Міністерство освіти і науки України

Харківський національний університет ім. В. Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В.о. завідувача кафедри БІСТ

Мелкозьорова О.М.

_____

« » 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Організаційні рекомендації з захисту банківських систем»

оцінка « » Керівник к.т.н. доцент Мелкозьорова О. М.

Голова ЕК

Лемешко О.В._____ Рецензент д.т.н. Краснобаєв В.А.

Виконавець: студентка групи КБ-42

Назаренко Р.Ю,

Харків – 2024

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел. Загальним обсягом робота складає 40 сторінок, має 1 рисунок. Список використаних джерел містить 4 найменування і займає 1 сторінку.

Метою дипломної роботи розробка організаційних рекомендацій для підвищення рівня захисту банківських систем.

У роботі використовуються такі методи дослідження: методи аналізу сучасних загроз, вивчення найкращих практик у сфері кібербезпеки та розробка пропозицій щодо оптимізації внутрішніх політик і процедур безпеки.

Мета дослідження є розвиток теоретичних знань та практичних навичок у галузі захисту інформаційних систем, особливо в банківській сфері, і спрямована на формування ефективних рекомендацій для захисту банківських систем.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ РЕСУРСИ БАНКІВ, ЗАХИСТ БАНКІВСЬКИХ СИСТЕМ, ОРГАНІЗАЦІЙНІ ЗАХОДИ, ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ.

ANNOTATIONS

The thesis consists of an introduction, three sections, general conclusions, and a list of used sources. The total volume of the work is 40 pages, has 1 figure. The list of used sources contains 4 names and occupies 1 page.

The aim of the thesis is to develop organizational recommendations for increasing the level of protection of banking systems.

The following research methods are used in the work: methods of analyzing modern threats, studying best practices in the field of cyber security, and developing proposals for optimizing internal security policies and procedures.

The purpose of the study is the development of theoretical knowledge and practical skills in the field of protection of information systems, especially in the banking sector, and is aimed at the formation of effective recommendations for the protection of banking systems.

Keywords: INFORMATION SECURITY, INFORMATION RESOURCES OF BANKS, PROTECTION OF BANKING SYSTEMS, ORGANIZATIONAL MEASURES, THREATS TO INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

НСМЕП - Національної системи масових електронних платежів

СУІБ - Система управління інформаційною безпекою

СЕП - Системи електронних платежів

ВСТУП

В умовах глобалізації економічних процесів та швидкого розвитку цифрових технологій, фінансові установи стикаються з безпрецедентними викликами у сфері захисту своїх інформаційних систем. Фінансові операції все більше залежать від цифрових технологій, безпека банківських систем набуває вирішального значення. Цифровізація банківських послуг не тільки спрощує управління фінансами для клієнтів, але й відкриває нові вектори атак для кіберзлочинців. Злам банківської системи може мати не лише економічні наслідки, але й підривати довіру клієнтів та впливати на стабільність фінансового ринку в цілому. Також банки є частиною національної і глобальної фінансової системи, тобто будь-які серйозні порушення безпеки в одному банку можуть мати ефект доміно, впливаючи на інші фінансові установи та загальну економічну стабільність. Зростаюча кількість кібератак на банки по всьому світу підкреслює потребу у сильних організаційних заходах та передових технологічних рішеннях. Проблема захисту не тільки технічна, але й організаційна, що вимагає комплексного підходу та регулярного перегляду процедур з безпеки. Ефективні організаційні заходи з захисту банківських систем дозволяють мінімізувати ризики несанкціонованого доступу, втрати або пошкодження даних, а також забезпечити відповідність нормативним вимогам у сфері інформаційної безпеки. Тому питання організаційних заходів щодо захисту інформації в банках залишається актуальним і вимагає постійної уваги та вдосконалення.

За останні роки значно збільшилась кількість та складність кібератак, спрямованих на фінансові установи. Згідно зі статистичними даними, банки все частіше стають мішенню для хакерів, які використовують різні методи для отримання доступу до конфіденційної інформації та фінансових ресурсів.

Актуальність. Дослідження в цій галузі спрямоване на розробку та впровадження комплексних організаційних заходів, які допоможуть банкам ефективно протистояти сучасним загрозам, забезпечувати надійний захист

інформації та відповідати нормативним вимогам. Результати роботи будуть корисні для банківських установ, регуляторів та фахівців з інформаційної безпеки, сприяючи підвищенню рівня безпеки банківських систем на національному та міжнародному рівні.

Мета роботи: розробка організаційних рекомендацій для підвищення рівня захисту банківських систем.

Методи дослідження: аналіз сучасних загроз, вивчення кращих практик в галузі кібербезпеки та розробку пропозицій щодо оптимізації внутрішніх політик і процедур безпеки.

Дана робота спрямована на розвиток теоретичних знань та практичних навичок у сфері захисту інформаційних систем, зокрема в банківській сфері, і сподівається допомогти в подальшому формуванні ефективних рекомендації з захисту банківських систем.

1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Поняття кібербезпеки та кіберзахисту

Кібербезпека - це практика захисту систем, мереж та програм від цифрових атак. Ці кібератаки зазвичай спрямовані на доступ, зміну або знищення конфіденційної інформації, вимагання грошей у користувачів або переривання нормальних бізнес-процесів.

Сучасний світ як ніколи оснащений великою кількістю засобів зв’язку. Світову економіку формують люди, які спілкуються, перебуваючи в різних часових поясах, і отримують доступ до важливої інформації звідусіль. Кібербезпека стимулює продуктивність і впровадження інновацій, що дає користувачам змогу впевнено працювати та спілкуватись онлайн. Правильні рішення й процеси дають компаніям і державним установам змогу користуватися технологіями для покращення спілкування й надання послуг, не ризикуючи постраждати від атак.

Основні аспекти кібербезпеки включають:

- Безпека мережі: Захист комп'ютерних мереж від атак зловмисників, які намагаються отримати несанкціонований доступ до систем та даних.
- Безпека програмного забезпечення: Захист додатків від загроз, що можуть використовувати вразливості у програмному забезпеченні. Це включає регулярні оновлення та виправлення програмного забезпечення.
- Безпека даних: Захист даних під час зберігання та передачі. Це включає шифрування, резервне копіювання та управління доступом до даних.
- Операційна безпека: Включає процеси та рішення щодо обробки і захисту даних. Наприклад, управління користувачами, контроль доступу та аудит дій користувачів.

- Освітня та інформаційна безпека: Забезпечення обізнаності працівників та користувачів про ризики кібербезпеки та навчання їх правильній поведінці в цифровому середовищі.
- Планування відновлення після інцидентів та безперервність бізнесу: Стратегії для відновлення систем та операцій після кіберінциденту, щоб мінімізувати вплив на бізнес.
- Управління ідентифікацією та доступом: Використання багатофакторної автентифікації та інших методів для гарантування, що тільки авторизовані користувачі мають доступ до ресурсів.

Кібербезпека включає використання технологій, процесів та засобів для захисту інформаційних систем та даних від атак, що допомагає забезпечити конфіденційність, цілісність і доступність інформації.

Кіберзахист - це сукупність заходів та технологій, спрямованих на захист інформаційних систем, мереж та даних від кібератак, несанкціонованого доступу, пошкодження або знищення. Він є складовою кібербезпеки і передбачає активне використання засобів захисту для виявлення, запобігання та реагування на загрози в кіберпросторі.

Основні компоненти кіберзахисту включають:

- Превентивні заходи: фаєрволи та системи виявлення вторгнень (забезпечують моніторинг мережевого трафіку та блокують потенційні загрози) та антивірусне та антималварне програмне забезпечення (захищає від шкідливих програм та вірусів).
- Контроль доступу: мінімізація привілеїв (забезпечення доступу до ресурсів лише тим користувачам, які дійсно цього потребують та багатофакторна автентифікація (використання кількох методів перевірки для підтвердження особи користувача).
- Шифрування даних: захист даних під час передачі та зберігання за допомогою шифрування, що ускладнює доступ до них для неавторизованих осіб.

- Моніторинг та виявлення загроз: використання засобів для безперервного моніторингу систем та мереж для виявлення аномальної активності та потенційних загроз.
- Планування реагування на інциденти: розробка планів дій на випадок кіберінцидентів, що включають виявлення, реагування та відновлення після атак.
- Навчання та підвищення обізнаності: постійне навчання персоналу щодо актуальних загроз та методів їх запобігання.
- Оновлення та патч-менеджмент: регулярне оновлення програмного забезпечення та встановлення патчів для усунення відомих вразливостей.
- Резервне копіювання та відновлення: регулярне створення резервних копій критичних даних та перевірка їх цілісності для забезпечення можливості відновлення після інцидентів.

Кіберзахист має на меті забезпечити стійкість інформаційних систем до атак, зменшити ризики та наслідки кібератак, а також забезпечити безперебійну роботу організацій.

Кібербезпека та кіберзахист є тісно пов'язаними поняттями, але вони мають деякі відмінності:

1) Обсяг і концепція:
   - Кібербезпека є ширшим поняттям, що охоплює всі аспекти захисту інформаційних систем та даних від кіберзагроз. Вона включає як технічні, так і організаційні заходи, управління ризиками, законодавчу відповідність, освіту персоналу та інші компоненти.
   - Кіберзахист є підмножиною кібербезпеки і фокусується на активних заходах щодо захисту систем та мереж від загроз. Це більш технічний аспект, спрямований на запобігання, виявлення та реагування на атаки.
2) Цілі та акценти:

- Кібербезпека ставить акцент на забезпеченні конфіденційності, цілісності та доступності інформації, управлінні ризиками, відповідності нормативним вимогам та загальній безпеці інформаційного середовища.
- Кіберзахист зосереджується на конкретних методах і технологіях для протидії атакам, таких як встановлення фаєрволів, систем виявлення вторгнень, антивірусного програмного забезпечення, а також на заходах для відновлення після атак.

3) Практичне застосування:
   - Кібербезпека включає розробку політик і процедур, навчання персоналу, оцінку та управління ризиками, планування безперервності бізнесу та відновлення після інцидентів.
   - Кіберзахист охоплює більш конкретні технічні заходи, такі як моніторинг мережевого трафіку, шифрування даних, регулярне оновлення програмного забезпечення, резервне копіювання та застосування багатофакторної автентифікації.
4) Організаційна структура:
   - У великих організаціях кібербезпека зазвичай включає різні відділи та ролі, що відповідають за різні аспекти безпеки, включаючи правові, адміністративні та технічні питання.
   - Кіберзахист зазвичай здійснюється спеціалізованими командами, такими як команди реагування на інциденти або оперативні центри безпеки, які займаються технічним захистом і реагуванням на загрози.

Таким чином, кібербезпека є всеосяжною дисципліною, що включає в себе широкий спектр заходів для захисту інформаційних систем, тоді як кіберзахист концентрується на конкретних технічних заходах і активних діях для запобігання та реагування на кібератаки.Захист інформації є одним із основних потреб цифрової ери. Незважаючи на те, що це має бути комплексний підхід, у більшості

організацій вона реалізується лише у форматі встановлення та налаштування технічних засобів. Забуваючи про необхідність вжиття організаційних заходів, компанії та установи суттєво знижують ефективність захисту своїх даних.

1.2 Організаційний захист інформації

Захист інформації – це комплекс заходів, спрямований на досягнення певного рівня інформаційної безпеки. Це процес прийняття заходів для забезпечення конфіденційності, цілісності та доступу до інформації с ціллю запобігання несанкціонованого доступ, використання, змінення та знищення інформації.

Захист інформації містить в собі правові, організаційні та технічні заходи. Тільки ефективне сполучення всіх заходів зможе забезпечити надійний захист інформації в різних установах.

Організаційний захист інформації є організаційним початком, так званим «ядром» у загальній системі захисту конфіденційної інформації організації. Від повноти та якості рішення керівництвом організації та посадовими особами організаційних завдань залежить ефективність функціонування системи захисту інформації в цілому. Роль та місце організаційного захисту інформації в загальній системі заходів, спрямованих на захист конфіденційної інформації, визначаються винятковою важливістю прийняття керівництвом своєчасних та вірних рішень з урахуванням наявних у його розпорядженні сил, засобів, методів та способів захисту.

До визначення організаційного захисту, його напрямів та умов, є сенс розглянути джерела конфіденційної інформації та канали її витоку. Основними джерелами конфіденційної інформації є:

- персонал організації, допущений до конфіденційної інформації;
- носії конфіденційної інформації (документи, вироби);
- технічні засоби, призначені для зберігання та обробки інформації;
- засоби комунікації, що використовуються з метою передачі інформації;

- повідомлення, що передаються каналами зв'язку, що містять конфіденційну інформацію.

Способи обміну конфіденційною інформацією (наприклад, між співробітниками організації) можуть мати як безпосередній (особистий) характер, так і характер передачі повідомлень, що формуються на основі інформації, за допомогою технічних засобів і засобів комунікацій.

Організаційні канали передачі та обміну конфіденційною інформацією в ході їх функціонування можуть бути під негативним впливом з боку зловмисників, спрямованому на отримання цієї інформації. Цей вплив, у свою чергу, може призвести до виникнення каналів витоку конфіденційної інформації та вимагати від керівництва організації, керівників структурних підрозділів та персоналу вжиття заходів щодо захисту конфіденційної інформації, спрямованих на недопущення її витоку та несанкціонованого поширення.

Для визначення необхідних заходів щодо захисту інформації необхідно провести класифікацію всіх можливих каналів витоку інформації залежно від напрямів та специфіки діяльності організації, видів конфіденційної інформації, особливостей функціонування системи захисту інформації та інших факторів. Організаційні канали витоку конфіденційної інформації, що виникають у процесі діяльності організації, можна підрозділити наступним чином:

- за джерелами загроз інформації, що захищається (зовнішні та внутрішні);
- за видами конфіденційної інформації або таємниць (державна, комерційна, службова чи інша таємниця; персональні дані працівників організації);
- за джерелами конфіденційної інформації (персонал, носії інформації, технічні засоби зберігання та обробки інформації, засоби комунікації, повідомлення, що передаються або приймаються тощо);
- за способами або засобами доступу до інформації, що захищається (застосування технічних засобів, безпосередня і цілеспрямована робота з персоналом організації, здійснення безпосереднього доступу до інформації);

- за характером взаємодії з партнерами (канали витоку, що виникають у відсутність взаємодії, при здійсненні взаємодії, в умовах конкурентної боротьби);
- за тривалістю або часом дії (канали витоку постійної, короткочасної, а також періодичної чи епізодичної дії);
- за напрямами діяльності організації (канали витоку, що виникають у звичайних умовах або за повсякденної діяльності організації, при виконанні спільної роботи, здійснення міжнародного співробітництва, проведення нарад, виїзд персоналу за кордон, у ході рекламної та публікаторської або видавничої діяльності, при проведенні наукових досліджень про відрядження співробітників організації);
- через причин виникнення каналів витоку інформації (дії зловмисників, помилки персоналу, розголошення конфіденційної інформації, випадкові обставини).

Серед основних напрямів захисту інформації поряд з організаційною виділяють правовий та інженерно-технічний захист інформації. Проте організаційному захисту інформації серед цих напрямів приділяється особливе місце.

Організаційний захист інформації призначений, за допомогою вибору конкретних сил і засобів, у тому числі правових та інженерно-технічних, реалізувати на практиці спланованої керівництвом організації заходи щодо захисту інформації. Ці заходи вживаються в залежності від конкретної обстановки в організації, пов'язаної з наявністю можливих загроз, що впливають на інформацію, що захищається, і ведуть до її витоку.

Роль керівництва організації у вирішенні завдань захисту інформації важко переоцінити. Основними напрямками діяльності, що здійснюється керівником організації у цій галузі, є: планування заходів щодо захисту інформації та персональний контроль за їх виконанням, прийняття рішень про безпосередній доступ до конфіденційної інформації своїх співробітників та представників інших організацій, розподіл обов'язків та завдань між посадовими особами та

структурними підрозділами, аналітична робота тощо. Мета вжитих керівництвом організації та посадовими особами організаційних заходів – виключення витоку інформації та, таким чином, зменшення або повне виключення можливості заподіяння організації шкоди, до якої цей витік може призвести.

Система заходів захисту інформації у сенсі слова має будуватися з тих початкових умов і чинників, які, своєю чергою, визначаються станом спрямованості розвідок противника чи процесами конкурента над ринком товарів та послуг, спрямованими на оволодіння інформацією, що підлягає захисту. Це діє як на державному рівні, так і на рівні конкретної організації.

У нормативній та науковій літературі використовуються два приблизно рівнозначні визначення організаційного захисту інформації.

Організаційний захист інформації складова частина системи захисту інформації, що визначає та виробляє порядок та правила функціонування об'єктів захисту та діяльності посадових осіб з метою забезпечення захисту інформації.

Організаційний захист інформації в організації – це регламентація виробничої діяльності та взаємовідносин суб'єктів (співробітників організації) на нормативно-правовій основі, що виключає або послаблює завдання шкоди даній організації.

Основними напрямками організаційного захисту інформації є:

- Організація допуску та доступу до конфіденційної інформації та документів.
- Організація роботи з носіями відомостей.
- Організація внутрішньооб'єктного та пропускного режимів та охорони;
- Організація роботи з персоналом.
- Комплексне планування заходів щодо захисту інформації.
- Організація аналітичної роботи щодо попередження конфіденційної інформації та контролю її здійснення. витоку

Побудова системи організаційного захисту інформації має базуватись на наступних принципах:

- принцип комплексного підходу ефективне використання сил, засобів, способів і методів захисту інформації для вирішення поставлених завдань, залежно від конкретної ситуації, що складається, і наявності факторів, що послаблюють або підсилюють загрозу інформації, що захищається;
- принцип оперативності прийняття управлінських рішень (суттєво впливає на ефективність функціонування та гнучкість системи захисту інформації та відображає націленість керівництва та персоналу організації на вирішення завдань захисту інформації; даний принцип спрямований, у тому числі, і на випередження передбачуваних загроз цілісності конфіденційної інформації);
- принцип персональної відповідальності - найбільш ефективний розподіл завдань із захисту інформації між керівництвом та персоналом організації та визначення відповідальності за повноту та якість їх виконання.

Серед основних умов організаційного захисту можна виділити такі:

- безперервність всебічного аналізу функціонування системи захисту інформації з метою вжиття своєчасних заходів щодо підвищення її ефективності;
- неухильне дотримання керівництвом та персоналом організації встановлених і правил захисту конфіденційної інформації.

За дотримання перелічених умов забезпечується найбільш повне і якісне вирішення завдань захисту конфіденційної інформації для організації.

1.3 Організаційні заходи захисту інформації

Організаційні заходи захисту інформації – це набір процедур, політик, практик та правил, які впроваджуються в організації для забезпечення безпеки інформації. Ці заходи допомагають захистити інформаційні ресурси, мережі та системи від внутрішніх та зовнішніх загроз, таких як: несанкціонований доступ, витік даних, віруси, атаки та інші форми кіберзлочинів.

До організаційних заходів належать:

- заходи, що здійснюються при проектуванні, будівництві та обладнанні службових та виробничих будівель та приміщень. Їх мета – виключення можливості таємного проникнення на територію та приміщення; забезпечення зручності контролю проходу та переміщення людей, проїзду транспорту та інших засобів пересування; створення окремих виробничих типу конфіденційності робіт із самостійними системами доступу тощо;
- заходи, що здійснюються при виборі персоналу, що включають ознайомлення зі співробітниками, їх вивчення, навчання правил роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація та підтримка надійного пропускного режиму та контролю відвідувачів;
- організація надійної охорони приміщень та території;
- організація зберігання та використання документів та носіїв конфіденційної інформації, включаючи порядок обліку, видачі, виконання та повернення;
- Організація захисту інформації: призначення відповідального за захист інформації у конкретних виробничих колективах, проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядок обліку, зберігання та знищення документів тощо;
- Організація регулярного навчання співробітників.

Розробка комплексу організаційних засобів захисту інформації повинна входити в компетенцію служби безпеки. Найчастіше фахівці з безпеки:

- розробляють внутрішню документацію, що встановлює правила роботи з комп'ютерною технікою та конфіденційною інформацією;
- проводять інструктаж і періодичні перевірки персоналу;
- ініціюють підписання додаткових угод до трудових договорів, де вказана відповідальність за розголошення або неправомірне використання відомостей, що стали відомі по роботі;

- розмежовують зони відповідальності, щоби виключити ситуації, коли масиви найбільш важливих даних знаходяться в розпорядженні одного із співробітників;
- організують роботу в загальних програмах документообігу і стежать, щоби критично важливі файли не зберігалися поза мережевих дисків;
- впроваджують програмні продукти, що захищають дані від копіювання або знищення будь-яким користувачем, в тому числі топменеджментом організації;
- складають плани відновлення системи на випадок виходу з ладу з якихось причин.

Регламент щодо забезпечення інформаційної безпеки – внутрішній документ організації, що враховує особливості бізнес-процесів і інформаційної інфраструктури, а також архітектуру системи.

В будь-якій діяльності виникають труднощі, які потребують вирішення. Щоб ефективно їх вирішувати, необхідно застосовувати системний підхід, аналізувати причини їх виникнення та розробляти оптимальні стратегії їх подолання. При реалізації організаційних заходів можливе виникнення таких проблем:

- Велика кількість нормативно-правових документів. По-перше, спеціалістам з захисту потрібно знати про те, що нормативно-правова база велика та має різні документ для різних організацій та напрямів, по-друге, для вивчення потрібних документів потрібно багато часу.
- Зміна нормативно-правових актів. Інформаційні технології – це галузь, яка постійно розвивається, тому питання захисту інформації маю встигати за розвитком. Звідси виходить постійна зміна актів, що ускладнює роботу фахівців.
- Складність мов нормативно-правових актів. Зазвичай нормативно-правові акти поєднують між собою технічну та юридичну мови, що ускладнює роботу фахівців.

- Зміна технічної інфраструктури. Будь-які змін в ІТ-інфраструктурі організації, такі як поява нового сервера чи робочого місця, зміна діючих робочих місць, введення, виведення з експлуатації або модернізація інформаційних систем, повинні відображатись у внутрішній організаційно-розпорядчій документації. Але є дуже поширеними ситуації, коли регламентуючу документацію розробляють один раз, а далі її актуалізують або актуалізують вкрай рідко. Звичайно регламенти, що не відповідають дійсності, не працюють і не сприяють досягненню потрібного рівня інформаційної безпеки.
- Кадрові перестановки. Більш ніж 80% випадків кіберінцидентів пов'язані з помилкам працівників. Будь-які кадрові зміни впливають на інформаційну безпеку. По-перше, кожний новий співробітник несе разом с собою рівень кваліфікації та розуміння безпеки, що може створювати вразливості в системі. По-друге, зміни в складі фахівців можуть призвести до розголошення інформації або до несанкціонованого доступу зі сторін звільнених співробітників. Крім цього, кадрові зміни також потребують регулярного оновлення доступів та привілей для забезпечення відповідного рівня захисту даних. Тому діяльність співробітників, які отримують доступ к інформаційним системам, повинна чітко регламентуватися.
- Дефіцит спеціалістів в області захисту інформації. Великій кількості організацій не вистачає висококваліфікованих спеціалістів з захисту інформації. Тому нерідко питання захисту переходять до некваліфікованих співробітників, що призводить до низького рівня захисту або його відсутності. Також потрібно відмітити, що навіть кваліфікований фахівець має постійно модернізувати свої знання: проходити періодично перенавчання чи підвищення кваліфікації.
- Проблеми фінансування. Внутрішню організаційно-розпорядчу документацію можна розробити самостійно, або можна звернутися до

інтеграторів, які мають професійний досвід та відповідну ліцензію у сфері інформаційної безпеки. Проте ці послуг є достатньо дорогими, при тому таку документацію постійно потрібно підтримувати в актуальному стані.

2 ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВСЬКОЇ УСТАНОВИ

2.1 Поняття інформаційної безпеки банківської установи

Становлення України як правової держави зумовлює реформування усіх сфер життя суспільства, зокрема правовідносин в економічній, фінансовій сфері, які в значній мірі ґрунтуються на ефективній банківській діяльності.

Необхідною умовою побудови та функціонування банківської системи є повне забезпечення безпеки у всіх сферах банківської діяльності, важливою складовою якої є безпека економічної інформації.

Знаючи, що банківська система будь-якої сучасної держави не існує відсторонено, а перебуває у тісному взаємозв'язку із банківськими системами інших країн і міжнародними банківськими організаціями, проблема забезпечення надійності, безпечності, стабільності банківської діяльності виходить далеко поза межи суто внутрішньодержавного регулювання.

Стрімка інформатизація та розвиток глобальних інформаційно-комунікаційних мереж, окрім автоматизації звичних банківських процесів, ще й постійно надають можливості створення нових банківських послуг, таких як «SMS-банкінг», «Інтернет-банкінг», «WebMoney Banking» тощо.

В умовах значної залежності банківської діяльності від надійності інформаційних технологій, які вона використовує, забезпечення інформаційної безпеки стає однією з фундаментальних засад існування банківської системи взагалі. Одним з основних напрямів забезпечення інформаційної безпеки будь-якої банківської установи є охорона банківської таємниці.

У структурі інформаційної безпеки банківської установи виділяють такі основні складові:

- безпека інформаційних ресурсів;
- безпека інформаційної інфраструктури;
- безпека «інформаційного поля».

Інформаційні ресурси банківської установи – це взаємозв'язана, упорядкована, систематизована і закріплена на матеріальних носіях інформація,

яка належить банківській установі. Відповідно безпека інформаційних ресурсів полягає у збереженні такої інформації від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності).

Безпека інформаційної інфраструктури полягає у такому стані захищеності електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку банківської установи, яка забезпечує цілісність і доступність інформації, що в них обробляється (зберігається чи циркулює).

Безпека інформаційного середовища банківської установи базується на контролі здебільшого несистематизованих потоків інформації, які поширюються різними учасниками інформаційних відносин, такими як телерадіоорганізації, друковані ЗМІ, Інтернет-видання, конкуренти, органи державної влади, місцевого самоврядування тощо.

Інформаційна безпека будь-якої організації базується на комплексі заходів, що виконуються відповідно до встановлених вимог. Основними джерелами цих вимог є:

1) Результати оцінювання ризиків для організації, які враховують загальну бізнес-стратегію та цілі. Під час оцінки ризиків ідентифікують загрози для ресурсів системи управління інформаційною безпекою, оцінюють вразливість та ймовірність подій, а також визначають величину потенційного впливу.
2) Правові вимоги, визначені законодавством, договорами та угодами з партнерами.
3) Власний набір принципів, цілей та бізнес-вимог щодо обробки інформації, розроблений організацією для підтримки своєї діяльності.

Методичними рекомендаціями щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України серед джерел вимог з інформаційної безпеки визначено:

- закони України;
- нормативно-правові акти Національного банку України;

- вимоги платіжних систем та систем переказу коштів;
- внутрішні нормативні документи банку;
- умови угод та договорів з третіми сторонами тощо.

Важливим є те, що вимоги з інформаційної безпеки для платіжних систем та систем переказів коштів висуваються платіжною організацією платіжної системи та системи переказу коштів, тому вони можуть відрізнятися від вимог Національного банку України (крім СЕП та НСМЕП, платіжними організаціями яких є Національний банк України).

Особливу увагу потрібно приділяти умовам угод і договорів з третіми сторонами. Відповідно до стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010, безпека інформації та засобів її обробки в банку не повинна погіршуватися через введення в експлуатацію продуктів або послуг зовнішніх постачальників. Якщо є бізнес-потреба співпрацювати із зовнішніми сторонами, що може вимагати доступу до інформації або засобів її обробки банку, або в отриманні від них чи наданні їм продуктів і послуг, банк повинен проводити оцінку ризиків для визначення вимог щодо заходів безпеки та наслідків можливих порушень. Заходи безпеки мають бути погоджені та визначені в угоді із зовнішньою стороною. Це стосується не лише договорів про надання послуг клієнтам банку (системи типу «клієнт-банк», інтернет-банкінг, мобільний банкінг тощо), а й послуг зовнішніх постачальників (розробка та супровід програмного забезпечення, придбання та технічне обслуговування обладнання, надання послуг зв’язку тощо).

Огляд вимог з вищезазначених джерел сприяє точному визначенню цілей СУІБ та заходів безпеки, які здатні знизити ризики та вразливості в діяльності банку, враховуючи специфіку його функціонування.

Вразливості, що можуть спричинити негативний вплив загроз на інформаційну безпеку банку, можуть бути розглянуті на таких рівнях:

- банк загалом;
- процеси та процедури;

- системи управління;
- персонал;
- фізичне середовище;
- конфігурація програмно-технічних комплексів, обладнання тощо;
- залежність від зовнішніх організацій.

Некоректно впроваджені або неефективні заходи безпеки є одним із типів вразливостей, які знижують рівень безпеки як банку загалом, так і кожного окремого бізнес-процесу чи банківського продукту.

Оцінювання інформаційної безпеки банківської установи здійснюється з урахуванням основних аспектів інформаційної безпеки, які включають:

- Конфіденційність: властивість інформації, що гарантує її недоступність для неавторизованих користувачів або процесів.
- Цілісність: властивість інформації, що забезпечує її неможливість модифікації неавторизованими користувачами або процесами. Цілісність системи означає, що жоден компонент системи не може бути видалений, змінений або доданий з порушенням політики безпеки.
- Доступність: властивість ресурсу системи, яка гарантує, що авторизований користувач або процес може використовувати ресурс відповідно до встановлених правил без значних затримок, тобто у необхідній формі, місці та часі.
- Спостережність: властивість системи, яка дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно ідентифікувати користувачів і процеси, причетні до певних подій, з метою запобігання порушенням політики безпеки та забезпечення відповідальності за певні дії.

Нормативно-правові засади забезпечення інформаційної безпеки в Україні становлять: Закон України «Про інформацію», Закон України «Про доступ до публічної інформації», Закон України «Про захист інформації в інформаційно-

телекомуникаційних системах», Закон України «Про електронний документ і електронний документообіг», Закон України «Про електронний цифровий підпис», Закон України «Про захист персональних даних».

Основи забезпечення інформаційної безпеки в банківській діяльності визначаються: Законом України «Про банки і банківську діяльність», Законом України «Про Національний банк України», Законом України «Про платіжні системи та переказ коштів в Україні», нормативно-правовими актами Національного банку України.

2.2 Загрози інформаційній безпеці банківської установи

Найбільш серйозними загрозами для безпеки інформаційних ресурсів є витік або втрата цих ресурсів, зокрема відомостей, що становлять банківську таємницю. Загрози можуть реалізовуватися через:

- підкуп осіб, які мають безпосередній доступ до банківської таємниці та іншої конфіденційної інформації банку;
- необережне або недбале поводження з банківською таємницею та іншою інформацією з обмеженим доступом;
- недотримання вимог щодо збереження конфіденційної інформації під час контактів з контролюючими та наглядовими органами через правову та психологічну непідготовленість відповідальних працівників банку.

Протидія таким загрозам повинна передбачати:

- визначення надійності працівників, які працюватимуть з банківською таємницею та іншою конфіденційною інформацією;
- організацію спеціального діловодства для відомостей, що становлять банківську таємницю та іншу інформацію з обмеженим доступом;
- обґрунтування та впровадження диференційованого доступу працівників до банківської таємниці та конфіденційної інформації, що

дозволяє ознайомлюватися і працювати з нею лише в межах виконання функціональних обов'язків;

- закріплення персональної відповідальності працівників за збереження наданих їм або розроблених документів та інших носіїв інформації з обмеженим доступом;
- обмеження доступу працівників і сторонніх осіб до приміщень, де обробляється або зберігається конфіденційна інформація;
- впровадження заходів контролю за роботою працівників з носіями конфіденційної інформації та ефективної системи виявлення і фіксації протиправних дій з такою інформацією;
- створення надійної та ефективної системи зберігання носіїв інформації, яка унеможливлює несанкціоноване ознайомлення, знищення чи підробку інформації.

Суттєвими загрозами для безпеки інформаційної інфраструктури є:

- неофіційний доступ і зняття захищеної інформації, що охороняється за допомогою технічних засобів;
- перехоплення інформації, що передається через засоби і системи зв'язку та обчислювальні техніки, шляхом використання технічних засобів негласного зняття інформації, несанкціонованого доступу до неї та навмисних технічних впливів під час її обробки та зберігання;
- підслуховування конфіденційних переговорів за допомогою технічних засобів у службових приміщеннях, транспортних засобах тощо.

Протидія таким загрозам має базуватися на широкому та економічно обґрунтованому застосуванні технічних засобів безпеки інформаційної інфраструктури.

Конкретними заходами для усунення загроз безпеці інформаційної інфраструктури банківської установи мають бути:

- Забезпечення цілісності засобів захисту, технічного та програмного середовища шляхом фізичного збереження інформаційних ресурсів,

стабільності програмного забезпечення та ефективної роботи захисних механізмів, що ізолюють їх від несанкціонованого доступу.

- Захист інформації від витоку через фізичні поля шляхом контролю за акустичними та електромагнітними випромінюваннями та захисту комунікаційних мереж та будівельних конструкцій.
- Використання криптографічного захисту для найціннішої інформації під час обробки у комп'ютерних системах та мережах електрозв'язку.
- Надання різнорівневого доступу до даних та операцій за допомогою програмно-технічних засобів, а також розмежування прав доступу користувачів до інформаційних ресурсів залежно від їхньої ролі та обов'язків.
- Ідентифікація користувачів та їхніх дій у системах засобів обчислення та мережах електрозв'язку з використанням різних методів аутентифікації, таких як паролі, ключі, картки та біометричні дані.
- Реєстрація дій користувачів з інформаційними ресурсами для виявлення потенційних загроз та протиправних спроб доступу.
- Запобігання передачі інформації по незахищеним зв'язкам та виявлення програм-вірусів у системах обробки даних.
- Регулярна перевірка технічних засобів та приміщень для виявлення можливих пристроїв несанкціонованого доступу.
- Організація спеціальних приміщень для забезпечення конфіденційності під час проведення конфіденційних переговорів та інших конфіденційних процесів.

Серйозними загрозами для безпеки "інформаційного поля" є підривання репутації банківської установи, виникнення проблем у взаємовідносинах з реальними та потенційними клієнтами, конкурентами, контролюючими та правоохоронними органами. Ці загрози в основному викликаються поширенням недостовірної, заздалегідь неправдивої інформації про банківську установу та

здійсненням негативних інформаційних впливів на її керівництво, працівників і т.д.

Щоб ліквідувати загрози безпеці "інформаційного поля" банківської установи, потрібно вжити такі конкретні заходи:

- Створення ефективної інформаційно-аналітичної системи.
- Швидка реакція на поширення недостовірної інформації про банк.
- Координація та централізоване поширення позитивної інформації про банк, що підвищує його імідж серед клієнтів.
- Встановлення інформаційної співпраці з державними та місцевими органами влади в рамках чинного законодавства.

Отже, з огляду на вищезазначені загрози та заходи їх подолання, система забезпечення інформаційної безпеки банківської установи може бути охарактеризована як комплексний набір організаційних, технічних, програмних і криптографічних заходів для захисту інформації, забезпечення цілісності та доступності, а також протидії негативному інформаційному впливу.

2.3 Управління інформаційною безпекою в банківській установі та супровід цього процесу документацією

Система управління інформаційною безпекою представляє сучасний підхід до забезпечення безпеки інформаційних активів у організації, що ґрунтується на найкращих міжнародних практиках. Стандарти Національного банку України базуються на міжнародних стандартах ISO 27001 та ISO 27002, а також включають додаткові вимоги щодо захисту інформації, адаптовані до конкретних потреб банківської галузі та вимог правового середовища, які вже відображені у нормативних документах Національного банку України.

Відповідність системи управління інформаційною безпекою стандартам Національного банку України, зокрема СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, забезпечує відповідність міжнародним стандартам ISO 27001 та ISO 27002 і надає можливість отримати відповідний сертифікат.

Необхідність впровадження стандартів управління інформаційною безпекою у банках України визначена вимогами Базельського комітету з управління та зменшення операційних ризиків банків в рамках Базельських стандартів (Basel II).

Впровадження стандартів управління інформаційною безпекою в банках України дозволить:

- оптимізувати витрати на створення та підтримку системи інформаційної безпеки;
- постійно моніторити та оцінювати ризики з урахуванням бізнес-цілей;
- ефективно виявляти найкритичніші ризики та знижувати ймовірність їх відтворення;
- розробити дієву політику інформаційної безпеки та забезпечити її якісне виконання;
- ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу;
- забезпечити розуміння питань інформаційної безпеки керівництвом та всіма працівниками банку;
- підвищити репутацію та ринкову привабливість банків;
- знизити ризики рейдерських та інших шкідливих для банку атак.

Слід зазначити, що ці переваги не можуть бути досягнуті лише формальним підходом до розробки, впровадження та функціонування системи управління інформаційною безпекою. Їх досягнення безпосередньо залежить від зацікавленості керівництва та працівників банку в підвищенні рівня інформаційної безпеки.

Крім того, впровадження стандартів управління інформаційною безпекою не може бути одноразовою акцією. Це постійний процес, що включає розробку, впровадження, функціонування, моніторинг, перегляд, підтримку та вдосконалення СУІБ. Саме тому методологічною основою управління

інформаційною безпекою згідно зі стандартами серії ISO 27000 є процесний підхід.

Для ефективного функціонування організації потрібно визначити та керувати численними видами діяльності. Будь-яку діяльність, яка використовує ресурси і потребує управління для перетворення вхідних даних у вихідні, можна вважати процесом. Часто вихідні дані одного процесу стають вхідними даними для наступного процесу.

Застосування системи процесів у межах організації, разом із ідентифікацією цих процесів та їх взаємодій, а також управління ними, можна назвати «процесним підходом». Процесний підхід до управління інформаційною безпекою акцентує увагу на:

- розумінні вимог інформаційної безпеки організації і необхідності розробки політики та цілей у цій сфері;
- впровадженні заходів безпеки та забезпеченні їх функціонування для управління ризиками інформаційної безпеки організації у контексті загальних бізнес-ризиків;
- моніторингу та перегляді продуктивності й ефективності СУІБ, а також на постійному вдосконаленні, заснованому на об'єктивному вимірюванні.

У межах такого підходу до процесів СУІБ застосовується модель «Плануй-Виконуй-Перевіряй-Дій» («Plan-Do-Check-Act»), яка наведена на Рисунку 2.1. Ця модель описана у вступі до стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010. СУІБ, використовуючи як вхідні дані вимоги інформаційної безпеки та очікування зацікавлених сторін, за допомогою необхідних дій і процесів генерує вихідні дані інформаційної безпеки, що відповідають цим вимогам та очікуванням.

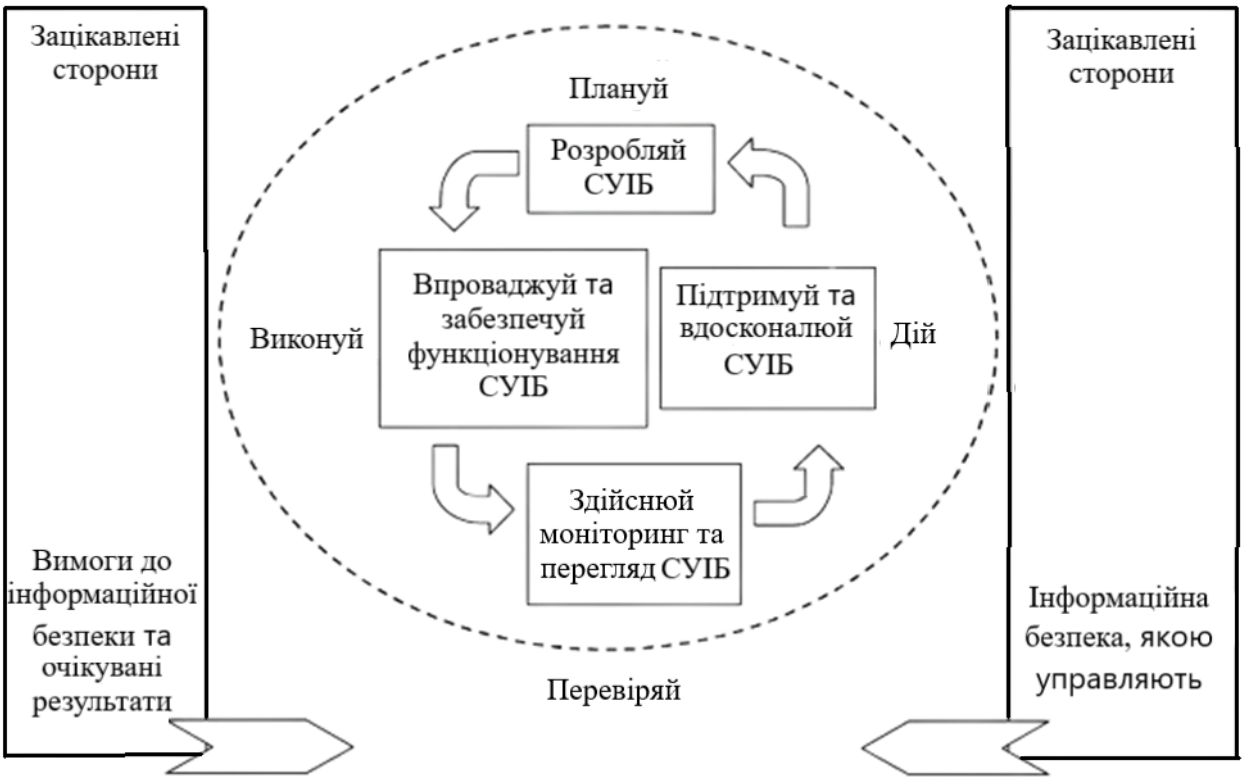

Рисунок 2.1 – Модель «Плануй-Виконуй-Перевіряй-Дій»

Плануй (розробляй СУІБ). Розробити політику СУІБ, а також визначити цілі, процеси та процедури, необхідні для управління ризиками та вдосконалення інформаційної безпеки, щоб досягати результатів, які відповідають загальним політикам та цілям організації.

Виконуй (впроваджуй, забезпечуй функціонування СУІБ). Впровадити та забезпечити функціонування політики інформаційної безпеки, заходів безпеки, процесів та процедур СУІБ.

Перевіряй (здійснюй моніторинг та перегляд СУІБ). Оцінювати та, за можливості, вимірювати ефективність процесів згідно з політикою, цілями СУІБ та практичним досвідом, і звітувати про результати керівництву для перегляду.

Дій (підтримуй та вдосконалюй СУІБ). Вживати коригувальні та запобіжні заходи на основі результатів внутрішнього аудиту і перегляду СУІБ з боку керівництва або іншої важливої інформації, щоб забезпечити постійне вдосконалення СУІБ.

Процес управління ризиками інформаційної безпеки банку повинен охоплювати:

- Аналіз та ідентифікацію ризиків.
- Оцінку ризиків з урахуванням їхнього впливу на бізнес та ймовірності виникнення.
- Інформування осіб, які приймають рішення, та акціонерів банку про ймовірності та впливи цих ризиків, щоб ймовірність і наслідки були зрозумілими.
- Встановлення порядку та пріоритетів обробки ризиків.
- Визначення пріоритетів виконання дій щодо зниження ризиків.
- Участь керівництва у процесі прийняття рішень щодо управління ризиками та його інформування про стан управління ризиками.
- Ефективний моніторинг та регулярний перегляд ризиків і процесу управління ризиками.
- Інформування керівництва та персоналу про ризики і дії щодо їх управління.

3 РЕКОМЕНДАЦІЇ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЗАБЕЗБЕЧЕННЯ ЗАХИСТУ БАНКІВСЬКИХ СИСТЕМ

3.1 Документація СУІБ

Загальний комплект документів, необхідний для впровадження СУІБ відповідно до стандарту ISO 27001, має чотирирівневу структуру.

3.1.1. Адміністративні документи

Адміністративні документи є обов’язковою початком підготовки до впровадження СУІБ. Вони включають::

- Наказ про створення спеціального керівного органу з питань інформаційної безпеки (за необхідністю).
- Положення про спеціальний керівний орган з питань інформаційної безпеки (за його наявності).
- Наказ про покладення обов'язків цього органу на існуючий керівний орган (за відсутності спеціального органу).
- Наказ про впровадження та функціонування СУІБ.
- Наказ про призначення керівника проекту впровадження та функціонування СУІБ.
- Положення про службу захисту інформації (підрозділ інформаційної безпеки).
- Положення про службу безпеки (охорона, пропускний та внутрішньо-банківський режим тощо).
- Посадові інструкції відповідальних за впровадження та функціонування СУІБ осіб.
- Організаційна структура банку.

Ці документи повинні бути оформлені відповідно до правил внутрішнього діловодства банку і можуть бути комбінованими залежно від специфіки роботи банку. Наприклад, якщо підрозділ захисту інформації є частиною структурного

підрозділу разом з фахівцями з фізичної безпеки, може створюватися єдине положення про підрозділ банківської безпеки, а назви підрозділів формуються згідно з внутрішніми правилами банку.

3.1.2 Документи верхнього рівня

Документи верхнього рівня є основою СУІБ і поділяються на дві групи. Перша група включає два ключові документи, що визначають стратегію розвитку банку та загальну політику інформаційної безпеки.

Стратегія розвитку банку містить основні стратегічні цілі банку, включаючи впровадження нових бізнес-процесів і банківських продуктів із використанням новітніх технологій, які потребують захисту інформації. Цей документ забезпечує планування розвитку інфраструктури банку та заходів безпеки для зменшення операційних ризиків.

Політика інформаційної безпеки банку включає основні цілі та принципи забезпечення безпеки банку. Ці документи мають бути короткими, не більше 2-3 сторінок, зрозумілими для всіх працівників банку та достатньо конкретними.

Друга група документів верхнього рівня описує основу побудови СУІБ і включає:

1) Цілі СУІБ.
2) Сфера застосування СУІБ.
3) Організаційна структура банку, яка охоплюється СУІБ.
4) Політика управління інформаційною безпекою.
5) Опис методології оцінки ризиків.
6) Звіт щодо оцінки ризиків.
7) Опис методології оброблення ризиків з визначенням критеріїв прийняття залишкових ризиків.
8) План оброблення ризиків.
9) Положення щодо застосовності.

Перші чотири документи можуть бути об'єднані в один – політику управління інформаційною безпекою, але перші три мають бути обов'язково доданими у вигляді окремих розділів.

Політика управління інформаційною безпекою створюється передостанньою, після завершення аналізу поточного стану інформаційної безпеки, оцінки ризиків та розробки плану оброблення ризиків. Вона повинна містити інформацію про необхідні заходи безпеки та плани щодо зменшення ризиків. Створення окремих цільових політик дозволяє уникнути докладного опису всіх заходів безпеки в одному документі, надаючи замість цього посилання на відповідні політики.

Останнім створюється документ "Політика щодо застосовності", в якому міститься перелік заходів безпеки відповідно до стандарту Національного банку України, доповнений додатковими заходами безпеки (з поясненням причин їх реалізації та коротким описом їх впровадження в банку).

Наведений перелік документів другої групи верхнього рівня є неповним і необов'язковим, його можна скоротити або доповнити іншими документами. При визначенні переліку цих документів слід враховувати, що короткі, чіткі та зрозумілі документи є більш зручними та ефективними, ніж один великий та складно структурований документ. Останній складно використовувати і оновлювати у зв’язку зі змінами інфраструктури банку, технології обробки інформації та заміни засобів захисту. Для полегшення роботи з усіма документами рекомендується ввести єдиний підхід до їх структури.

3.1.3.Документи середнього рівня

Документи середнього рівня фактично є технічними і описують способи реалізації заходів безпеки для захисту ресурсів СУІБ від загроз. Вони деталізують конкретні операції, які мають виконуватися різними користувачами, визначають питання розподілу повноважень та відповідальності за кожну операцію, встановлюють строки виконання кожної операції та шаблони угод із зовнішніми сторонами тощо.

Ці документи повинні створюватися не лише спеціалістами з інформаційної безпеки, але й спеціалістами відповідних підрозділів, зокрема: фахівцями з інформаційних технологій, фізичного захисту, роботи з персоналом, юридичного відділу та ін. Основними користувачами документів середнього рівня є керівники відповідних підрозділів, відповідальні особи за окремі ресурси СУІБ та адміністратори.

Перелік документів середнього рівня формується згідно із Додатком А стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010. До них в основному належать описи різноманітних процедур щодо:

3.1.4 Документи нижнього рівня

Документи нижнього рівня можна поділити на дві групи.

Перша група включає записи різного типу, що вимагаються стандартами. Це журнали реєстрації подій, таких як несправності обладнання, журнали аудиту різних систем (операційної, прикладних програм, надання доступу до мережі Інтернет тощо). Частина цих записів ведеться автоматично, тому важливо забезпечити їх збереження та захист від знищення і несанкціонованої модифікації.

Друга група документів нижнього рівня містить інструкції (пам'ятки) щодо виконання різних операцій з інформаційної безпеки, призначені для кінцевих користувачів. При правильному підході до створення документації ці документи є ефективним інструментом для зменшення ризиків, пов’язаних з людським фактором.

3.2 Рекомендації стосовно документації

Створення документації може бути довгим та важким процесом, тож для полегшення роботи спеціалістів та поліпшення якості створених документів можна використати наступні рекомендації:

1) Політика управління інформаційною безпекою може бути розділена на дві частини: зовнішня політика, що описує управління інформаційною

безпекою для зовнішніх зв'язків банку та внутрішня політика, що описує для працівників банку правила інформаційної безпеки.

2) Щоб скоротити обсяг політики управління інформаційною безпекою, рекомендується окремі питання винести в спеціалізовані цільові політики (положення) з відповідними посиланнями. Банк може створити такі окремі документи:
   - Перелік законодавчих, регуляторних і нормативних вимог з інформаційної безпеки.
   - Перелік відомостей, що містять інформацію з обмеженим доступом.
   - Перелік критичних бізнес-процесів, банківських продуктів і програмно-технічних комплексів.
   - Політика визначення критичних бізнес-процесів і банківських продуктів.
   - Політика надання доступу до інформації.
   - Політика контролю доступу.
   - Політика парольного захисту.
   - Політика антивірусного захисту.
   - Політика захисту мережі банку.
   - Політика віддаленого доступу до ресурсів мережі.
   - Політика ідентифікації та автентифікації ресурсів СУІБ.
   - Політика криптографічного захисту інформації.
   - Політика «чистого екрана та чистого стола».
   - Інші політики відповідно до технології організації операційної роботи банку.
3) Під час перегляду наявних документів та підготовки нових рекомендується дотримуватися єдиних правил оформлення, що забезпечить легкість їх сприйняття користувачами.
4) Типова структура документів відповідно до міжнародних стандартів:
   - Титульний лист.

- Вступ.
- Терміни та скорочення.
- Ціль документа.
- Сфера застосування.
- Предмет документа та опис дій.
- Ролі та відповідальності.
- Перегляд документа.
- Перелік взаємопов'язаних документів.
- Історія змін.

Серед загальних рекомендацій щодо формування документів можна виділити такі:

- оформляти всі документи у єдиному стилі;
- робити документи простими для розуміння і максимально короткими;
- використовувати блок-схеми, рисунки, таблиці для спрощення розуміння;
- поєднувати загальні правила для користувачів в одному документі, якщо це можливо;
- відображати вимоги з інформаційної безпеки в посадових інструкціях;
- обирати оптимальний варіант поширення документів в електронному або паперовому вигляді залежно від технології документообігу банку (у разі використання електронних документів забезпечити їх цілісність протягом усього періоду використання);
- постійно переглядати перелік документації для оптимізації та зменшення обсягу конкретних документів;
- створювати журнали для записів лише там, де цього вимагають стандарти та чинні правила бізнесу (рекомендується автоматизувати процедуру ведення журналів, якщо це можливо).

Ці рекомендації полегшать не тільки процес створення документації, але, за допомогою систематизації та спрощення викладення умов, спростять фахівцям процедуру дотримання всіх вимог, що описані в цих документах.

3.3 Загальні організаційні рекомендації

Окрім рекомендації стосовно ведення документації, можна додати також загальні організаційні рекомендації, наприклад:

- Розширення політик моніторингу та реагування. Посилення моніторингу та аналітики поведінки користувачів допоможе вчасно виявляти і нейтралізувати внутрішні загрози та несанкціоновані дії. Система моніторингу. Створення системи реагування дозволить оперативно реагувати на потенційні загрози безпеці.
- Комплексні плани відновлення. Розробка та регулярне оновлення планів відновлення після інцидентів допоможе мінімізувати наслідки атак та забезпечити швидке відновлення нормальної роботи.
- Розробка стратегії безпеки. Банк повинен розробити стратегію безпеки, яка охоплює всі аспекти захисту систем, включаючи захист від кібератак, фізичний захист приміщень та даних, а також політику доступу.
- Удосконалення політики доступу. Важливо мати чітку політику доступу до банківських систем, включаючи визначення рівнів доступу, автентифікацію користувачів, обмеження доступу до конфіденційної інформації та регулярне оновлення паролів.
- Впровадження правил внутрішнього контролю. Установлення правил внутрішнього контролю, які обмежують можливість виникнення внутрішнього шахрайства або зловживань з боку працівників.
- Забезпечення відповідності стандартам безпеки. Відповідність міжнародним та національним стандартам безпеки, таким як PCI DSS

(стандарт безпеки платіжних карт), ISO 27001 (стандарт кібербезпеки) та іншим.

- Зміцнення партнерств. Банки повинні активно співпрацювати з національними та міжнародними організаціями кібербезпеки для обміну знаннями та кращих практик. Співпраця може включати спільні навчання, розробку стандартів та відповіді на інциденти.

Ці рекомендації допоможуть забезпечити ефективний рівень захисту банківських систем від сучасних кіберзагроз.

ВИСНОВКИ

Інформаційна безпека є ключовим аспектом забезпечення стабільності, надійності та ефективності банківських установ. В умовах цифрової трансформації та зростання кіберзагроз захист інформаційних ресурсів банків стає пріоритетним завданням. В ході виконання дипломної роботи було розроблено низку рекомендацій, які слід дотримуватись для якісного захисту в організаційному напрямі.

Впровадження стандартів управління інформаційною безпекою, зокрема ISO 27001 та ISO 27002, а також національних стандартів, дозволяє створити системний підхід до захисту інформації. Це забезпечує відповідність банку міжнародним вимогам та підвищує його ринкову привабливість.

Захист банківських систем повинен включати як організаційні, так і технічні заходи. Це охоплює створення політик безпеки, управління ризиками, впровадження технічних рішень для захисту мереж, систем та даних, а також підготовку персоналу.

Процес управління ризиками інформаційної безпеки є безперервним і включає ідентифікацію, оцінку, обробку та моніторинг ризиків. Це дозволяє вчасно виявляти та мінімізувати вплив потенційних загроз на бізнес-процеси банку.

Ефективне управління інформаційною безпекою вимагає активної участі керівництва банку. Це включає прийняття стратегічних рішень, підтримку впровадження політик безпеки та постійний моніторинг стану захищеності інформаційних ресурсів.

Підвищення обізнаності працівників банку щодо питань інформаційної безпеки є важливим елементом захисту. Регулярні навчання та тренінги допомагають зменшити ризики, пов’язані з людським фактором.

Створення чіткої і структурованої документації з інформаційної безпеки є необхідною умовою ефективного функціонування СУІБ. Документи повинні

бути зрозумілими, короткими та регулярно оновлюватися відповідно до змін у банківській інфраструктурі та вимог законодавства.

Загалом, ефективне впровадження організаційних рекомендацій з захисту банківських систем забезпечить високий рівень захисту інформаційних ресурсів, що сприятиме зниженню операційних ризиків та підвищенню довіри клієнтів до банківської установи.

Отже інформаційна безпека виступає одним з основних чинників сучасної банківської діяльності та становить фундамент її стабільності, надійності, ефективності. Забезпечення інформаційної безпеки банківської установи є складним безперервним динамічним процесом, який вимагає постійної уваги, моніторингу, удосконалення та відповідного правового забезпечення згідно з вимогами законодавства України та міжнародних стандартів управління інформаційною безпекою.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Безпека банківських систем : навч. посіб. / П. С. Усік, К. О. Буравченко; М-во освіти і науки України, Центральноукр. нац. техн. ун-т.— Кропивницький: ЦНТУ, 2022.
2. Методи захисту в банківській діяльності Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD): Видання офіційне/ Київ: НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ, 2010.
3. Інформаційні технології – Методи захисту - Системи менеджменту інформаційної безпеки – Вимоги/ МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001/ Друга редакція, 2013.
4. Інформаційна безпека банківської установи [Електронний ресурс]/ Режим доступу : http://obt.inf.ua/page10.html