рамках побудови системи підвищення поінформованості користувачів в області ІБ.

Під підвищенням обізнаності працівників підприємства у сфері ІБ розуміється цілеспрямований, організований, планомірно і систематично здійснюваний процес підвищення рівня знань працівників та формування необхідних навичок у сфері ІБ, створення корпоративної культури у цій галузі та атмосфери усвідомлення необхідності дотримання вимог ІБ.

Відповідно до цих вимог повинна бути організована документально оформлена та затверджена керівництвом робота з персоналом у цьому напрямі, включаючи розробку та реалізацію планів та програм навчання та підвищення поінформованості в галузі ІБ та контролю результатів виконання зазначених планів.

Періодичність навчання та зміст програм [19]:

- за існуючими політиками ІБ;

- щодо застосовуваних захисних заходів;

- щодо правильного використання захисних заходів відповідно до внутрішніх документів;

- щодо значущості та важливості діяльності працівників для забезпечення ІБ.

У загальному випадку до системи підвищення обізнаності працівників компанії пред'являються такі вимоги:

- можливість регулярного навчання будь-якої кількості працівників, незалежно від їхнього територіального місцезнаходження і без відриву від робочого процесу;

- простота та доступність навчальних матеріалів для різних категорій працівників;

- можливість оперативного внесення змін до програм підвищення обізнаності та навчальних матеріалів.

Важливим аспектом роботи щодо підвищення обізнаності персоналу з питань ІБ є безперервність цього процесу. Законодавство та вимоги регуляторів швидко змінюються, з'являються нові загрози ІБ, нові інформаційні системи – все це необхідно оперативно відображати у програмах підвищення обізнаності. Для працівників компанії безперервність навчання полягає у повторенні вимог та правил ІБ. Також важливо інформувати всіх працівників про зміни, що відбулися, у політиках безпеки та процедурах забезпечення ІБ.

Кінцевою метою реалізації вищезгаданих програм є зниження збитків і втрат (матеріальних, моральних, репутаційних) від загроз, пов'язаних з людським фактором при роботі з інформаційними ресурсами компанії.

Як і будь-яка система навчання, система підвищення обізнаності має на увазі використання певних форм, видів та методів навчання. Вибір того чи іншого методу або форми залежить від цілого ряду факторів, таких як: цілі

організації, кадрова політика, характеристики персоналу, що навчається, його чисельність і фінансування.

В рамках підвищення обізнаності в області ІБ навчання може проходити в наступних формах:

- очного навчання (у своїй компанії або в спеціалізованих організаціях);

- дистанційного навчання (електронні курси, у формі тестування, вебінарів, онлайн-конференцій тощо);

- самостійного вивчення навчальних матеріалів.

Розглядати очне навчання як метод регулярного підвищення обізнаності працівників з питань ІБ не завжди вигідно та ефективно, оскільки відрив від основної діяльності значної кількості працівників негативно впливає на бізнес компанії. Ця форма найбільше підходить для державних структур та невеликих компаній, де можна одночасно зібрати всіх працівників з мінімальним відривом від основної діяльності.

Для великих компаній, банків, що мають розгалужену регіональну мережу, найбільш підходящим є використання систем дистанційного навчання, які дозволяють одночасно навчати і контролювати навчання великої кількості персоналу. Сьогодні на ринку представлені різноманітні системи дистанційного навчання: Digital Security E-Learning System, Web-Tutor, ELeaP LMS та ін.). Вибір системи залежить від необхідної кількості учнів, необхідних ресурсів для розробки курсів та тестів термінів запровадження, можливості придбання готових курсів, вартості. Ряд виробників систем дистанційного навчання пропонують не лише купівлю своїх систем, а й їхню оренду.

Додатково в процесі навчання можуть використовуватися так звані нестандартні засоби, що дозволяють підтримувати атмосферу ІБ, завдяки яким працівник запам'ятовує окремі положення політики безпеки та розуміє важливість вимог ІБ на емоційному та підсвідомому рівні: скрінсейвери, відеоролики, мультимедійні матеріали, блоки новин з ІБ, плакати, офісне приладдя з короткою інформацією щодо забезпечення ІБ.

Найбільший ефект дає комплексне застосування різних форм і методів навчання в рамках багаторівневої системи підвищення обізнаності працівників компанії в галузі ІБ, з використанням:

- очного навчання у вигляді інструктажу із забезпечення ІБ, який проводять фахівці служби ІБ новоприйнятими працівниками, а також спеціалізованих курсів для окремих категорій працівників;

- дистанційного навчання, що проводиться періодично, за кількома програмами різного рівня;

- ІБ компанії, з виявлених порушень та інших актуальних питань;

- самостійної роботи з нормативними документами;

- консультацій та проведення нарад з окремих питань забезпечення ІБ.

Систему підвищення обізнаності працівників компанії, як один із процесів системи менеджменту ІБ, доцільно організовувати у вигляді циклічної моделі Демінга «Планування – Реалізація – Перевірка – Удосконалення», яка є основою моделі менеджменту.

Етап «планування» – на цьому етапі здійснюється постановка цілей навчання, закупівля/розробка та введення в експлуатацію системи навчання, розробка навчальних програм та необхідних навчальних матеріалів, підготовка організаційно-розпорядчих документів щодо організації навчання.

Найбільш складним і, мабуть, найвідповідальнішим завданням є розробка (або придбання у спеціалізованих компаній) навчальних програм та навчальних матеріалів, які мають враховувати специфіку діяльності компанії та існуючий рівень обізнаності персоналу з питань ІБ. Для цього попередньо проводиться аналіз існуючих політик безпеки, використовуваних захисних заходів, кількості, видів та наслідків інцидентів ІБ з метою виявлення проблемних областей та рівня поінформованості працівників в області ІБ.

Зміст навчальних програм зазвичай типовий, що розкриває основні положення безпекової політики, правил використання інформаційних ресурсів, але з обов'язковим урахуванням специфіки компанії, особливостей обробки інформації та інших нюансів.

Працівникам необхідно чітко розуміти, що таке ІБ та які наслідки можуть бути для компанії у разі недотримання її вимог. Для правильного формування культури ІБ працівники компанії повинні розуміти, чому важливо захищати інформацію, які види конфіденційної інформації використовуються в компанії, які існують загрози, і які захисні заходи необхідно використовувати і як.

Особливу увагу необхідно акцентувати на розгляді поняття та основних видів інцидентів ІБ, їх ознаках та доведення інформації про те, що необхідно робити у разі виявлення інциденту ІБ і до кого звертатися в цьому випадку.

У курсах до працівників компанії повинні бути доведені вимоги законодавства України і локальних нормативних актів в області ІБ.

Оскільки підвищення обізнаності в області ІБ для більшості працівників не є профільним навчанням, засоби та матеріали, що використовуються у навчальній програмі та навчальних матеріалах, повинні бути простими для сприйняття, цікавими та максимально зрозумілими.

Етап «Реалізація» – тут реалізується розроблена програма і здійснюється контроль засвоєння знань працівниками компанії.

Перш ніж використовувати систему дистанційного навчання, провадиться інструктаж користувачів, навчання, як правильно її використовувати, встановленим порядком видаються навчальні завдання та провадиться контроль їх виконання. Можливе виділення окремих груп учнів відповідно до виконуваного функціоналу та рівня обізнаності.

На даному етапі найважливішим елементом є контроль навчання працівників: по-перше, необхідно мати зворотний зв'язок, щоб оцінити ефективність проведення навчання, по-друге, деякі підходять до навчання несерйозно, або не проходять навчання, або не здають тести. Таких працівників треба виявляти і домагатися успішного проходження ними курсу навчання.

Для контролю можна використовувати різні форми: тестування, опитування на знання політик безпеки.

Етап «Перевірка» – на цьому етапі проводиться оцінка ефективності реалізації навчальних програм, що включає оцінку отриманих працівниками

знань і умінь, оцінку дієвості проведених заходів, а також аналіз змін статистики інцидентів ІБ.

Можливо застосування наступних способів оцінки ефективності реалізації програми:

- збір та аналіз статистики інцидентів ІБ в компанії;

- відкриті перевірки (тести, опитування, інтерв'ю, анкетування, зовнішній або внутрішній аудит);

- приховані перевірки (телефонні дзвінки та електронні листи провокаційного характеру з використанням прийомів соціальної інженерії, моніторинг дій користувачів, зовнішній або внутрішній аудит).

Тут необхідно відповісти на запитання: наскільки програма відповідає вимогам політики безпеки компанії та як її можна оцінити, виміряти ефективність (можна, наприклад, скористатися метрикою даною, О. Лукацьким [9]).

Етап «Удосконалення» – на даному етапі проводиться корекція та поліпшення роботи, переробка програм та навчальних матеріалів, їх оновлення.

Зазвичай переробка навчальних програм проводиться після суттєвої зміни вимог законодавства, нормативних документів, вимог ІБ компанії, правил обробки інформації.

У компанії має бути визначено перелік документів, які є свідченням виконання програм навчання та підвищення обізнаності з ІБ.

Зокрема, такими документами можуть бути:

- документи (журнали), що підтверджують проходження працівниками навчання в галузі ІБ із зазначенням рівня освіти, навичок, досвіду та кваліфікації учнів;

- документи, що містять результати перевірок навчання працівників;

- документи, що містять результати перевірок обізнаності в галузі ІБ.

Як відомо, компетенція працівників – це один із ключових факторів успішного розвитку та стабільної роботи будь-якої компанії. Оскільки сучасні банківські організації дуже активно використовують інформаційні технології,

розвиток знань та навичок співробітників у галузі інформаційної безпеки нарівні з компетенціями в рамках їхньої основної діяльності стає дуже важливою частиною професійного вдосконалення персоналу, причому не лише офісного.

Участь усіх співробітників у вирішенні питань інформаційної безпеки дозволяє підвищити захищеність активів компанії та позитивно позначається як у взаємодії персоналу всередині компанії, так і на взаєминах з її контрагентами. Компетентність співробітників у питаннях ІБ, вміння застосовувати ці навички та знання в основній діяльності суттєво підвищують довіру з боку клієнтів та партнерів та сприяють більш стабільним відносинам, оскільки помітно знижують бізнес-ризики.

У банках зазвичай [29] застосовується багатоступінчаста програма, яка включає такі напрямки:

• вивчення основ інформаційної безпеки для всіх новоприйнятих співробітників;

• комплексне навчання керівників усіх рівнів основам інформаційної безпеки;

• дистанційне навчання та тестування співробітників за основними вимогами інформаційної безпеки;

• проведення тематичних заходів з найбільш актуальних питань ІБ;

• використання тематичних розсилок електронною поштою та корпоративних постерів з інформаційної безпеки з метою підвищення уваги співробітників до питань ІБ та їх оперативного інформування щодо найважливіших для компанії аспектів інформаційної безпеки.

Вивчення основ інформаційної безпеки відбувається на періодичній основі (щоквартально, щомісяця тощо для всіх новоприйнятих співробітників за цей період) у вигляді тематичних секцій у рамках спеціально розробленої програми адаптації нових співробітників. Ці секції включають ознайомлення з основними правилами, порядками і засобами захисту у банку і спрямовані не тільки на доведення основних вимог до працівників, але й на роз'яснення ролі й значимості ІБ як для банка загалом, так і для окремого працівника.

Комплексне навчання, яке включає огляд структури, вимог та методів забезпечення інформаційної безпеки у банку є сенс проводити щорічно. Мета – роз'яснення потреб та вигод від забезпечення інформаційної безпеки.

В рамках цих освітніх програм повинні висвітлюватися основи українського та міжнародного законодавства, а також найбільш цікавий досвід ІБ, що найкраще зарекомендував себе. Якщо крім теорії співробітників знайомити з типовими прикладами зовнішніх та внутрішніх порушень інформаційної безпеки, а також способами запобігання цим порушенням та мінімізації пов'язаних з ними ризиків, то навчання допомагає співробітникам зрозуміти свою роль у справі забезпечення інформаційної безпеки банку. Крім того, з'являється можливість більшою мірою залучити керівників підрозділів до забезпечення ІБ, що сприяє формуванню додаткового каналу впливу та контролю за діями працівників.

Альтернативою очним заходам є інтерактивні дистанційні методи навчання працівників. Для цього в банках використовуються спеціально розроблені динамічні навчальні матеріали (відеоролики та flash-листівки) з прикладами виробничих ситуацій, пов'язаних із порушеннями інформаційної безпеки, та роз'ясненнями про те, як слід діяти, якщо такі ситуації виникнуть. Дані заходи охоплюють всіх працівників банку. Періодичність заходів визначає служба безпеки банку.

У діяльності будь-якої компанії зустрічаються виробничі ситуації, що потребують особливої уваги та індивідуального підходу. Щодо таких випадків у банку розробляються та проводяться спеціальні тематичні курси. Необхідність таких курсів може бути викликана, наприклад, змінами в законодавстві чи галузевих вимогах щодо інформаційної безпеки або різними небажаними подіями. Як правило, дані курси орієнтовані на вузьке коло працівників та спрямовані на доведення до зацікавлених осіб детальних роз'яснень або на привернення їх уваги до виявлених прогалин у знаннях та навичках, що належать до ІБ, та до необхідності посилення контролю у цих галузях. Зокрема, є курси, націлені на підвищення обізнаності у сфері обробки інформації, що містить

персональні дані чи іншу конфіденційну інформацію, у межах конкретного підрозділу банку та з урахуванням його специфіки.

Ще одним каналом підвищення інформованості працівників банку у питаннях інформаційної безпеки є розсилка корпоративною електронною поштою попереджувальних або роз'яснювальних повідомлень. Подібні розсилки дозволяють оперативно сповіщати співробітників про зміни у внутрішній або зовнішній нормативній базі з інформаційної безпеки, доводити до персоналу інформацію про ризики, пов'язані з нововиявленими вразливостями у застосованому ПЗ або при використанні Інтернету, а також скоригувати дії працівників при отриманні спам-повідомлень.

Щоб підтримувати обізнаність працівників, у банку також практикується розклеювання постерів у місцях, які масово відвідують співробітники: у внутрішніх господарських приміщеннях, у холах, коридорах, переговорних кімнатах тощо. Найпростіший плакат, що нагадує про необхідність блокування комп'ютера при залишенні робочого місця, доволі часто має більший ефект, ніж усні нагадування про необхідність цього зробити. Співробітник, побачивши його, згадує про безпеку та навіть іноді повертається на своє робоче місце, щоб заблокувати комп'ютер.

Усі навчальні заходи обов'язково повинні завершуватися перевірками засвоєних співробітниками знань та навичок. Аналіз результатів повинен використовуються для вдосконалення навчальних матеріалів.

Всі перелічені вище заходи не лише торкаються аспектів інформаційної безпеки при роботі безпосередньо в офісах банку, але й при роботі на домашніх комп'ютерах та мобільних пристроях – співробітники зможуть застосовувати ці знання у повсякденній діяльності, розповідати про це членам своїх сімей та друзям. Безумовно, ці заходи розраховані на довгострокову перспективу – вони допоможуть знизити ризики та мінімізувати загрози банківській системі України.

Для більшого залучення керівництва банку до вирішення питань інформаційної безпеки у банку організовані та працюють різні колегіальні

органи. Наприклад, за участю топ-менеджменту банку проводяться засідання Комітету з інформаційної безпеки, в рамках якого роз'яснюються бізнес-мети та вигоди від реалізації як окремих робіт, так і комплексних проектів у галузі ІБ. Подібні комітети дозволяють не лише спланувати та затвердити ключові напрями розвитку інформаційної безпеки банку, а й надати учасникам комітету розгорнуті роз'яснення потреб у тій чи іншій діяльності, сформувати правильні очікування та донести до керівників інформацію як про їх особистий ступінь участі та залучення, так і про внесок на зміцнення інформаційної безпеки, який вносять підлеглі ним підрозділи та співробітники.

За будь-якої ефективності та повноти заходів щодо підвищення обізнаності працівників дуже важливо забезпечити можливості контрольованого застосування працівниками компанії своїх знань та навичок у галузі інформаційної безпеки, адже, на жаль, не завжди отримані знання можуть бути використані виключно на благо компанії.

Безумовно, підвищення обізнаності в галузі інформаційної безпеки – це лише частина комплексу заходів щодо забезпечення ІБ, і досягти синергії можна лише за їх взаємозв'язку з коректно налаштованими технічними засобами захисту, достатньо повними та реально працюючими нормативними документами та за адекватної міри відповідальності кожного співробітника компанії.

Взагалі можна використовувати досконалі програмно-технічні способи та засоби забезпечення інформаційної безпеки, писати найправильніші та найповніші документи (політики) з інформаційної безпеки, але без участі в цій роботі всіх працівників банку ефективність системи забезпечення інформаційної безпеки (далі – СЗІБ) буде мінімальною. Людський фактор є найслабшою ланкою будь-якої СЗІБ [33].

Для мінімізації ризиків, пов'язаних з людським фактором, необхідно організувати документально оформлену та затверджену керівництвом банку роботу з персоналом у напрямку підвищення обізнаності та навчання в галузі інформаційної безпеки. Включаючи розробку та реалізацію планів, програм

навчання та підвищення обізнаності в галузі інформаційної безпеки, а також контроль результатів виконання зазначених планів.

Навчання персоналу в галузі інформаційної безпеки необхідне для наступних цілей:

- розвитку та підтримки у працівників усвідомлення важливості безпеки при використанні інформаційних технологій, знання порядку дій у разі виникнення небажаних подій та інцидентів;

- усвідомлення працівниками їх ролі та місця, а також обов'язків та відповідальності за забезпечення захисту інформації у банку;

- підвищення рівня знання працівниками основних правил забезпечення інформаційної безпеки;

- доведення до працівників основних положень, обмежень та вимог існуючих документів (політик) у галузі інформаційної безпеки;

- доведення до працівників інформації про те, які засоби захисту використовуються, а також про те, як ці засоби правильно і ефективно використовувати.

Навчання в галузі інформаційної безпеки має включати такі напрямки:

- підвищення загальної обізнаності працівників банку щодо інформаційної безпеки;

- безпечна робота з персональними даними у банку;

- організація безперервності ведення бізнесу та відновлення діяльності після переривань.

Основними формами навчання є:

- індивідуальне навчання (вступний, повторний та позачерговий інструктажі);

- спеціальне навчання із залученням зовнішніх навчальних центрів;

- підвищення обізнаності: дистанційне навчання, методами соціальної інженерії (пам'ятками, плакатами, screenlock'ерами тощо, що відображають усі вимоги нормативних документів банку з інформаційної безпеки).

До програми навчання та підвищення обізнаності слід включати таку інформацію про:

- існуючі політики інформаційної безпеки;

- заходи захисту, які застосовуються в банку;

- правильне використання захисних заходів відповідно до внутрішніх документів банку;

- значимість та важливість діяльності працівників для забезпечення інформаційної безпеки банку.

Також необхідно визначити перелік документів, які є свідченням виконання програм навчання та підвищення обізнаності з інформаційної безпеки.

Індивідуальне навчання (інструктажі) мають завершуватися перевіркою знань усним опитуванням, а також оцінкою набутих навичок безпечних способів роботи. Знання перевіряє працівник, який проводив інструктаж.

При розподіленій структурі банку має сенс покласти обов'язки проведення навчання та підвищення обізнаності у сфері інформаційної безпеки на спеціального працівника (адміністратора інформаційної безпеки), призначеного у кожному віддаленому підрозділі.

У рамках самооцінки внутрішнім аудиторам банку необхідно регулярно контролювати рівень обізнаності працівників підрозділів, що перевіряються, повноту та правильність оформлення документів з навчання, своєчасність доведення нових вимог з інформаційної безпеки.

Служба інформаційної безпеки має відслідковувати ефективність навчання, у тому числі шляхом кількісного та якісного аналізу дій працівників банку, які пішли у відповідь на певні події.

Система навчання є масштабованим процесом, спрямованим на постійне підвищення рівня знань, навичок та кваліфікації в галузі інформаційної безпеки працівників банку та інтегрується з діючими кадровими бізнес-процесами.

Таким чином внаслідок впровадження системи навчання та підвищення поінформованості в галузі інформаційної безпеки у банку суттєво зменшиться

кількість інцидентів у цій галузі, пов'язаних з людським фактором, а також скоротиться нецільове використання ресурсів.

Висновки до розділу 3

З урахуванням дедалі більшої міграції бізнесу до електронного середовища значимість питань забезпечення ІБ зростає. Безпека продукту або сервісу стає реальною конкурентною перевагою. З часом все більше використовуються вбудовані засоби захисту на відміну від накладених, що є закономірним процесом. Основний фокус з точки зору побудови систем ІБ спрямований на управління цією системою.

Основними технологіями захисту від націлених атак є, насамперед, різні інструменти виявлення аномалій – як на локальних комп'ютерах, так і на рівні мережевої активності, зокрема міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS, IPS), запобігання витоку інформації DLP, захисту кінцевих точок, антивіруси, системи управління інформацією та подіями інформаційної безпеки - SIEM. До нових технологічних засобів захисту відносять: пісочниці, які імітують робочі станції організації, засоби аналізу аномальної мережевої активності та поведінкового аналізу робочих станцій. Водночас для протидії сучасним кіберзагрозам організація має використовувати комплексний підхід, який поєднує кілька кордонів захисту із застосуванням різних технологій безпеки.

Підвищення обізнаності персоналу – це один з найважливіших етапів впровадження системи забезпечення ІБ, який спрямований на навчання персоналу та підтримку його знань у актуальному стані. Навчання персоналу банку з питань ІБ – запорука високої ефективності всієї системи безпеки загалом. Крім того, більшість інцидентів ІБ можна не допустити, оскільки понад половина всіх інцидентів спричинені діями працівників банків просто через незнання вимог та правил ІБ.

ВИСНОВКИ

Підсумовуючи, варто відзначити велике значення банківських систем в економіці держави, а, отже, питання забезпечення інформаційної безпеки банків має вирішуватися ефективно. Специфіка та особливості системи забезпечення ІБ є індивідуальними для кожної банківської установи, тому комплексний і професійний підхід до організації систем захисту – необхідна умова роботи всієї банківської системи.

Аналіз вітчизняного законодавства показав, що основними актами, які регулюють питання інформаційної безпеки у банківській сфері є Закони України «Про банки і банківську діяльність», «Про Національний банк України», «Про електронні довірчі послуги», «Про основні засади забезпечення кібербезпеки України» тощо.

Водночас ключову роль у нормативному регулюванні питань інформаційної безпеки вітчизняних банківських установ відіграє НБУ, який посилив контроль за виконанням банківськими установами заходів щодо забезпечення інформаційної безпеки та кіберзахисту, що в умовах сучасних кіберзагроз має сприяти удосконаленню організації діяльності банків.

Так, НБУ впровадив новий вид контролю за банківськими установами у вигляді безвиїзного нагляду та виїзних перевірок, які здійснюватимуть фахівці регулятора у сфері інформаційної безпеки та кіберзахисту. Крім цього, банки зобов’язані проводити самооцінку стану власної інформаційної безпеки та кіберзахисту. Також НБУ ухвалив мінімальні обов'язкові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків; принципи управління інформаційною безпекою; вимоги щодо банківських інформаційних систем, які взаємодіють з інформаційними системами НБУ.

Встановлено, що до основних актуальних загроз інформаційній безпеці банків можна віднести атаки на процесингові центри банків із виведенням коштів через банкомати, атаки зловмисників на системи дистанційного банківського обслуговування (ДБО) клієнтів, шахрайство з використанням

методів соціальної інженерії та здирство. Також варто відмітити людський фактор – основна та головна загроза інформаційної безпеки, що прямо залежить від людських відносин. Витік інформації найчастіше відбувається з провини банківського персоналу.

Атаки типу APT досі залишаються одними з найбільш поширених та небезпечних для банківської сфери. Такі атаки добре сплановані та при належному фінансуванні можуть тривати багато місяців. До основних етапів APT-атак відносять: підготовка, проникнення, розповсюдження, досягнення цілей.

Сприятлива ситуація для кіберзлочинців, яка сформувалася в останні роки, пов'язана з високою доступністю та простотою використання більш складного та гнучкого шкідливого ПЗ для ботнетів у поєднанні зі значним приростом кількості незахищених IoT-пристроїв. Це зробило кримінальні ботнети основним компонентом зростаючої цифрової підпільної економіки.

Основними технологіями захисту від націлених атак та ботнетів є, насамперед, різні інструменти виявлення аномалій – як на локальних комп'ютерах, так і на рівні мережевої активності, зокрема міжмережеві екрани, системи виявлення та запобігання вторгненням, запобігання витоку інформації, захисту кінцевих точок, антивіруси, системи управління інформацією та подіями інформаційної безпеки. До нових технологічних засобів захисту відносять: пісочниці, які імітують робочі станції організації, засоби аналізу аномальної мережевої активності та поведінкового аналізу робочих станцій. Водночас для протидії сучасним кіберзагрозам банк має використовувати комплексний підхід, який поєднує кілька кордонів захисту і різні технології безпеки.

Підвищення обізнаності персоналу – це один з найважливіших етапів впровадження системи забезпечення ІБ, який спрямований на навчання персоналу та підтримку його знань у актуальному стані. Навчання персоналу банку з питань ІБ – запорука високої ефективності всієї системи безпеки загалом. Крім того, більшість інцидентів ІБ можна не допустити, оскільки понад половина всіх інцидентів спричинені діями працівників банків просто через незнання вимог та правил ІБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Advanced Persistent Threat (APT). Таргетированные или целевые кибератаки. URL: https://www.tadviser.ru/ (дата звернення: 21.12.2021)

2. Fundamentals of Cybersecurity in Banks. URL: https://www.qentelli.com/thought-leadership/insights/fundamentals-cybersecurity-banks (дата звернення: 21.12.2021)

3. Information Security in Banking and the Insider Threat. URL: https://www.isdecisions.com/blog/it-infrastructure/information-security-in-banking-insider-threat/ (дата звернення: 21.12.2021)

4. Waschke Marvin. Personal Cybersecurity How to Avoid and Recover from Cybercrime. 2017. 379 с.

5. Microsoft помогла остановить ботнет, управляемый через светодиодную консоль. URL: https://habr.com/ru/news/t/498142/ (дата звернення: 21.12.2021)

6. Bowen Pauline, Hash Joan, Wilson Mark. Information Security Handbook: A Guide for Managers. 2006. 180 с.

7. Campbell Tony. Practical Information Security Management. A Complete Guide to Planning and Implementation. 2016. 270 с.

8. Скородумов А. Информационная безопасность в банковской сфере: время перемен. URL: https://www.tbforum.ru/blog/informatsionnaya-bezopasnost-v-bankovskoy-sfere-vremya-peremen (дата звернення: 21.12.2021)

9. Лукацкий А. Как оценить программу повышения осведомленности? / Бизнес без опасности. URL: https://lukatsky.blogspot.com/2011/08/blog-post_19.html (дата звернення: 21.12.2021)

10. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. 2004. 508 с.

11. Ботнет сети: как это работает и как на них зарабатывают. URL: https://networkguru.ru/botnet-seti/ (дата звернення: 21.12.2021)

12. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. К.: НАУ, 2013. 432 с.

13. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

14. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. 2015. 288 с.

15. Закон України від 07.12.2000 № 2121-III «Про банки і банківську діяльність». URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text (дата звернення: 21.12.2021)

16. Закон України 05.10.2017 № 2155-VIII «Про електронні довірчі послуги. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 21.12.2021)

17. Закон України від 20.05.1999 № 679-XIV «Про Національний банк України». URL: https://zakon.rada.gov.ua/laws/show/679-14#Text (дата звернення: 21.12.2021)

18. Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.12.2021)

19. Писаренко И. Повышение осведомленности пользователей по вопросам ИБ. URL: https://lib.itsec.ru/articles2/control/povyshenie-osvedomlennosti-polzovateley-po-voprosam-ib (дата звернення: 21.12.2021)

20. Информационная банковская безопасность и ее необходимость. URL: https://finexpert24.com/poleznye-materialy/articles/bankovskaya-deyatelnost/informatsionnaya-bankovskaya-bezopasnost-i-ee-neobhodimost/ (дата звернення: 21.12.2021)

21. Информационная безопасность банков. URL: https://arinteg.ru/articles/informatsionnaya-bezopasnost-bankov-26722.html#:~:text=%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC% (дата звернення: 21.12.2021)

22. Інформаційна безпека банків: посилюється контроль за кіберзахистом. URL: http://www.visnuk.com.ua/uk/news/100022274-informatsiyna-bezpeka-bankiv-posilyuyetsya-kontrol-za-kiberzakhistom (дата звернення: 21.12.2021)

23. Как работает хакерская экономика. URL: https://habr.com/ru/post/5054/ (дата звернення: 21.12.2021)

24. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. URL: http://veche.kiev.ua/journal/598/ (дата звернення: 21.12.2021)

25. Насколько защищены от кибератак банки и биржи: Статистика и мнения экспертов. URL: https://habr.com/ru/company/iticapital/blog/308014/ (дата звернення: 21.12.2021)

26. Остроухов В. В., Присяжнюк М. М., Петрик В. М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник / За ред. Є.Д.Скулиша. К., 2010. 776 с.

27. Постанова Правління НБУ №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 21.12.2021)

28. Постанова Правління НБУ № 4 від 16.01.2021 «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг». URL: https://zakon.rada.gov.ua/laws/show/v0004500-21#Text (дата звернення: 21.12.2021)

29. Чаплыгин Р. Комплексная профилактика / OSP – Гид по технологиям цифровой трансформации. URL: https://www.osp.ru/cio/2012/09/13017729 (дата звернення: 21.12.2021)

30. Украинские власти разоблачили крупную группировку криптовымогателей. URL: https://habr.com/ru/news/t/563224/ (дата звернення: 21.12.2021)

31. Украинский мега-ботнет. URL: https://habr.com/ru/post/58063/ (дата звернення: 21.12.2021)

32. Урсул А., Цырдя Т. Информационная безопасность. сущность, содержание и принципы ее обеспечения. URL: http://www.security.ase.md/publ/ru/pubru22.html (дата звернення: 21.12.2021)

33. Учить или не учить? BIS Journal. 2012. №4 (7). URL: https://ib-bank.ru/bisjournal/post/69 (дата звернення: 21.12.2021)

34. Шилан Н. Н., Кривонос Ю. М., Бирюков М. Г. Компьютерные преступления и проблемы защиты информации. URL: https://it-crime.at.ua/index/vidpovidalnist_quot_insajderiv_quot/0-36 (дата звернення: 21.12.2021)

35. Юдін О. К., Богуш В. М. Інформаційна безпека держави: Навч. посіб. Харків: Консул, 2005. 508 с.

36. Cybersecurity in Banking: Bank hackers, ransomware, and more. URL: https://businessinsights.bitdefender.com/cybersecurity-in-banking-bank-hackers-ransomware-and-more (дата звернення: 21.12.2021)

37. NIST Special Publication (SP) 800-50, Building an Information Technology Security Awareness and Training Program. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf (дата звернення: 21.12.2021)

38. The 5 Biggest Threats to a Bank's Cyber Security. URL: https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security/ (дата звернення: 21.12.2021)

39. Ахрамович В. М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур». Державний університет телекомунікацій. К.:ДУТ, 2019. 163 с.

40. Ахрамович В. М., Чегренець В. М. Управління ризиками інформаційної безпеки комерційного банку. Сучасний захист інформації. 2019. № 2. 59 с.

41. Бєлоусова К.І., Бєлоусов Я.І. Забезпечення інформаційної безпеки – реалізація стратегії банківської установи. Науковий вісник ДУІКТ. 2010.

42. Бондаренко М. Ф. Визначення та обґрунтування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін. Радиотехника. 2003. № 134. С. 9-25.

43. Диба М.О., Зубок М.І., Яременко С.М. Інформаційні ризики в банківській діяльності. Вісник НБУ. 2007.

44. Домарєв В. В., Домарєв Д. В., Гордієнко С. Б. Обґрунтування основних функцій системи управління інформаційною безпекою. Вісник Державного університету інформаційно-комунікаційних технологій. 2012. Т. 10. № 2.

45. Євсеєв С. П., Грищук Р. В. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах. Ukrainian Scientific Journal of Information Security. 2017.

46. Зачосова Н. В., Чабаненко Ю. А. Формування системи економічної безпеки фінансових установ: монографія. Черкаси. 2016. 375 с.

47. Зубок М. І., Яременко С. М. Безпека банківської діяльності : підручник. К. : КНЕУ, 2012. 542 с.

48. Кібальник Л. О., Напора І. Ю. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки. Черкаси. 2016.

49. Козаченко І. П., Голубєв В. О. Загальні принципи захисту банківської комп'ютерної інформації. Центр дослідження проблем комп'ютерної злочинності. URL: http://www.crime-research.ru/library/Koz_gol.htm (дата звернення: 21.12.2021)

50. Корченко А. О., Скачек Л.М., Хорошко В.О. Банківська безпека: Підручник. К.: ПВП «Задруга», 2014. С.185.

51. Корченко О. Г. Аудит та управління інцидентами інформаційної безпеки / О. Г. Корченко, С. О. Гнатюк, С. В. Казмірчук та ін. Київ, 2014. 190 с. URL:https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf (дата звернення: 21.12.2021)

52. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима. Проблеми економіки. 2013. № 4. С. 341-347. URL: http://nbuv.gov.ua/UJRN/Pekon_2013_4_46 (дата звернення: 21.12.2021)

53. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11 (дата звернення: 21.12.2021)

54. Напора І. Ю. Інформаційна безпека банківських установ як об'єкт наукових досліджень. Вісник Черкаського університету. Серія: Економічні науки. 2014. №39.

55. Напора І. Ю. Організація системи інформаційної безпеки банківських установ. Вісник Черкаського університету. Серія: Економічні науки. 2016. № 4. С.80-86.

56. Отенко І. П., Мішин О. Ю., Мішина С. В. Організація та управління фінансово-економічною безпекою банківських установ : навчальний посібник. Х.: ХНЕУ ім. С. Кузнеця, 2015. 240 с. URL: http://repository.hneu.edu.ua/bitstream/ (дата звернення: 21.12.2021)

57. Пичугина П. А. Проблемы обеспечения информационной безопасности в банковских информационных системах. URL: http://www.tvvlibrary.narod.ru/papers/2011/6-11.pdf (дата звернення: 21.12.2021)

58. Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0829500-15#n464 (дата звернення: 21.12.2021)

59. Ролдугіна Ю. В., Ковальова І. В. Особливості інформаційної безпеки банків. Актуальні проблеми економічного і соціального розвитку регіону. 2011. С.283-287.

60. Світлична В.Ю. Забезпечення інформаційної безпеки банківських установ. Кримський економічний вісник: Науковий журнал. №1 (08) лютий, 2014. Частина ІІ. Сімферополь, 2014. С.172-175.

61. Тихомиров О.О. Правові засади охорони банківської таємниці: ел. навч. посібник. Київ: Нац. акад. СБУ, 2016. URL: http://obt.inf.ua/ (дата звернення: 21.12.2021)