МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

МАГІСТЕРСЬКА РОБОТА

Освітньо – кваліфікаційного рівня магістра

За спеціальністю 125 «Кібербезпека»

На тему:

Аналіз сучасного стану кібербезпеки банківської та фінансової структури України

Виконав: студент 6 курсу, групи БКз-812м НІКУЛІН С.А.

Керівник: к.т.н., доцент НЕЛАСА Г.В.

Актуальність теми

Обрана тема є на даний час **актуальною**, тому що Кібербезпека банківської та фінансової структури України є одним із найважливіших питань національної безпеки. У сучасних умовах зростання кіберзагроз, які можуть призвести до серйозних фінансових втрат, порушення роботи банківських систем та навіть до дестабілізації фінансової системи країни, забезпечення кібербезпеки банків та фінансових установ є пріоритетним завданням для держави та бізнесу.

Метою проведення досліджень магістерської роботи є аналіз сучасного стан кібербезпеки банківської та фінансової структури України.

Об’єктом дослідження даної роботи є банківська та фінансова структури України.

Предметом дослідження є кібербезпека банківської та фінансової структури України.

Задачі дослідження

1

- охарактеризувати основні кіберзагрози, яким піддається банківська та фінансова структура України;

2

- проаналізувати стан кібербезпеки банків та фінансових установ в Україні;

3

- розробити пропозиції щодо підвищення кібербезпеки банківської та фінансової структури України.

Основні види кіберзагроз

Зловмисне програмне забезпечення

це програмний код, який розроблений з метою завдати шкоди комп'ютеру або його користувачам

Злом

це програмний код, який розроблений з метою завдати шкоди комп'ютеру або його користувачам;

Фішинг

це вид шахрайства, при якому зловмисники намагаються отримати особисту інформацію про жертву, такі як логін, пароль або номер кредитної картки

DDoS-атака

це атака, при якій зловмисники намагаються зробити веб-сайт або службу недоступними для користувачів

Соціальна інженерія

це атака, яка включає в себе маніпуляцію людьми, щоб отримати доступ до конфіденційної інформації або фінансових ресурсів;

Наслідки кібератак

- фінансові втрати
- втрата довіри клієнтів
- пошкодження репутації
- юридичні проблеми

Заходи з кібербезпеки

- кіберзахист передачі даних (шифрування);
- двофакторна аутентифікація;
- моніторинг та виявлення вторгнень;
- безпека мобільних додатків;
- навчання та підвищення свідомості (кліенти та співробітники);
- резервне копіювання та відновлення даних;
- Взаємодія з кіберполіцією та іншими агентствами.

Правові засади інформаційної безпеки в банківській та фінансовій сферах України

Правові засади інформаційної безпеки в банківській та фінансовій сферах України закріплені в наступних нормативно-правових актах:

- Закон України «Про Національний банк України»
- Закон України «Про банки і банківську діяльність»
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
- Закон України «Про основні засади забезпечення кібербезпеки України»

Ці нормативно-правові акти встановлюють вимоги до забезпечення інформаційної безпеки в банківській та фінансовій сферах. Зокрема, вони передбачають, що банки та інші фінансові установи повинні:

- Приймати необхідні організаційні та технічні заходи для захисту інформації, що є об’єктом захисту в банківській та фінансовій сферах.
- Створювати систему управління інформаційною безпекою.
- Проводити оцінку ризиків інформаційної безпеки.
- Здійснювати моніторинг інформаційної безпеки.

МЕТОДИ ЗАХИСТУ В БАНКІВСЬКИХ ТА ФІНАНСОВИХ УСТАНОВАХ

Технічний захист конфіденційної інформації та захист компьютерної мережі

- підключення до декількох провайдерів;
- фізична безпека (спеціальні приміщення для обладнання, контроль доступу, відеоспостереження, охорона);
- безпека мережевих пристроїв (захист паролями,безпечне програмне забезпечення, фільтрація трафіку);
- безпека програмного забезпечення (захист паролями, безпечне програмне забезпечення, антивірусне програмне забезпечення, брандмауер);
- безпека даних (шифрування, регулярне резервне копіювання, контроль доступу);
- безпека користувачів (освіта користувачів, політика безпеки, контроль відповідності)

МЕТОДИ ЗАХИСТУ В БАНКІВСЬКИХ ТА ФІНАНСОВИХ УСТАНОВАХ

Програмний захист інформації

Функціональне призначення ПЗ:

- ідентифікація (присвоєння унікального образу, імені, числа);
- аутентифікація (встановлення достовірності).

Програмні засоби забезпечення інформаційної безпеки:

- програмно-апаратні шифратори мережевого трафіку;
- встановлення екранів (Firewall);
- захищені мережеві криптопротоколи;
- програмні засоби виявлення атак;
- програмні засоби аналізу захищеності;
- антивірусне ПЗ
- захищені мережеві операційні системи (ОС)

МЕТОДИ ЗАХИСТУ В БАНКІВСЬКИХ ТА ФІНАНСОВИХ УСТАНОВАХ

Криптографічний захист інформації

Криптографічний алгоритм – це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв’язаного (шифрованого) тексту

Криптографічні алгоритми:

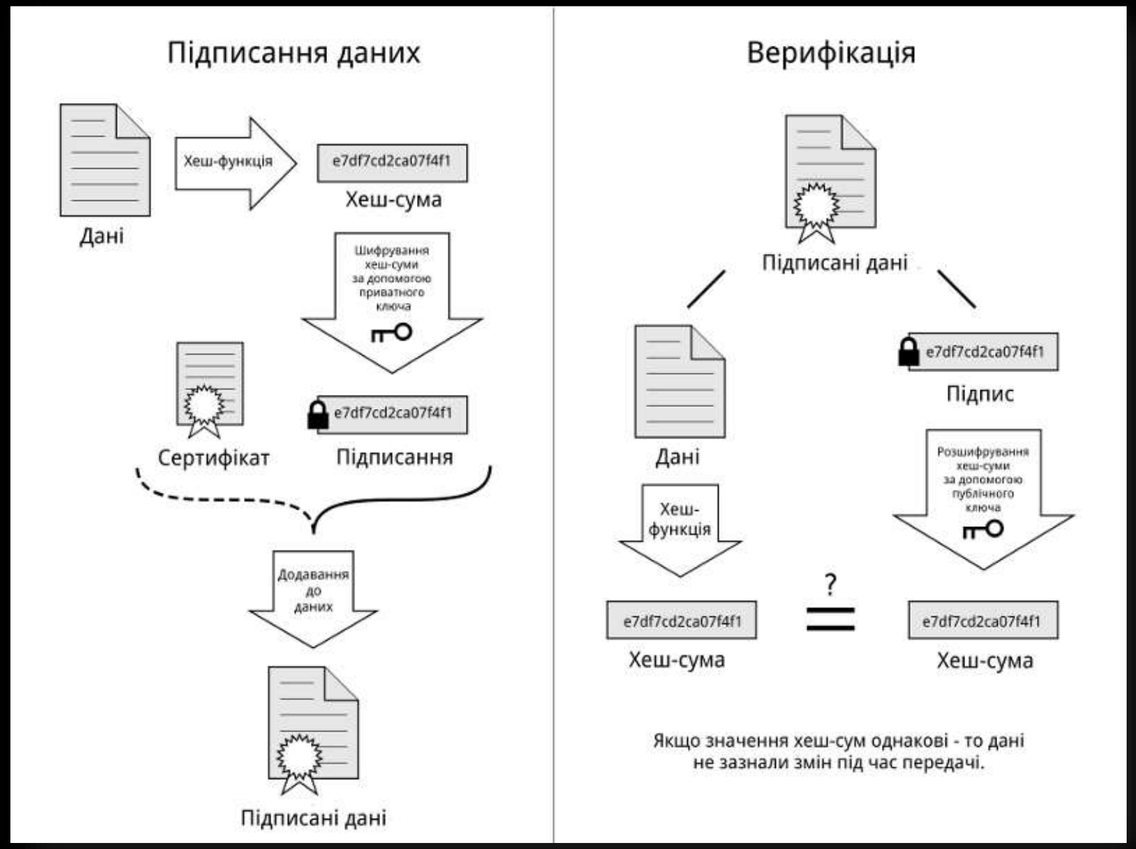
- симетричні (шифрування і розшифрування виконується однаковим ключем); DES, 3DES (Triple DES), AES
- асиметричні (шифрування і розшифрування виконують за допомогою різних ключів) RSA, Алгоритм Діффі-Геллмана.

Електронний цифровий підпис

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка називається електронним цифровим підписом

Електронний цифровий підпис

- Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка називається електронним цифровим підписом



Методи розподілу ключів:

- метод базових/сеансових ключів;
- метод відкритих ключів

Кіберзахист банківської системи України в сучасних умовах цифрових трансформацій

Тренди банківської цифровізації:

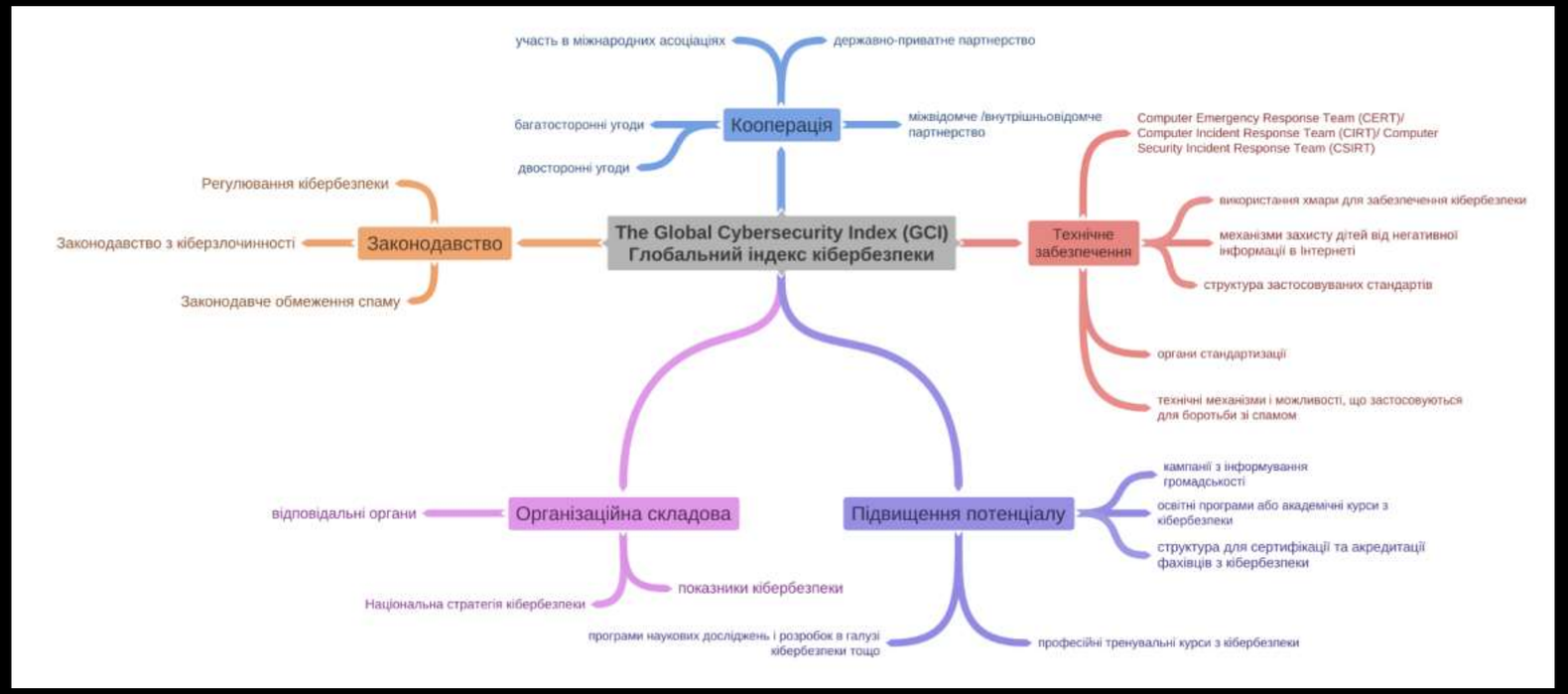
- широке застосування і оптимізація віддаленої роботи працівників;
- значне зростання операцій онлайн;
- спрощення доступу до послуг банку;
- значний розвиток каналів дистанційного продажу;

Найпоширініші: DDoS-атаки різного характеру, від яких страждає вся банківська система, та фішингові атаки різних типів (різні види шахрайства)

Кількість кіберінцидентів у 2022 році збільшилася втричі ніж у 2021.

Протягом 2022 року – понад 7000 кібератак

Порівняння практик та стратегій кібербезпеки в Україні з іншими країнами



Публічна діаграма від https://coggle.it/

Україна посіла у рейтингу GCI 2018 року 54 місце, а у 2021 році – 78 місце, втративши 24 позиції.

Висновок

Робота включає в себе аналіз нормативно-правової бази, організаційних та технічних заходів, що застосовуються в Україні для забезпечення кібербезпеки банківської та фінансової структури.
Результати дослідження:
- аналіз ефективності заходів і методів кібербезпеки,
- аналіз загроз та вразливостей;
- порівняльний аналіз кібербезпеки в Україні з іншими країнами;
- виявлено недоліки в існуючій системі безпеки;
- розроблено конкретні пропозиції щодо підвищення кібербезпеки банківської та фінансової структури України.