Міністерство освіти і науки України
Центральноукраїнський національний технічний університет

Усік П. С., Буравченко К.О.

БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ

Навчальний посібник

Кропивницький
2022

УДК 004.7

Рекомендовано Вченою радою Центральноукраїнського національного технічного університету, протокол № 9 від 30 травня 2022 року

Рецензенти:

Гнатюк С.О., доктор технічних наук, професор, заступник декана факультету кібербезпеки, комп'ютерної та програмної інженерії з наукової роботи Національного авіаційного університету;

Євсєєв С.П., доктор технічних наук, професор, завідувач кафедрою кібербезпеки Національного технічного університету «Харківський політехнічний університет».

Усік П.С., Буравченко К.О.

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. — 194 с.

У навчальному посібнику розглянуто теоретичні й практичні питання основ і положень теорії безпеки банківських систем. Особливу увагу приділено системі управління інформаційною безпекою, в тому числі її нормативно-правовим забезпеченням.

Навчальний посібник призначений для студентів, які навчаються за спеціальністю «Кібербезпека», а також аспірантів, науковців та інженерно-технічних працівників з напряму «Інформаційні технології».

ВСТУП

В умовах широкого застосування обчислювальної техніки і засобів обміну інформацією поширюються можливості її витоку та несанкціонованого доступу до неї зі злочинною метою. Особливо уразливими сьогодні залишаються незахищені системи зв'язку, в тому числі обчислювальні мережі банків та комерційних установ. Інформація, циркулююча в них, може бути незаконно змінена, викрадена або знищена.

З метою протидії злочинам у сфері комп`ютерної інформації, або зменшення збитків від них, необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації. Необхідно знати також основні законодавчі положення в цій області, організаційні, програмно-технічні та інші заходи забезпечення безпеки інформації.

Актуальність даної проблеми пов'язана із зростанням можливостей обчислювальної техніки. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів роблять інформацію більш уразливою.

Метою даного навчального посібника є отримання досконалих знань в області безпеки банківських систем та їх практичних застосувань, а також формування професійної компетентності майбутніх фахівців з кібербезпеки, достатньої для роботи та розвитку кар’єри.

РОЗДІЛ 1. ОСНОВНІ ПОНЯТТЯ КІБЕРБЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

Суть, мета, завдання інформаційної безпеки банківських установ

Спочатку розглянемо коротко поняття безпеки банку загалом.

Безпека банку – це стан стійкої життєдіяльності, при якому забезпечується реалізація основних інтересів і пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування.

Метою діяльності банку щодо забезпечення інформаційної безпеки є зниження загроз інформаційній безпеці до прийнятного для банку рівня.

Основними завданнями банку щодо забезпечення інформаційної безпеки є:

– виявлення потенційних загроз інформаційній безпеці банку і вразливостей;

– запобігання інцидентам інформаційної безпеки;

– нейтралізація або мінімізація загроз інформаційній безпеці банку.

У структурі інформаційної безпеки банківської установи виділяють такі основні складові:

– безпека інформаційних ресурсів;

– безпека інформаційної інфраструктури;

– безпека інформаційного поля.

Під **інформаційними ресурсами банку** розуміють взаємозв’язану, упорядковану, систематизовану інформацію, яка циркулює в інформаційній системі банківської установи, зберігається на матеріальних носіях, і яка належить банківській установі. Відповідно безпека інформаційних ресурсів полягає у збереженні такої інформації від

несанкціонованого розповсюдження, використання і порушення її конфіденційності.

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 поля" банківської установи ґрунтується на контрольованості здебільшого несистематизованих потоків інформації, що оприлюднюється різноманітними учасниками інформаційних відносин: теле-радіо-організаціями, друкованими ЗМІ, Інтернет-виданнями, конкурентами, органами державної влади, місцевого самоврядування тощо.

Незважаючи на стрімкий розвиток інформаційно-комунікаційних технологій завдання дієвого вирішення питань інформаційної безпеки для кожної організації є індивідуальним.

Для банківських установ процеси забезпечення інформаційної безпеки чітко регламентовані. Існують закони і стандарти забезпечення належного рівня інформаційної безпеки, якими банки повинні керуватися у своїй діяльності, зокрема: Закони України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", стандарти Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, основою яких є на Міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27002, які забезпечують відповідність вимогам Базельського комітету Basel II з управління та зменшення операційних ризиків банків та інші.

Міжнародні стандарти управління інформаційною безпекою серії ISO 27000, дотримання яких є обов'язковим у банківській системі України, щодо інформаційної безпеки організації передбачають використання таких термінів:

Під **інформаційною безпекою** розуміють захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, в тому числі власникам і користувачам інформації і підтримуючої інфраструктури.

Засоби оброблення інформації – будь-яка система оброблення інформації, послуга чи інфраструктура, чи місце, де вони фізично розміщені.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Подія інформаційної безпеки – ідентифікована подія системи, служби або мережі, яка вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту чи раніше невідому ситуацію, яка може мати відношення до безпеки.

Інцидент інформаційної безпеки – одна або серія небажаних чи непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації бізнес-операцій і загрози інформаційній безпеці.

Загроза – потенційна причина небажаного інциденту, який може призвести до шкоди для системи або організації.

Вразливість – слабкість ресурсу СУІБ або групи ресурсів СУІБ, якою можуть скористатися одна або більше загроз.

Ризик – комбінація ймовірності події та її наслідку (ризиком інформаційної безпеки банку вважається ймовірність того, що визначена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду банку).

Оцінювання ризику – процес порівняння кількісно оціненого ризику із заданими критеріями ризику для встановлення його значимості.

Управління ризиком – скоординовані дії в організації щодо регулювання та контролю ризику.

Заходи безпеки – засоби управління ризиком, які включають політику, процедури, настанови, практику або організаційні заходи, які можуть бути адміністративного, технічного, управлінського або правового характеру.

Політика – загальні наміри та вказівки, затверджені керівництвом.

Згідно зі стандартом ISO/IEC 27001 практична реалізація заходів інформаційної безпеки банків повинна відбуватись за допомогою:

– розроблення політики системи управління інформаційної безпекою;

– забезпечення відповідності цілей системи управління заходам інформаційної безпеки;

– розподіл ролей і обов'язків, пов'язаних із інформаційною безпекою;

– доведення до персоналу організації важливості забезпечення та дотримання політики інформаційної безпеки;

– надання достатніх ресурсів для забезпечення підтримки інформаційної безпеки;

– побудова системи управління ризиками для забезпечення належного рівня інформаційної безпеки;

– забезпечення проведення внутрішнього аудиту системи управління інформаційною безпекою;

– проведення перевірок управлінських рішень, що запроваджуються керівництвом, щодо забезпечення належного рівня інформаційної безпеки.

Інформаційна безпека досягається впровадженням відповідних **заходів безпеки**, які охоплюють політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці заходи безпеки

необхідно розробити, впровадити, здійснювати моніторинг, переглядати та, за необхідності, вдосконалювати для гарантування досягнення певного рівня безпеки та бізнес-цілій банку. Це треба виконувати узгоджено з іншими процесами управління банком.

Інформація та допоміжні процеси, системи і мережі є важливими бізнес-ресурсами системи управління інформаційною безпекою (СУІБ). Визначення, досягнення, підтримка та вдосконалення інформаційної безпеки може бути суттєвим для підтримки конкурентоспроможності, готівкового обігу, рентабельності, комерційної репутації та відповідності законодавству.

Інформаційна безпека банківської установи, ґрунтується на системі заходів безпеки, що здійснюються відповідно до вимог безпеки. Основними джерелами вимог інформаційної безпеки організації є:

1) результат оцінювання ризиків для організації, який враховує загальну бізнес-стратегію та цілі;

2) правові вимоги, визначені законодавством, договорами і угодами організації з партнерами;

3) власний набір принципів, цілей та бізнес-вимог щодо оброблення інформації, який розроблено організацією для підтримки свого функціонування.

До сервісів оцінювання інформаційної безпеки банківської установи належать:

– конфіденційність;

– цілісність;

– доступність;

– спостережність (властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії).

Вплив основних сервісів інформаційної безпеки оцінюється щодо кожного бізнес-процесу, програмно-технічного комплексу банку. Слід зазначити, що для різних бізнес-процесів можуть бути виявлені однакові ризики втрати основних сервісів безпеки. Це свідчить про певні прогалини в забезпеченні інформаційної безпеки банку в цілому. У такому разі відповідні заходи щодо зниження виявлених ризиків інформаційної безпеки необхідно проводити для всіх бізнес-процесів банку.

Інформаційна безпека автоматизованих систем обробки інформації банку

Безпека автоматизованих систем обробки інформації банку – властивість, що полягає у спроможності протидіяти спробам завдання збитків власникам і користувачам системи, тобто захищеності від спроб розкрадання чи руйнування її компонентів.

Головними завданнями будь-якої системи інформаційної безпеки є:

– забезпечення доступності даних для авторизованих користувачів – можливості оперативного отримання інформаційних послуг;

– гарантія цілісності інформації – її актуальності і захищеності від несанкціонованих змін або знищення;

– забезпечення конфіденційності відомостей.

Незважаючи на безліч можливостей витоку інформації, безпеку банківських даних та їх конфіденційність забезпечити цілком можливо. Існує досить велика кількість способів захисту комп'ютерів. Є методи, які ґрунтуються на застосуванні безпечних операційних систем та апаратного забезпечення, що здатне захистити комп'ютерну систему. Хоча під час проектування комп'ютерної системи необхідно взяти до уваги чимало характеристик. Безпека є серед них однією з найважливіших.

Небезпечні програми деколи не правильно уподібнюються з комп'ютерними вірусами, тоді коли вірус – лише один із злочинних видів шкідливих програм.

В автоматизованих банківських системах (АБС) вибір засобів захисту інформації – досить складна задача, а при її рішенні особливо необхідно врахувати можливість різних протиправних дій щодо порушення працездатності такої системи, вартість реалізації засобів захисту і наявність різних зацікавлених сторін. Варто зазначити, що важливість забезпечення інформаційної безпеки оцінена і на державному рівні, що відбивається у вимогах нормативно-правових актів. Наприкінці 2017 року, Національний банк України встановив вимоги до кіберзахисту, які повинні впроваджуватися банками. Вимоги спрямовані на посилення захисту інформації у банківській системі з урахуванням актуальних кіберзагроз.

Заходи безпеки інформації включають:

1. Контроль доступу до ресурсів АБС (управління доступом).
2. Ідентифікація і автентифікація АБС (користувачів процесів і т.д.).
3. Реєстрація та аналіз подій, що відбуваються в АБС.
4. Контроль цілісності об’єктів АБС.
5. Шифрування даних.
6. Резервування ресурсів і компонентів АБС.

Кожен напрямок включає кілька етапів роботи. **Управління доступу** – захист інформації шляхом регулювання доступу до всіх ресурсів системи. Регламентуються порядок роботи користувачів і персоналу, право доступу до окремих файлів в базах даних і т.д.

Доступ до даних банку захищається за допомогою системи ідентифікації, тобто паролями або електронними ключами. *Ідентифікація* – це присвоєння коду кожному об'єкту персонального ідентифікатора. *Автентифікація* – встановлення автентичності. Нові можливості дозволяють використовувати багатофакторну посилену ідентифікацію при авторизації в банківській системі. Така автентифікація особливо актуальна в роботі співробітників, що мають права введення і підтвердження фінансових документів.

Для аналізу ефективності вжитих заходів необхідно вести облік або запис, які будуть відзначати працездатність й дієвість застосованих засобів захисту інформації в банку. Ці функції забезпечують отримання й аналіз інформації про стан ресурсів системи, реєстрацію дій, які можуть бути визначені як небезпечні ситуації, ведення журналу, який допоможе оперативно зафіксувати події, що відбуваються в системі. Аналіз журналу, якщо його вести належним чином, може допомогти у визначенні засобів, які використовував зловмисник під час порушення системи захисту, у визначенні реального стану системи, у виборі способів розслідування в разі порушення і підказати шляхи виправлення ситуації.

Контроль за цілісністю (захист від несанкціонованої модифікації суб'єктів системи) – контроль за цілісністю атрибутів суб'єкта, контроль за послідовністю і повнотою процесів та режимів їх виконання. Механізм контролю цілісності здійснює стеження за незмінністю контрольованих об'єктів, захист від шкідливого коду. При несанкціонованому знищенні, додаванні зайвих елементів та модифікації даних, зміну порядку розташування даних, формуванні фальсифікованих платіжних документів у відповідь на законні запити, активної ретрансляції повідомлень з їх затримкою. Цілісність порушується при, викраденні або незаконної зміні алгоритмів роботи. Забезпечення цілісності – частина комплексу заходів по досягненню безпеки інформації. Загрози, що відносяться до можливостей несанкціонованої модифікації інформації, є загрозами цілісності. Загрози, що відносяться до можливостей несанкціонованого ознайомлення з інформацією є загрозами конфіденційності. В загальному випадку вважається, що для захисту інформації повинні бути створені механізми захисту. Це управління доступом до ресурсів, включаючи доступ до паролів, надання рівнів доступу до об’єктів, ідентифікація, реєстрація та облік роботи користувачів. Порушення цілісності може статись в наслідок наступних причин:

1. Помилки користувачів, які викликають викривлення чи втрату інформації.

2. Навмисні дії осіб, які не мають прав доступу до системи.

3. Збої обладнання, які викликають викривлення чи втрату інформації.

4. Фізичний вплив на носії інформації.

5. Вірусні впливи.

Одним з дієвих методів реалізації вимог цілісності інформації є крипто-графічний захист інформації (шифрування, хешування, електронний цифровий підпис).

При **комплексному підході до захисту АБС**, напрям забезпечення цілісності та доступності інформації переростає в план заходів, що спрямовані на забезпечення безперервності роботи АБС. Система шифрування даних забезпечує безпеку при обміні інформацією, тому всі дані, передані в банк або прийняті від банку, шифруються спеціальним методом згідно стандартів ISO 8730 та ISO 8731. Засоби шифрування доволі надійно захищають комп'ютерну інформацію від кіберзагроз. Кодування тексту за допомогою складних математичних алгоритмів, отримує все більшу популярність. Звичайно, що не один з алгоритмів шифрування не дає стовідсоткової гарантії захисту від зловмисників, але все ж, деякі методи шифрування досить складні, щоб дати змогу ознайомитися з повідомленнями зашифрованого змісту. Досить дієвим та потужним є застосування для захисту інформації криптозахисту, тобто систем, які дозволяють зашифрувати та дешифрувати інформаційні потоки.

RSA (абревіатура від англ. Прізвищ Rivest, Shamir та Adleman) – це один із поширених методів шифрування на сьогодні. Алгоритм, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, який не має бути секретним, за допомогою нього проводиться обмін повідомленнями. Електронний цифровий підпис (ЕЦП) – це дані в

електронній формі, отримані за результатами криптографічного перетворення, які додаються до інших даних або документів і забезпечують їх цілісність та ідентифікацію автора. Криптографічні методи широко застосовуються у АБС та мають реалізацію у вигляді програмних, апаратних чи програмно-апаратних методів захисту інформації. Криптографія є провідним засобом забезпечення конфіденційності і контролю цілісності інформації.

Суворий облік каналів та серверів, а також заходи, що забезпечують технічний захист інформації і безпеку банку мають на увазі захист резервних копій, забезпечення безперебійного живлення устаткування, що містить цінну інформацію, обмежений доступ до сейфів та захист від витоку інформації акустичним способом.

Резервування ресурсів та абонентів АБС передбачає: організацію регулярних процедур порятунку і резервного зберігання критичних даних, періодичну перевірку резервних пристроїв обробки даних, підготовку фахівців, здатних замінити адміністраторів систем, реєстрацію систем та зберігання носіїв інформації в суворо визначених місцях, видачу їх уповноваженим особам з необхідними відмітками в реєстр траційних документах.

Безпека банкоматів та платіжних терміналів повинна забезпечуватися з використанням традиційних засобів – антивірусного захисту. В той же час специфіка таких пристроїв вимагає застосування додаткових засобів захисту. Створення «замкнутого програмно-апаратного середовища», повністю виключає установку любого стороннього програмного забезпечення і підключення зовнішніх пристроїв.

Система безпеки в цілому це безперервний процес ідентифікації, аналізу та контролю. Оскільки інформація, що знаходиться в базі даних банків являє собою реальну матеріальну цінність, то вимоги до зберігання та обробки цієї інформації завжди будуть підвищеними.

Уточнення і доповнення безлічі актуальних загроз безпеки банківської інформації, безпека інформації і кібербезпека в банківському секторі, це основа для створення нового синергетичного підходу в області інформаційної безпеки АБС. Для аналізу основних видів загроз безпеки банківської інформації використовується відома модель безпеки – тріада CIA (Confidentiality, Integrity, Availability) (рис. 1.1).

Рис.1.1 Модель тріади CIA

У моделі «конфіденційність» – забезпечення доступу до інформації тільки авторизованим користувачам, «цілісність» – забезпечення достовірності і повноти інформації, «доступність» – забезпечення доступу до інформації.

Модель синергетичного підходу – оцінка безпеки банківських систем. В процесі аналізу ризиків інформаційної безпеки можуть використовуватися спеціалізовані програмні комплекси, що дозволяють

автоматизувати процес аналізу вихідних даних та розрахунку значень ризику.

Метою інформаційної безпеки є забезпечення трьох найважливіших сервісів безпеки. Відповідно моделі безпеки інформації включають: конфіденційність, цілісність і доступність. Слід зазначити ключову особливість, характерну тільки пропонованому синергетичному підходу до безпеки банківської інформації. Основна мета запропонованого підходу – це порушення в системі забезпечення банківської інформації керованих емерджентних властивостей, спрямованих на отримання синергетичного ефекту, який досягається завдяки якісно новому підходу до безпеки. Таким чином, виходячи із потреби дотримання правила триєдиної позиції до забезпечення безпеки банківської інформації в рамках синергетичного підходу при взаємодії вибраних профілів безпеки і з метою підвищення рівня її захищеності є оцінювання величини ризику аналогічного грошового капіталу.

РОЗДІЛ 2. БАНКІВСЬКА ТАЄМНИЦЯ

Захист банківської таємниці в правовому полі

Банківська таємниця (bank secrecy) – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

Відповідно до Закону України "Про банки і банківську діяльність" до б. т. відносять відомості та інформацію:

1) про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) про операції, проведені на користь чи за дорученням клієнта, та здійснені ним угоди;

3) про фінансово-економічний стан клієнтів;

4) про системи охорони банку та клієнтів;

5) про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;

6) стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) щодо звітності банку, за винятком тієї, що підлягає опублікуванню;

8) про коди банків для захисту інформації.

Згідно з положеннями статті 1076 Цивільного кодексу України та статті 60 Закону України «Про банки і банківську діяльність», **будь-яка інформація, що стосується клієнта, якою банк володіє на законних підставах, є банківською таємницею, тобто до банківської таємниці належить інформація про діяльність і фінансовий** стан клієнта, що

стала відома банку у процесі його обслуговування і взаємовідносин з ним або з третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

Поняття «конфіденційна інформація» наведено в Законі України «Про інформацію», де зазначено, що остання за своїм правовим режимом є інформацією з обмеженим доступом і вона являє собою «... відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов» (ст. 30).

Відповідно до пункту 1 статті 1076 Цивільного кодексу України, відомості, що складають банківську таємницю, можуть бути надані банком органам державної влади та їх посадовим особам виключно у випадках та в порядку, встановлених законом України «Про банки і банківську діяльність».

Стаття 62 (Порядок розкриття банківської таємниці) Закону України «Про банки і банківську діяльність» **передбачає декілька випадків розкриття банками інформації, що становить банківську таємницю, у повному обсязі**, а саме:

1) на письмовий запит або з письмового дозволу власника такої інформації;

2) на письмову вимогу суду або за рішенням суду;

3) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;

4) органам Державної податкової служби України на їх письмову вимогу з питань оподаткування або валютного контролю стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу.

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:

1) бути викладена на бланку державного органу встановленої форми;

2) бути надана за підписом керівника державного органу, скріпленого гербовою печаткою;

3) містити передбачені цим Законом підстави для отримання цієї інформації;

4) містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Банку забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їх імена зазначені у документах, угодах та операціях клієнта.

Банк **має право надавати загальну інформацію, що становить банківську таємницю, іншим банкам в обсягах, необхідних при наданні кредитів, банківських гарантій.**

Обмеження стосовно отримання інформації, що містить банківську таємницю, передбачені цією статтею, не поширюються на службовців Національного банку України або уповноважених ними осіб, які в межах повноважень, наданих Законом України "Про Національний банк України", здійснюють функції банківського нагляду або валютного контролю.

Особи, винні в порушенні порядку розкриття та використання банківської таємниці, несуть відповідальність згідно із законами України.

Письмова вимога суду щодо надання інформації, яка містить банківську таємницю, має відповідати нормам частини 2 статті 62 Закону України «Про банки і банківську діяльність».

Подібним чином визначений і правовий режим захисту конфіденційної інформації. Відповідно до ч. 3 ст. 30 Закону України «Про інформацію», власникам конфіденційної інформації надано право самим

включати її до категорії конфіденційної, визначати режим доступу до неї і встановлювати систему її захисту.

Враховуючи, що перелік відомостей, які становлять комерційну таємницю, визначається керівником підприємства (банку), необхідно пам’ятати, що, згідно з Постановою Кабінету Міністрів України № 611 від 9 серпня 1993 р., не можуть бути комерційною таємницею:

– установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;

– інформація за всіма встановленими формами державної звітності;

– дані, необхідні для перевірки, обчислення і сплати податків та інших обов'язкових платежів;

– інформація про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, що є суб'єктами підприємництва;

– документи про платоспроможність;

– інформація про забруднення навколишнього природного середовища, невиконання умов безпеки праці, реалізацію продукції, яка завдала шкоди здоров'ю, а також інші порушення законодавства України і розміри завданих при цьому збитків;

– відомості, які, відповідно до чинного законодавства, підлягають оголошенню.

Відповідно до чинного законодавства, за посягання на комерційну та банківську таємниці може наставати кримінальна, цивільна, адміністративна або дисциплінарна відповідальність.

Кримінальна відповідальність може настати за дії, передбачені ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю» і ст. 232 «Розголошення комерційної таємниці» Кримінального кодексу України.

Під **незаконним збиранням** з метою використання або використання відомостей, що становлять комерційну таємницю, розуміють

умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності. Такі дії караються штрафом від 200 до 1000 неоподатковуваних мінімумів доходів громадян, або обмеженням волі на термін до п'яти років, або позбавленням волі на термін до трьох років.

Статтею передбачена відповідальність за такі злочини:

– незаконне збирання з метою використання відомостей, що становлять комерційну таємницю;

– незаконне використання відомостей, що становлять комерційну таємницю, якщо це завдало великої матеріальної шкоди суб'єкту підприємницької діяльності.

Незаконним збиранням відомостей можуть бути активні дії, спрямовані на добування таких відомостей у будь-який спосіб: вилучення, незаконне ознайомлення, прослуховування телефонних розмов, опитування співробітників, одержання відомостей за плату або через погрози, насильство тощо.

Під **незаконним використанням відомостей**, що становлять комерційну таємницю, слід розуміти впровадження чужих таємниць у власне виробництво, урахування здобутих відомостей під час планування власної діяльності, продажу, розголошення відомостей тощо.

Обов'язковою ознакою незаконного використання комерційної таємниці є наслідки у вигляді істотної матеріальної шкоди. Оскільки кримінальне покарання настає за незаконне збирання і незаконне використання відомостей, що становлять комерційну таємницю, необхідно визначити критерії законності чи незаконності такого збору. Критеріями законного отримання інформації можуть бути:

– наявність підстав для збирання і використання відомостей, передбачених законом чи договором;

– наявність необхідних повноважень;

– наявність згоди власника таємниці на ознайомлення з нею відповідних осіб.

Умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, карається штрафом від 200 до 500 неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатись певною діяльністю на термін до трьох років, або виправними роботами на термін до двох років, або позбавленням волі на той самий термін.

Кримінальній відповідальності за незаконне розголошення комерційної таємниці підлягають лише особи, яким відомості, що становлять комерційну таємницю, стали відомі у зв'язку з їхньою професійною чи службовою діяльністю і які юридично зобов'язані зберігати ці відомості.

Способи розголошення можуть бути різні: повідомлення іншим особам, надання їм для ознайомлення документів, повідомлення закритих відомостей у засобах масової інформації.

Суб'єктом злочину можуть бути працівники банку, яким комерційна таємниця відома у зв'язку із їхньою професійною або службовою діяльністю, а також посадові особи і співробітники правоохоронних органів, органів податкової служби, які у зв'язку зі своїм посадовим становищем чи особливостями професійної діяльності отримують інформацію, що становить комерційну таємницю.

Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, якщо це призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, розповсюдження комп'ютерного вірусу через застосування програмних і технічних засобів, призначених для

незаконного проникнення в ці машини, системи чи комп'ютерні мережі, є злочином і карається у порядку, передбаченому кримінальним законодавством. До цього виду злочинів належать і викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем, а також порушення правил експлуатації, автоматизованих електронно-обчислювальних систем чи комп'ютерних мереж, коли це спричинило викрадення, перекручення чи знищення комп'ютерної інформації. За перелічені дії відповідальність настає згідно зі ст. 361, 362, 363 Кримінального кодексу України.

Цивільна відповідальність ґрунтується на цивільно-правових відносинах, за яких одна сторона зобов'язана відшкодовувати другій збитки, завдані протиправними діями у зв'язку з посяганням на комерційну (банківську) таємницю.

Згідно з Цивільним кодексом України, збитки — це всі витрати, зроблені кредитором, втрата або пошкодження його майна, у разі порушення умов договорів, також стягнення збитків при виникненні зобов'язань із заподіяння шкоди.

Шкода як збитки, заподіяні протиправним посяганням на комерційну (банківську) таємницю, має місце в обох випадках, але правова природа їх відшкодування залежатиме від виду зобов'язань.

У першому випадку збитки, заподіяні протиправним посяганням на комерційну (банківську) таємницю, відшкодовуються винною стороною згідно із передбаченими угодою (договором) зобов'язаннями.

У другому випадку відшкодування збитків здійснюється не за угодою чи договором, а на загальних підставах і принципах відповідальності за заподіяння шкоди. В основі таких зобов'язань лежить не порушення умов угоди (договору), а факт заподіяння шкоди. При цьому відшкодування збитків здійснюється через подання цивільного позову до суду.

Адміністративна відповідальність за посягання на таємниці банку ґрунтується на положеннях Кодексу України про адміністративні правопорушення. Оскільки посягання на таємниці підприємства, фірми, банку законодавством України віднесено до дій, які кваліфікуються як недобросовісна конкуренція, адміністративну відповідальність за такі дії передбачено у ст. 164.3 Кодексу України про адміністративні правопорушення. Згідно із вказаною статтею, отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця тягне за собою накладення штрафу від 9 до 18 неоподатковуваних мінімумів доходів громадян.

Крім того, законодавець передбачив адміністративну відповідальність за посягання безпосередньо на банківську таємницю. Так, згідно зі ст. 164.11 Кодексу України про адміністративні правопорушення, незаконне розголошення або використання інформації, що становить банківську таємницю, особою, якій ця інформація стала відома у зв'язку з виконанням професійних чи службових обов'язків, тягне за собою накладення штрафу від 100 до 200 неоподатковуваних мінімумів доходів громадян.

Дисциплінарна відповідальність за посягання на таємниці банку ґрунтується на положеннях трудового законодавства України та нормативної бази самих банків. Слід зазначити, що в останньому випадку відповідальність можуть нести тільки працівники банку.

Банківські установи повинні впроваджувати, підтримувати та покращувати систему управління інформаційною безпекою відповідно до вимог міжнародного стандарту ISO 27001, а персонал дотримуватись законодавчих вимог та внутрішніх вимог щодо забезпечення інформаційної безпеки.

Відповідно до пункту 1 статті 1076 Цивільного кодексу України, відомості, що складають банківську таємницю, можуть бути надані банком

органам державної влади та їх посадовим особам виключно у випадках та в порядку, встановлених законом України «Про банки і банківську діяльність».

Стаття 62 (Порядок розкриття банківської таємниці) Закону України «Про банки і банківську діяльність» передбачає декілька випадків розкриття банками інформації, що становить банківську таємницю, у повному обсязі, а саме:

1) на письмовий запит або з письмового дозволу власника такої інформації;

2) на письмову вимогу суду або за рішенням суду;

3) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;

4) органам Державної податкової служби України на їх письмову вимогу з питань оподаткування або валютного контролю стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу.

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:

1) бути викладена на бланку державного органу встановленої форми;

2) бути надана за підписом керівника державного органу, скріпленого гербовою печаткою;

3) містити передбачені цим Законом підстави для отримання цієї інформації;

4) містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

До форм державної звітності відносять лише форми, установлені (затверджені) Міністерством статистики України. Під документами про

платоспроможність і даними, що необхідні для перевірки обчислення податків, не можна розуміти документи і відомості про операції клієнтів банку, оскільки вони, згідно з Законом України «Про банки і банківську діяльність», належать до банківської таємниці. Як відомо, у разі розходження у правових нормах повинен діяти принцип верховенства закону над підзаконним актом.

Банківські установи повинні впроваджувати, підтримувати та покращувати систему управління інформаційною безпекою відповідно до вимог міжнародного стандарту ISO 27001, а персонал дотримуватись законодавчих вимог та внутрішніх вимог щодо забезпечення інформаційної безпеки.

Злочини передбачені сферою використання комп'ютерів, систем та комп'ютерних мереж

Кримінально-процесуальним кодексом України передбачені покарання:

Стаття 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж:

1. Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин їх, систем чи комп'ютерних мереж що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, – караються штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років або обмеженням волі на тій самий термін.

2. Ті самі дії, якщо заподіяли істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб, – караються обмеженням волі на

термін до п'яти років або позбавленням волі на термін від трьох до п'яти років.

Стаття 362. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем:

1. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовою персоною своїм службовим становищем – караються штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, – караються штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на термін до трьох років, або позбавленням волі на тій самий термін.

3. Дії, передбачені частинами першою або іншою цієї статті якщо заподіяли істотну шкоду, – караються позбавленням волі на термін від двох до п'яти років.

Стаття 363. Порушення правив експлуатації автоматизованих електронно-обчислювальних систем:

1. Порушення правив експлуатації в автоматизованих електронно-обчислювальних машин їх систем чи комп'ютерних систем персоною, яка відповідає за їх, експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин їх систем чи комп'ютерних мереж, – карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або позбавленням обіймати певні посади чи займатися певною діяльністю на термін до п'яти років, або виправними роботами на термін до двох років.

2. Ті саме діяння, якщо воно заподіяло істотну шкоду, – карається штрафом до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років, або обмеженням волі на термін до п'яти років, із позбавленням обіймати певні посади чи займатися певною діяльністю на термін до трьох років або без такого.

Стаття 176. Порушення авторського права і суміжних прав:

1. Незаконне відтворення, розповсюдження творів науки літератури, мистецтва, комп'ютерних програм і баз даних, а так саме незаконне відтворення, розповсюдження виконань, фонограм і програм мовлення їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах інших носіях інформації, а також інше використання чужих творів, комп'ютерних програм і баз даних об'єктів суміжних має рацію без дозволу осіб, які мають авторське право або суміжні, якщо ці дії завдали матеріальної шкоди у великому розмірі, – караються штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років, з конфіскацією всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм програм мовлення та обладнання і матеріалів, призначених для їх виготовлення й відтворення.

2. Ті самі дії, якщо вчинені повторно або завдали матеріальної шкоди в особливо великому розмірі, – караються штрафом від двохсот до восьмисот неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років, або позбавленням волі на тій самий термін, із конфіскацією всіх примірників, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, програм мовлення, аудіо- та відеокасет, дискет інших носіїв інформації та обладнання і матеріалів, призначених для їх виготовлення й відтворення.

3. Дії, передбачені частинами першою або іншою цієї статті учинені службовою персоною з використанням службового становища щодо підлеглої особини, – громадян.

Стаття 200. Незаконні дії з документами на переказ платіжними картками та іншими засобами доступу до банківських рахунків обладнанням для їх виготовлення:

1. Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так саме придбання зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток або їх використання чи збут – карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на термін до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, – караються позбавленням волі на термін від двох до п'яти років.

Примітка. Під документами на переказ слід розуміти документ у паперовому або електронному виді, що використовується банками чи їх, клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів.

РОЗДІЛ 3. РИЗИКИ КІБЕРБЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

Загрози інформаційної безпеки банківської установи. Класифікація загроз

Під **загрозою** розуміється потенційно можлива подія, дія, процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам. Загроза проявляються через низький захист або знаходження вразливих місць у системі захисту інформаційних систем.

Основними завданнями системи інформаційної безпеки є:

– виявлення та усунення загроз безпеки нанесенню економічного, фінансового, матеріального та морального збитку;

– створення механізмів реагування на загрози розвитку і функціонуванню підприємства та національній безпеці;

– прийняття заходів щодо забезпечення безпеки персоналу підприємства та інше.

В інформаційних взаємовідносинах банків можуть виникати два види загроз: загрози, пов’язані з посяганням на їх інформаційні ресурси (які має обмежений доступ) – **загрози інформації** та загрози, що виникають під час формування інформаційного середовища (умов) діяльності таких суб’єктів – **інформаційні загрози**.

Інформаційні загрози можуть бути обумовлені:

– природними факторами;

– людськими факторами.

До природніх факторів відносяться такі джерел загроз, які об'єднують обставини, що становлять непереборну силу. До непереборної сили відносять стихійні лиха або інші обставини, що неможливо передбачити або запобігти, або можливо

передбачити, але неможливо запобігти при сучасному рівні людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до тих, що захищаються і під ними розуміються насамперед природні катаклізми (пожежі, землетруси, повені, урагани та інші форс-мажорні обставини).

До людських факторів відносяться:

– загрози випадкового характеру (помилки обробки, передачі, обміну інформації);

– загрози навмисного характеру (несанкціонований доступ до інформації).

Навмисні загрози призводять до шкідливих наслідків користувачам автоматизованих інформаційних систем і можуть бути *активні* і *пасивні*.

Пасивні загрози спрямовані на несанкціоноване використання інформаційних ресурсів і не впливають на функціонування системи.

Активні загрози спрямовані на порушення нормального процесу функціонування системи через вплив на апаратні, програмні та інформаційні ресурси. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і т.п.

Розглядаючи загрози банківській інформації, найбільш поширеними з них можна вважати:

Розголошення банківської інформації – це протиправні умисні чи необережні дії посадових чи інших осіб, які призвели до несанкціонованого, без службової необхідності оголошення відомостей, щодо яких установлений певний порядок їх розкриття.

Викраденням інформації є таємне вилучення носіїв інформації з метою подальшого їх використання іншою особою чи передання їх такій особі.

Знищенням є приведення носіїв інформації до стану, непридатного для їх подальшого використання, або ж до неможливості використання інформації, яка на них зберігалась.

Модифікацією інформації є внесення змін до змісту інформації, яка містилася на певних носіях, або ж до самих носіїв, у результаті чого використання даної інформації стає неможливим взагалі чи така інформація потребує суттєвого уточнення та аналізу.

Незаконне використання інформації означає використання певних даних, знань, технологій, які на праві власності на лежать певній юридичній чи фізичній особі, без її згоди або з порушенням установленого порядку їх використання особами, яким така інформація відома у зв'язку з їхнього службовою чи іншою діяльністю.

Несанкціонованим буде також доступ до інформації з порушенням установлених правил доступу до неї.

Загрози інформаційної безпеки класифіковані за різними ознаками.

1. За аспектом інформаційної безпеки, на який спрямовані загрози.

– *Загрози конфіденційності* – полягає в тому, що інформація стає відомою тому, хто не має повноважень доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в обчислювальній системі чи переданої від однієї системи до іншої. До загрози порушення конфіденційності, використовується термін «витік». Подібні загрози виникають внаслідок «людського фактору», збоїв в роботі програмних і апаратних засобів.

– *Загрози цілісності* – загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними факторами – від навмисних дій персоналу до виходу з ладу обладнання.

– *Загрози доступності* – створення умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

Найбільш небезпечними загрозами є порушення конфіденційності інформації та витік інформації, оскільки банки побоюються цього з двох причин. По-перше, кожен витік конфіденційної інформації та персональних даних банку підриває його репутацію, так як в очах його партнерів, інвесторів і клієнтів банк набуває імідж організації, яка не в змозі навести порядок в своїх власних стінах. По-друге, інциденти такого роду можуть призвести до втрати конкурентоздатності банку, через витік клієнтської бази банківської установи.

2. За розташуванням джерела загроз:

– *внутрішні* – джерела загроз розташовуються всередині системи(виток інформації, неавторизований доступ);

– *зовнішні* – джерела загроз знаходяться поза системою(шкідливі програми, атаки хакерів, Ddos-атаки, таргінг атаки, спам, фішинг, промислові загрози, шпигунське програмне забезпечення, botnets).

3. За розмірами завдання шкоди:

– *загальні* – нанесення збитку об’єкту безпеки в цілому, заподіяння значної шкоди;

– *локальні* – заподіяння шкоди окремим частинам об’єкта безпеки;

– *приватні* – заподіяння шкоди окремим властивостям елементів об’єкта безпеки.

4. За ступенем впливу на інформаційну систему:

– *пасивні* – структура і зміст системи не змінюються;

– *активні* – структура і зміст системи піддається змінам.

5. За природою виникнення:

– *природні* (об’єктивні) – викликані впливом на інформаційне середовище об’єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини;

– *штучні* (суб'єктивні) – викликані впливом на інформаційну сферу людини.

Серед штучних загроз в свою чергу виділяють:

– *ненавмисні* (випадкові) загрози – помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної і комунікаційної техніки;

– *навмисні* (умисні) загрози – неправомірний доступ до інформації, розробка спеціального програмного забезпечення, що використовується для здійснення незаконного втручання, розробка та поширення вірусних програм і т.і. Навмисні загрози обумовлені діями людей.

Особливу увагу слід звернути на людські джерела загроз, які можуть мати різну мотивацію – від політичних причин до простого самоствердження. Найбільш ймовірними та найбільш серйозними можна вважати загрози від власних працівників банку, в тому числі ті загрози, які можуть виникати від недостатньої обізнаності персоналу в питаннях інформаційної безпеки.

Варто також звернути увагу на загрози, пов'язані з глобалізацією інформаційних і телекомунікаційних технологій. У зв'язку з процесом міжнародної інтеграції та глобалізації обсяги та різноманітність загроз значно розширилися. Банки можуть зазнавати інформаційного удару щодо своїх інформаційних та фінансових ресурсів із глобального інформаційного простору. Серед найпоширеніших глобальних загроз – комп'ютерний тероризм і комп'ютерне хуліганство. Значне поширення Інтернет-технологій і відносна анонімність користувачів спровокували появу так званих хакерів, крекерів та ін. Вони є катастрофічно небезпечними для банківських комп'ютерних технологій, оскільки не тільки руйнують системи їх захисту, а можуть отримати досить важливу банківську інформацію з метою її знищення або передавання конкурентам банку.

Загрози інформаційним ресурсам банківської установи можуть бути реалізовані шляхом:

– підкупу осіб, які мають безпосередній доступ до банківської таємниці та іншої інформації з обмеженим доступом банківської установи;

– необережного, недбалого поводження з банківською таємницею та іншою інформацією з обмеженим доступом;

– недотримання вимог збереження інформації з обмеженим доступом, встановлених у банківській установі, при контактах з контролюючими і наглядовими органами внаслідок правової та психологічної непідготовленості відповідальних працівників банківської установи тощо.

У реалізації загроз банківській інформації важливе місце займають канали її витоку, до яких можна віднести: візуально-оптичні, акустичні та акустично-перероблювальні, електромагнітні, матеріально-речові.

Протидія переліченим загрозам має полягати, насамперед, у:

– визначенні надійності працівників підприємства, які працюватимуть з банківською таємницею та іншою інформацією з обмеженим доступом;

– організації спеціального діловодства з відомостями, що становлять та інформацію з обмеженим доступом банківської установи;

– обґрунтуванні і закріпленні диференційованого доступу працівників до банківської таємниці та іншої інформації з обмеженим доступом, при якому працівник може ознайомлюватися і вчиняти певні дії з нею виключно для виконання покладених на нього функціональних обов’язків;

– закріпленні персональної відповідальності працівника за збереження наданих йому або розроблених ним документів, інших носіїв інформації, що містять інформацію з обмеженим доступом банківської установи;

– обмеженні доступу працівників і сторонніх осіб до приміщень, у яких обробляється (зберігається) інформація з обмеженим доступом банківської установи;

– впровадженні заходів контролю за роботою працівників з носіями інформації з обмеженим доступом банківської установи, а також ефективної системи виявлення і фіксації протиправних діянь з такою інформацією;

– впровадженні надійної і ефективної системи зберігання носіїв інформації, що виключає несанкціоноване ознайомлення з ними, їх знищення чи підробку.

Суттєвими загрозами безпеці інформаційної інфраструктури є:

– неофіційний доступ та зняття інформації, що охороняється, технічними засобами;

– перехоплення інформації, що циркулює в засобах і системах зв'язку та обчислювальної техніки, за допомогою технічних засобів негласного зняття інформації, несанкціонованого доступу до інформації та навмисних технічних впливів на них в процесі обробки та зберігання;

– підслуховування з використанням технічних засобів конфіденційних переговорів, що ведуться в службових приміщеннях, автотранспорті тощо.

Протидія таким загрозам має полягати, передусім, у широкому і головне економічно доцільному застосуванні технічних засобів безпеки інформаційної інфраструктури.

Вразливість систем безпеки банківської установи. Класифікація вразливостей

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори вразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носії.

Вразливість інформації є одним із головних показників стану її захищеності. Тому визначення ступеня вразливості інформації у процесі організації її захисту має досить суттєве значення. Результати, отримані у процесі визначення вразливості інформації, використовуються для встановлення складу інформації, яка підлягає безпосередньому захисту тобто об'єктів захисту. Загальний підхід тут полягає у тому, що захисту, підлягає вся інформація з обмеженим доступом і найбільш важлива частина відкритої інформації. При цьому інформація з обмеженим доступом повинна захищатися від втрати і несанкціонованого витоку, а відкрита – лише від втрати.

Основні вразливості виникають внаслідок дії наступних факторів:

– недосконаліть програмного забезпечення, апаратної платформи;

– різні характеристики будови автоматизованих систем в інформаційному потоці;

– частина процесів функціонування систем є неповноцінною;

– неточність протоколів обміну інформацією та інтерфейсу;

– складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливі і випадкові загрози через недостатні міри захисту і дії масового загрозливого фактору.

Існує поділ вразливостей за класами:

– об'єктивні;

– випадкові;

– суб'єктивні.

Якщо усунути або, як мінімум, послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему зберігання інформації. Таким чином, класифікація погроз ІБ розподіляється за характером загрози, видом впливу, джерелом та об'єктом загрози.

Управління ризиками інформаційної безпеки банків

Оскільки сучасна діяльність банківських установ значною мірою перебуває в інформаційній площині, банки, як ніхто інший із суб'єктів підприємництва, є об'єктами інформаційних загроз і впливу інформаційних ризиків.

Інформаційні ризики банківської установи за своїм походженням поділяються на три категорії:

– ризики, пов'язані з втратою інформації. Особливо це небезпечно, коли існує ризик втрати такої важливої для банку і його клієнтів інформації, як банківська таємниця, або іншої інформації з обмеженим доступом;

– ризики, пов'язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація);

– ризики, пов'язані з інформаційним впливом на діяльність банків (поширення неправдивої та негативної для банків інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів банків, інформаційний тероризм).

Пошук заходів з попередження збитку, заподіяного від реалізації інформаційних загроз, може бути забезпечено через **систему управління інформаційними ризиками**. Данна система має забезпечувати не лише надійний захист інформаційних ресурсів, а й сприяти ідентифікації інформаційних ризиків, виявленню факторів та умов їх появи й забезпечувати їх мінімізацію у процесі діяльності банківської установи.

Враховуючи значну роль інформації у діяльності банків, система управління інформаційними ризиками має включати певні підсистеми:

– підсистему захисту інформації;

– підсистему збирання інформації та інформаційних досліджень;

– підсистему протидії інформаційному впливу;

– управляючу підсистему.

Основними завданнями підсистеми захисту інформації банку мають бути: виявлення інформації, що підлягає захисту, визначення місць зосередження та носіїв інформації, яка підлягає захисту, визначення можливих способів несанкціонованого доступу до такої інформації, розроблення й упровадження організаційних, правових, технічних, програмних, криптографічних та апаратних заходів захисту інформації.

З огляду на те, що в банках зосереджено доволі значні обсяги інформації з обмеженим доступом, та те, що банки є єдиними серед суб'єктів підприємницької діяльності, на кого в законодавчому порядку покладено захист чужих таємниць, питання аналізу, контролю та мінімізації втрати інформації для банків є доволі важливими.

Питання мінімізації ризику втрати інформації є доволі серйозним для банків, однак як банки не намагалися виключити ризик втрати інформації, зробити це майже неможливо. Керівництво банків повинно бути орієнтовано на певний ризик втрати інформації, щоб виникнення якоїсь непередбачуваної ситуації не стало проблемою, яку неможливо вирішити. У цьому випадку банки завжди передбачатимуть дії на випадок втрати інформації, розраховувати свої можливості щодо ліквідації наслідків і бути готовими до неадекватного розвитку ситуації в інформаційних взаємовідносинах зі своїми клієнтами, акціонерами, партнерами та іншими суб'єктами.

Також для мінімізації ризику втрати інформації банки мають вживати відповідних заходів, поділяючи їх відповідно до певних загроз. Серед таких заходів насамперед мають бути: формування правових умов захисту інформації безпосередньо у банку. Під такими умовами слід розуміти розроблення нормативно-правових документів банку стосовно захисту всіх видів інформації (документованої, електронної, знань працівників банку). Зазначеними документами мають регулюватися взаємовідносини банку з його працівниками, клієнтами, партнерами,

іншими створення системи захисту інформації, яка функціонує в банківській інформаційній мережі.

Функціями цієї системи повинно бути:

– передбачати комплекс організаційних, технічних, апаратних, криптографічних заходів і забезпечувати гарантований захист від посягань на електронну інформацію банку;

– забезпечення контролю за носіями інформації, своєчасне реагування на всі збої в захисті інформації, що зберігається та функціонує в інформаційних мережах банку;

– запровадження надійної системи документообігу в банку;

– забезпечення надійної охорони банків, особливо з точки зору виключення можливості несанкціонованого доступу до них та їх винесення документів чи електронних носіїв інформації.

Отже, управління інформаційними ризиками з позиції мінімізації загроз утрати інформації в банку є доволі трудомістким і багатогранним процесом, який охоплює різні види організаційної, правової, інженерно-технічної, кадрової та безпосередньо інформаційної роботи. Цей процес, як бачимо, пов’язано з іншими системами (підсистемами), які можуть бути у складі системи управління інформаційною безпекою банківської установи.

Відповідно до стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 після виконання оцінювання ризиків банк має оцінити альтернативні варіанти оброблення ризиків. Можливими варіантами оброблення ризиків можуть бути:

– зниження ризиків шляхом застосування належних заходів безпеки;

– свідоме та об’єктивне прийняття ризиків за умови, що вони чітко задовольняють політику організації та критерії прийняття ризиків;

– уникнення ризиків;

– перенесення відповідних бізнес-ризиків на інші сторони.

Для прийняття рішення щодо оброблення конкретних ризиків рекомендується визначити такі критерії стосовно кожного окремого ризику:

– низький ризик – 1-6;

– середній ризик – 7-14;

– високий ризик – 15-25.

Застосування належних заходів безпеки дасть змогу зменшити ризики.

Відповідно до Методичних рекомендацій щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків за стандартами Національного банку України **система управління ризиками банківської діяльності повинна будуватися на основі міжнародного стандарту ISO/IEC 27005 —Information technology – Security techniques – Information security risk management** (Управління ризиками інформаційної безпеки) з урахуванням особливостей діяльності банків України, стандартів і вимог Національного банку України з питань інформаційної безпеки.

Відповідно до Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженим постановою правління Національного банку України від 28.09.2017 № 95, банки зобов’язані:

– запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку. При цьому банк має право самостійно визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки;

– запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов’язкових вимог щодо організації заходів безпеки інформації, викладених у Положенні.

Процес управління ризиками інформаційної безпеки повинен здійснюватися для банку в цілому і зокрема включати:

– аналіз та ідентифікацію ризиків;

– оцінювання ризиків з точки зору їх впливу на бізнес та ймовірності їх появи;

– інформування особи, яка вправі приймати рішення та акціонерів банку про ймовірності та впливи цих ризиків;

– встановлення порядку та пріоритетів оброблення ризиків;

– становлення пріоритетів виконання дій щодо зниження ризиків;

– участь керівництва в процесі прийняття рішень щодо управління ризиками та його поінформованість щодо стану справ в управлінні ризиками;

– ефективний моніторинг та регулярний перегляд ризиків і процесу управління ризиками;

– інформування керівництва та персоналу щодо ризиків і дій щодо управління ними.

Аналіз ризиків передбачає їх визначення та оцінювання. Під час визначення ризиків установлюють, які саме інформаційні ризики можуть існувати чи існують в діяльності банку або в процесі проведення ним конкретної комерційної (банківської) операції, як вони можуть вплинути на діяльність чи операцію та яка існує ймовірність настання негативних наслідків від дії ризику.

Оцінювання інформаційного ризику передбачає визначення обсягу збитку, який може зазнати суб’єкт унаслідок вияву зазначеного ризику.

Сьогодні можна чітко виділити **дві основні групи методів оцінювання ризиків інформаційної безпеки**:

– *перша група* методів дає можливість встановити рівень ризику шляхом оцінювання ступеню відповідності визначеному набору вимог щодо забезпечення інформаційної безпеки;

– *друга група* методів оцінювання ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів збитку, завданих ними.

Методи першої і другої групи відрізняються застосуванням різних шкал для визначення величини ризику. У першому випадку ризик і усі його параметри виражаються в **кількісних значеннях**, у другому випадку використовуються **якісні шкали**.

Якісне оцінювання часто використовується спочатку для визначення загального рівня ризику і визначення основних ризиків. Далі може виникнути необхідність виконання більш специфічного або кількісного аналізу стосовно основних ризиків. **Кількісне оцінювання** ризиків є більш складним та потребує більше часу та ресурсів. Однак таке оцінювання буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Для виконання оцінки ризиків необхідно визначити шкалу для різних параметрів:

– оцінки величини наслідків реалізації загрози на сервіси безпеки (цілісність, конфіденційність, доступність, спостережність),

– оцінки ймовірності реалізації загрози.

Загальний рівень оцінки величини наслідків реалізації кожної загрози на сервіси безпеки визначається як максимальна величина з окремих оцінок впливу на цілісність, конфіденційність, доступність, спостережність.

Рівень ризику за окремою парою загроза/вразливість, яка може використовуватися для реалізації цієї загрози, визначається перемноженням загального рівня оцінки величини наслідків на оцінку ймовірності реалізації загрози.

Загальний рівень ризику для бізнес-процесу/банківського продукту, персоналу, фізичного середовища тощо дорівнює максимальної величині з усіх ризиків за кожною парою загроза/вразливість.

Процес управління ризиками інформаційної безпеки у банку є безперервним процесом і до нього може бути застосована модель ПВПД (плануй – виконуй – перевіряй – дій), наведена у вступі стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010.

Таким чином, одним із важливих аспектів під час формування системи інформаційної безпеки в банках є побудова системи управління ризиками банківської діяльності.

РОЗДІЛ 4. ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ

Нормативні документи захисту персональних даних даних

В Україні розроблено і впроваджено наступні законодавчі та нормативні документи щодо захисту інформації, технічного захисту інформації, захисту персональних даних, електронного цифрового підпису, технічного захисту інформації:

– Закон України «Про захист персональних даних»;

– Закон України «Про інформацію»;

– Закон України «Про доступ до публічної інформації»;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Закон України «Про телекомунікації»;

– Закон України «Про ліцензування видів господарської діяльності»;

– Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 №1126;

– Постанова Кабінету Міністрів України від 25.05.2011 №616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення»;

– Постанова Кабінету Міністрів України від 29.10.00 №1755 «Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу».

– Постанова Кабінету Міністрів України від 16.11.2016 №821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України».

– Постанова Кабінету Міністрів України від 21.06.17 №437 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від

провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації».

– Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 №1229.

– Постанова Кабінету Міністрів України від 13.03.02 №281 «Про деякі питання захисту інформації, охорона якої забезпечується державою».

– Постанова Кабінету Міністрів України від 29.03.06 №373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

– Постанова Кабінету Міністрів України від 12.04.02 №522 «Порядок підключення до глобальних мереж передачі даних».

– Положення про порядок надання відомостей з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців, затверджено Наказом Державного комітету України з питань регуляторної політики та підприємництва 20.10.2005 №97, Зареєстровано в Міністерстві юстиції України 28 жовтня 2005 р. за №1294/11574.

– Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 №93, зареєстровано в Міністерстві юстиції України 16.07.07 за №820/14087.

– Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 №87, зареєстровано в Міністерстві юстиції України 10.07.07 за №785/14052.

– Правила проведення робіт із сертифікації засобів захисту інформації, затверджені наказом Держспоживстандарту та Адміністрації Держспецзв'язку від 25.04.07 №75/91 та зареєстровані у Мін`юсті 14.05.07 №498/13765.

– Порядок формування реєстру організаторів державної експертизи у сфері технічного захисту інформації та реєстру експертів з питань технічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.04.08 №64.

– Порядок оновлення антивірусних програмних засобів, що мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 26.03.07 №45.

– Тимчасове положення про категоріювання об'єктів від 10.07.95 №35.

– ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

– ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

– ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

– НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

– НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

– НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації захисту інформації в комп'ютерних системах від несанкціонованого доступу.

– НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

– НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

– НД ТЗІ 2.5-010-2003 Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу.

– НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

– НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі зміною №1, затвердженою наказом ДСТСЗІ СБ України 18.06.02 №37).

– НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

– НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

– НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

– НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації.

– НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

В **законі України “Про інформацію”** від 02.10.92 р. № 2657-XII (остання редакція від 21.12.2019) визначаються основні терміни та положення про інформацію, який регулює відносини щодо створення, збирання, отримання, зберігання, використання, поширення, охорони, захисту інформації.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" №80/94-ВР від 05.07.1994 р., чинний (остання редакція від 19.04.2014). Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Державні органи в межах своїх повноважень за погодженням відповідно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації або підпорядкованим йому регіональним органом, встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

За законом особливості захисту інформації в системах, що забезпечують банківську діяльність, встановлюються Національним банком України.

Державний стандарт України ДСТУ 3396.0-96 чинний від 01.01.1997 р. включає: захист інформації, технічний захист інформації, основні положення.

Цей стандарт встановлює об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ),

неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Закон України Про криптографічний та технічний захист інформації. Цей Закон визначає правові та організаційні засади криптографічного та технічного захисту важливої для держави, суспільства і особи інформації, що обробляється або озвучується на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, охорона якої забезпечується державою відповідно до законодавства, регулює відносини між суб'єктами у цій сфері.

Поняття конфіденційності персональних даних

Необхідність забезпечення безпеки персональних даних в наш час – об'єктивна реальність. Сучасна людина не може самостійно протидіяти посяганню на його приватне життя. Підвищені технічні можливості щодо збору та обробки персональної інформації, розвиток засобів електронної комерції і соціальних мереж роблять необхідним вжиття заходів щодо захисту персональних даних.

Держава на законодавчому рівні вимагає від організацій та фізичних осіб, які обробляють персональні дані, забезпечити їх захист. Законодавство України в області захисту персональних даних ґрунтується на Конституції України, міжнародних договорах України, Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та інших нормативних документах.

Метою Українського законодавства у сфері захисту персональних даних є забезпечення захисту прав і свобод громадянина при обробці його персональних даних, в тому числі захисту прав на недоторканність приватного життя, особисту і сімейну таємницю. Законодавством регулюються відносини, пов'язані з обробкою персональних даних, що здійснюється державними органами влади, органами місцевого самоврядування, юридичними особами та фізичними особами.

Відповідно до Закону, персональні дані – будь-яка інформація, за допомогою якої можна однозначно ідентифікувати фізичну особу. До персональних даних відносяться: прізвище, ім'я, по батькові; рік, місяць, дата і місце народження; адреса; сімейний, соціальний, майновий стан; освіта, професія, доходи, інша інформація, що належить суб'єкту.

Операторами персональних даних є державний орган, юридична або фізична особа, які організують і (або) здійснюють обробку персональних даних, а також визначають цілі і зміст обробки персональних даних.

Обробка персональних даних – дії (операції) з персональними даними, включаючи збір, систематизацію, накопичення, зберігання, уточнення, використання, поширення, знеособлення, блокування, знищення персональних даних.

Інформаційна система персональних даних (далі ІСПД) – інформаційна система, що представляє собою сукупність персональних даних, що містяться в базі даних, а також інформаційних технологіях і технічних засобах, що дозволяють здійснювати обробку таких персональних даних з використанням засобів автоматизації або без використання таких засобів.

Регуляторами називаються органи державної влади, уповноважені здійснювати заходи щодо контролю і нагляду щодо дотримання вимог закону України «Про захист персональних даних».

Україна в питанні захисту персональних даних спирається на міжнародний досвід. Але в державі поки немає достатньої законодавчої бази і системи, здатної ефективно працювати в сучасних умовах.

Захист персональних даних

Проблема захисту персональних даних з кожним роком стає все більш актуальним не лише в Україні, а й в усьому світі. Із стрімким розвитком сучасних інформаційних технологій, ідентифікація фізичної особини є необхідною до надання багатьох послуг: надання кредитів, виплата допомоги, оплата комунальних послуг, робота з банківськими установами, оплата товару через інтернет тощо. Оскільки більшість подібних послуг надається через мережу та видалений доступ і без особистої присутності, можна із упевненістю сказати, що вимоги до захисту та безпеки персональних даних мають бути більш жорсткими.

Розглядаючи поняття персональні дані, необхідно сказати, що це інформація, що здатна ідентифікувати особу. Такими даними є: прізвище, ім'я, по батькові; дата, рік, місяць, місце народження; адреса реєстрації або прописки; номер паспорта і картки соціального страхування; відомості про соціальний та сімейний стан; власність на майно, освіта, професія, доходи.

Останнім часом з'явилося багато інших персональних даних: номера кредитних і дебетових банківських карт, PIN-коди, логіни та паролі від різних сервісів (наприклад, особистої пошти), дані GPS-приймача зі смартфону, що дозволяють відстежити переміщення користувача та інше.

Для боротьби із шахрайством в багатьох країнах на законодавчому рівні розроблялися нові вимоги безпеки до компаній, що працюють з персональними даними. Цей процес носить постійний характер, оскільки інформаційні технології розвиваються і, разом з ними, з'являються все нові вимоги щодо забезпечення безпеки інформації. З іншого боку, такий розвиток штовхає злочинців на винахід нових методів розкрадання даних.

Оскільки Україна підтримує курс європейського розвитку, розглянемо розвиток системи захисту персональної інформації в ЄС. Європейське законодавство вже більше двох десятиліть удосконалює систему захисту персональних даних. В 1995 році на території Європи введена директива, що зобов'язує країни, які входять до складу ЄС, забезпечити захист персональних даних громадян. Кожна європейська країна ухвалила свої закони про захист персональних даних, що найчастіше не збігалися із законами інших країн ЄС. Багато міжнародних компаній, що передають дані через кордон, стали зазнавати великі труднощі, що пов'язані з дотриманням законів різних країн. Саме тому в 2012 році було вирішено створити загальний регламент по захисту персональних даних на території ЄС (General Data Protection Regulation – **GDPR**), що прийшов на зміну існуючої колись директиви.

Після декількох років переговорів регламент було затверджено 25 травня 2016 року. У травні 2018 року набуло чинності нове положення про захист даних. У числі нововведень — заборона на збір персональних даних компаніями і державою без дозволу з боку фізичної особи. Виключення допускаються тільки в тому випадку, якщо в країні існують законодавчі акти, що зобов’язують до передачі інформації.

Протягом двох років, до 25 травня 2018 року, усі компанії, що зберігають, передають і обробляють особисті дані європейців, зобов'язані були забезпечити безпеку таких даних відповідно до положень GPDR. Варто відзначити, що це також стосується компаній, що перебувають за межами країн ЄС, що працюють із персональними даними громадян європейських країн (наприклад, України).

Також важливим для держав Європейського союзу є те, що підтверджувати дозвіл на обробку персональних даних можна не з 13 років, а лише з 16 років. На компанії з європейськими представництвами накладається ряд обмежень. Їм неможна виконувати обмін даними з

іншими підрозділами, якщо не виконуються правила по захисту даних. Також неможна передавати інформацію владі США та іншим країнам.

Слід зазначити, що в ЄС новий GPDR регламент привів до масового переходу інформаційних структур європейських підприємств у хмарні сховища. Щоб краще зрозуміти причини такої масової міграції, необхідно знати, що в GPDR усі підприємства діляться на дві основні категорії:

– **контролери даних** – це підприємства, діяльність яких містить у собі збір персональних даних, їх передачу, а також роботу з ними. Основні вимоги до таких компаній полягають у дотриманні правил, що стосуються згоди громадян на зберігання, обробку і передачу їх персональних даних;

– **оброблювачі даних** – це підприємства, що зберігають персональні дані безпосередньо на своїх серверах. Такі компанії зобов'язані забезпечити високий рівень інформаційної безпеки даних – від обмеження фізичного доступу до обладнання, де зберігається інформація, до жорстких вимог їх резервного копіювання та налагодження брандмауерів. Забезпечення цих стандартів – складний і коштовний процес.

Для багатьох компаній витрати на відповідність вимогам GDPR у якості оброблювача даних є дуже великими, тому більшість європейських підприємств переводять свої інформаційні системи в хмарні сховища.

Захист персональних даних українців знаходиться на критично низькому рівні. Лише у 2011 році в Україні набув чинності Закон України «Про захист персональних даних», згідно з нормами якого фізичні і юридичні особи, органи державної влади або органи місцевого самоврядування, фізичні особи – підприємці, що обробляють персональні дані, тобто відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікованою (ст.2 Закону), повинні зареєструвати бази персональних даних у спеціальному реєстрі баз даних, роботу якого контролює Державна служба з питань захисту персональних даних.

Усі персональні дані українців, починаючи з номера мобільного телефону і закінчуючи адресою проживання, сьогодні не захищені. Характерно те, що спеціальне законодавство, розроблене в Україні для збереження й захисту персональних даних, фактично діє тільки в тому випадку, коли витік інформації походить із якихось державних установ і підприємств. Відповідальність може настати, тільки якщо власник цих даних звернувся в правоохоронні органі. Дуже небезпечна ситуація зараз існує у використанні баз персональних даних системи Мінздраву України, що легко викрасти, бо вони практично не захищені.

Проблема в Україні ще збільшується тим, що громадяни добровільно передають свої дані при одержанні різних дисконтних карт та інших випадках, не замислюючись про можливі наслідки. Будь-який витік персональних даних приносить серйозні фінансові неприємності.

За даними компанії Searchinform, провідного виробника засобів від витоків даних у СНД, – більше 32% українських витоків інформації пов'язано з персональними даними. Проконтролювати в Україні, як саме зберігаються та обробляються персональні дані, досить складно і майже не можливо.

Таким чином, система захисту персональних даних в Україні потребує державного моніторингу та реформування на законодавчому рівні. В умовах неухильно зростаючого рівня кіберзлочинності у світі та низького рівня інформаційної культури громадян, а також відсутності розуміння ними всіх можливих кіберзагроз, необхідно на державному рівні забезпечити захист громадян від витоку персональних даних. Вести боротьбу з кіберзлочинністю з використанням персональних даних можна тільки на основі системного підходу на усіх рівнях.

РОЗДІЛ 5. ПОНЯТТЯ ПОЛІТИКИ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

Політика інформаційної безпеки банку

Політика інформаційної безпеки банку – сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури банку від випадкового і навмисного втручання в процес її функціонування. Політика формується на основі характеристики об'єкта застосування; аналізу поточного стану захищеності інформаційної інфраструктури банку; обліку можливих негативних факторів впливу та ймовірності їх реалізації; створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки з врахуванням вимог, що містяться в законах і нормативних актах держави, міжнародних, національних та промислових стандартах у галузі інформаційної безпеки, нормативних документах державного і відомчого характеру.

Розрізняють дві системи оцінки поточної ситуації у сфері інформаційної безпеки у банківських установах:

– «дослідження знизу догори» (прямий);

– «дослідження зверху вниз» (зворотній).

Метод «знизу догори» досить простий, потребує набагато менших капітальних вкладень, але й має менші можливості. Він базується на відомій схемі: «Ви – зловмисник. Ваші дії?» Тобто служба інформаційної безпеки банку, ґрунтуючись на даних про всі відомі види атак, намагається застосувати їх на практиці з метою перевірки, чи можлива така атака з боку реального зловмисника.

Метод «зверху вниз» є, детальним аналізом усієї наявної схеми зберігання та обробки інформації. Першим етапом цього методу є

визначення, які інформаційні об’єкти і потоки необхідно захищати. Далі вивчають поточний стан системи інформаційної безпеки з метою визначення того, що з класичних методик захисту інформації вже реалізоване, в якому обсязі та на якому рівні. На третьому етапі розробляється класифікація всіх інформаційних об’єктів на класи відповідно до їх конфіденційності, вимог до доступності та цілісності. На четвертому етапі з’ясовують, наскільки серйозний збиток може завдати банку розкриття або інша атака на кожний конкретний інформаційний об’єкт. Цей етап носить назву «розрахунок ризиків». У першому наближенні ризиком є добуток «можливого збитку від атаки» на «ймовірність такої атаки». Є безліч схем обчислення ризиків.

Залежно від стану інформаційної безпеки в банку виділимо **чотири основні типи політики інформаційної безпеки банку**:

1. **Програмна політика безпеки** використовуються при оцінці стану інформаційної небезпеки в банку і розробляється з метою визначення напрямів реструктуризації основних компонентів забезпечення інформаційної безпеки і їх реалізації. Програмна політика безпеки банку визначає множину стратегічних напрямків забезпечення інформаційної безпеки, види і обсяг ресурсів, які виділяються для реалізації політики;

2. **Формування проблемно-орієнтованої політики інформаційної безпеки банку** здійснюють у випадку інформаційної загрози в банку. Об’єктом застосування проблемно-орієнтованої політики безпеки є окрема проблема або задача в області забезпечення безпеки інформації в фінансово-кредитній організації. Необхідність розробки проблемно-орієнтованої політики безпеки часто вимагає у відповідь як появу і використання в організації нових технологій, так і виникнення нових загроз та слабкостей. Частіше за все проблемно-орієнтована політика безпеки уточнює, конкретизує положення програмної політики безпеки чи об’єктової політики безпеки;

3. **Системно-орієнтована політика інформаційної безпеки** банку використовується при стані інформаційного ризику, визначає напрямок, методи та процедури забезпечення інформаційної безпеки. Даний тип політики обмежений областю взаємодії самої системи і середовища її експлуатації. Для розробки пов'язаного та повного набору правил безпеки розробник повинен використовувати спеціальні прийоми, за допомогою яких на основі аналізу задач захисту формулюються правила безпеки;

4. **Системна політика** містить загальні вимоги до безпеки інформації та рішення щодо забезпечення режиму інформаційної безпеки. Повинна містити правила безпеки відносно фізичної безпеки, автентифікація, ідентифікації та управління доступом, правила застосування криптографічних засобів, правила забезпечення антивірусного захисту та інші питання моніторингу актуальності сформульованих та уточнених задач захисту в процесі експлуатації системи.

Актуальність питання впровадження політики інформаційної безпеки банківських установ пов'язано з швидким розвитком засобів і форм автоматизації процесів оброблення інформації та високою залежністю банківської установи від інформаційних ресурсів та мереж. Відсутність у банківській установі правил і контролю щодо інформаційної безпеки викликає проблеми з ефективністю її функціонування. Важливим є побудова ефективної політики інформаційної безпеки, адже через недостатню увагу до інформаційної безпеки відбувається витік інформації, що в свою чергу призводить до значних фінансових збитків та втрати довіри клієнтів. Банк повинен забезпечити власну безпеку, а також безпеку своїх клієнтів. Політика інформаційної безпеки визначає стратегію і тактику побудови системи захисту інформації

Ціллю розроблення політики безпеки є забезпечення регулювання та підтримку інформаційної безпеки з боку керівництва банку згідно з вимогами бізнесу та відповідними законами і нормативами.

Відповідно до цілей бізнесу керівництво банку повинно встановити чітке регулювання політики і забезпечити підтримку та зобов'язання щодо інформаційної безпеки виданням політики інформаційної безпеки та її підтримкою в банківській установі.

Метою політики інформаційної безпеки банку має бути забезпечення надійного захисту інформаційних ресурсів банку від зовнішніх та внутрішніх загроз завдяки впровадженню та ефективному функціонуванню системи управління інформаційної безпеки банку.

Основним завданням політики інформаційної безпеки є захист інформаційних активів від загроз, а саме:

– виявлення та мінімізація потенційних загроз інформаційній безпеці;

– захист інформаційних активів організації;

– забезпечення безпеки та конфіденційності інформації про клієнтів;

– забезпечення стабільної та ефективної діяльності банківської установи.

Фахівці виокремлюють наступні напрями щодо забезпечення інформаційної безпеки в контексті впровадження політики інформаційної безпеки банківської установи:

– перелік законодавчих, регуляторних, нормативних вимог;

– затвердження переліку відомостей, що містять інформацію з обмеженим доступом;

– встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів;

– визначення критичних бізнес-процесів/банківських продуктів/ програмно-технічних комплексів;

– забезпечення надання доступу до інформації, її контролю та захисту;

– проведення політики ідентифікації та автентифікації ресурсів;

– політика криптографічного захисту інформації;

– політика «чистого екрана» та «чистого столу»;

– проведення внутрішнього аудиту та вдосконалення системи управління інформаційної безпеки.

Виділимо такі **основні етапи розроблення політики інформаційної безпеки:**

– визначення та оцінювання інформаційних активів;

– визначення загроз безпеці;

– оцінка інформаційних ризиків;

– визначення відповідальності;

– створення комплексного документа;

– реалізація;

– управління програмою безпеки.

Кожній банківській установі доцільно розробити власну політику інформаційної безпеки та ефективно впроваджувати комплекс заходів із захисту конфіденційних даних та інформаційних процесів.

Політика інформаційної безпеки банку повинна бути затверджена керівництвом банку та доведена до відома всього персоналу та за необхідності до зовнішніх сторін.

Політика інформаційної безпеки повинна встановити зобов'язання керівництва банку і викласти підхід банківської установи до управління інформаційною безпекою.

Розглянемо ієрархічний підхід до впровадження інформаційної політики банківської установи (рис. 5.1).

Для забезпечення інформаційної безпеки банківської установи необхідно застосовувати комплекс заходів, яких повинен дотримуватися кожен працівник банку, виходячи з покладених на нього обов'язків та визначеними правилами згідно політики інформаційної безпеки банку.

Політика інформаційної безпеки банку повинна мати процедури для взаємодії з зовнішніми організаціями, до яких входять правоохоронні органи, інші організації, команди швидкого реагування, засоби масової

інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

Крім положень політики безпеки, описаних вище, необхідно продумати і описати процедури, що виконуються у випадку виявлення порушень правил безпеки. Для всіх видів порушень мають бути заготовлені відповідні процедури.

Інформаційну систему банку можна вважати захищеною, якщо всі операції виконуються згідно із суворо визначеними правилами безпеки, що забезпечують безпосередній захист об’єктів, ресурсів і операцій.

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим суворішими є вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система.

Очевидно, що будь-яка офіційна політика безпеки час від часу порушується. Порушення може бути наслідком недбалості користувачів, випадкової помилки, відсутності надійної та належної інформації про поточну політику чи її нерозуміння. Можливо, також, що деяка особа – група осіб свідомо роблять дії, що прямо суперечать затвердженій політиці безпеки. Необхідно заздалегідь визначити характер дій, що починаються у випадку виявлення порушень політики інформаційної безпеки, щоб ці дії були швидкими й правильними. Варто організувати розслідування, щоб зрозуміти, як і чому порушення стало можливим. Після цього потрібно внести коригування в систему захисту. Тип і серйозність цих коригувань залежить від типу порушення, яке сталося.

Рис. 5.1. Ієрархічний підхід до впровадження інформаційної політики банківської установи

Дотримання політики інформаційної безпеки повинно бути обов'язковим для усіх співробітників. Документи щодо системи управління інформаційною безпекою повинні бути доступними працівникам банку лише у межах їх обов'язків і повноважень. Кожний працівник банківської установи несе відповідальність за порушення правил згідно з чинним законодавством та внутрішніми нормативними документами.

Звичайно, неможливо побудувати ідеальну політику інформаційної безпеки банківської установи, оскільки банк це відкрита установа з тисячами клієнтів. З часом усе змінюється: устрій життя, нормативно-законодавча база, модернізується обладнання, змінюється програмне забезпечення, розвиваються технології, а водночас і шкідливе програмне забезпечення, змінюється обслуговуючий персонал.

Отже, політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її постійної придатності, адекватності та ефективності.

Політика інформаційної безпеки повинна мати власника, який несе затверджену керівництвом відповідальність за розвиток, перегляд і оцінювання політики безпеки. Перегляд повинен охоплювати оцінку можливостей вдосконалення політики інформаційної безпеки організації і підхід до управління інформаційною безпекою в разі змін інфраструктури організації, бізнес-обставин, правових умов або технічної інфраструктури.

Перегляд політики інформаційної безпеки повинен враховувати результати переглядів з боку керівництва. Повинні бути визначені процедури перегляду з боку керівництва, включаючи графік або періодичність перегляду.

Реалізація політики інформаційної безпеки банку

Реалізація політики інформаційної безпеки банківської установи починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання завдань із захисту інформаційної системи банку. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Також варто враховувати основні положення з безпеки інформації:

– економічна ефективність – вартість засобів захисту має бути меншою, ніж розміри можливого збитку;

– кожен користувач повинний мати мінімальний набір привілеїв, необхідний під час роботи;

– простота системи захисту інформаційної системи – захист буде тим ефективнішим, чим легше користувачу з ним працювати;

– відключення захисту при нормальному функціонуванні – захист не повинен відключатися, за винятком особливих випадків, коли співробітник із спеціальними повноваженнями може мати можливість відключити систему захисту;

– відкритість проектування і функціонування механізму захисту;

– незалежність системи захисту від суб'єктів захисту – розроблювачами не повинні бути ті, кого вона буде контролювати;

– загальний контроль без будь-яких виключень з безлічі контрольованих суб'єктів;

– звітність і підконтрольність системи захисту;

– відповідальність осіб, що займаються інформаційною безпекою;

– об'єкти захисту доцільно розділити на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;

– відмова від замовчування – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;

– система захисту об’єкту має бути цілком специфікованою, протестованою та погодженою;

– система повинна допускати зміну своїх параметрів адміністратором;

– важливі критичні рішення повинні прийматися людиною, а не комп’ютером;

– система захисту об’єкта повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, будуть робити помилки і шукати шляхи обходу механізмів захисту;

– інформація про існування механізмів захисту повинна бути, по можливості, схована від користувачів, робота яких контролюється.

При підтримці політики інформаційної безпеки банку потрібно постійне спостереження за вторгненнями зловмисників у мережу, виявлення вад і «дір» у системі захисту інформаційної системи, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку політики інформаційної безпеки банку лежить на відповідальній особі, призначеній керівництвом банку. Цей фахівець повинен оперативно реагувати на всі випадки зламу конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні та програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

РОЗДІЛ 6. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВСЬКИХ УСТАНОВ

Методи захисту інформації

Система управління інформаційною безпекою ґрунтується на трьох фундаментальних принципах управління:

– принцип розімкнутого керування;

– принцип компенсації;

– принцип зворотного зв'язку.

За принципом розімкнутого управління створюються власні політики безпеки, виконання яких контролюється відповідальними особами. В даний час більшість компаній виділяє для особи, відповідальної за розробку і реалізацію політик ІБ, позицію CISO (Chief Information Security Officer) – керівника відділу IT-безпеки або директора по IT-безпеки. Як правило, CISO очолює керуюча рада з питань інформаційної безпеки.

Принцип компенсації має на увазі, що в разі виникнення будь-яких відхилень від розробленої політики безпеки або зовнішніх факторів необхідно негайно вносити відповідні корективи в алгоритм управління, що компенсували б негативний результат зовнішніх впливів.

Наявність ланки **зворотного зв'язку** в системі управління інформаційною безпекою дозволяє не тільки виявити окрему загрозу, але і відреагувати на цілий ряд подій, на перший погляд ніяк не пов'язаних між собою. У цьому можуть допомогти продукти, що забезпечують централізоване зіставлення даних журналів подій з мережевих пристроїв і систем безпеки в режимі реального часу, автоматично зіставляючи дані і виділяючи події і загрози безпеці, що вимагають прийняття рішучих заходів, такі як Check Point Eventia Analyzer.

Побудова систем ІБ з урахуванням перерахованих принципів дозволяє використовувати існуючі методи оптимізації для покращення різних показників якості системи, таких як стійкість управління, швидкість реакції на існуючі та невідомі загрози

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 топ-менеджментом 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.

Захистити інформацію від несанкціонованого доступу можна за допомогою апаратно-програмних, програмних, біометричних, технічних і адміністративних засобів.

Апаратно-програмні засоби:

– спеціальні криптографічні плати, що вбудовуються в комп'ютер, за допомогою яких інформацію можна зашифрувати, створити електронний підпис, а також автентифікувати користувача;

– SmartCard — магнітна картка для зберігання секретного ключа, шифрування паролів;

– пристрої ActivCard для введення паролів, де пароль не вводиться, а розраховується, а також SmartReader для зчитування паролів. В цих пристроях всередині вмонтовано мікропроцесор, у пам'яті якого зберігається секретний код. Пароль, що вводиться користувачем, в комп'ютері перераховується, тобто створюється спеціальний код.

Програмні заходи:

– вбудовані у програми функції захисту даних;

– спеціальні криптографічні розробки.

За принципом побудови існуючі засоби захисту інформації можна поділити на два типи:

-засоби, в основі роботи яких лежать симетричні алгоритми для побудови ключової системи і системи автентифікації;

– засоби, основу роботи яких складають асиметричні алгоритми, що застосовуються для тих самих цілей.

У засобах першого типу обов'язковою є наявність центру розподілу ключів, що відповідає за їх створення, розповсюдження та вилучення. При цьому носії ключової інформації передаються абонентам із використанням фізично захищених каналів зв'язку. Ключі мають змінюватися досить часто, кількість абонентів має бути значною, тому ці засоби негнучкі та дорогі. Питання автентифікації вирішується довірою користувачів один одному, цифровий підпис неможливий. Центр розподілу ключів контролює всю інформацію. Захист інформації дуже низький.

У засобах другого типу ключі для шифрування автоматично генеруються, розповсюджуються і вилучаються для кожного сеансу

зв'язку. Функції служби розповсюдження ключів виконує сертифікаційний центр, де користувач реєструється, встановлюється його автентифікація, після чого ключі вилучаються. В таких засобах можливими є організація цифрового підпису та його перевірка. Протокол встановлення аутентичного зв'язку відповідає певному стандарту. Автентифікація є простою та суворою. При простій автентифікації відбувається обмін паролями між абонентами, які встановили зв'язок, із подальшою перевіркою відповідності цих паролів еталонним. При суворій автентифікації кожен абонент має два криптографічних ключі — секретний, відомий тільки даному абоненту, та відкритий — той, що передається в банк. Використовуючи секретний ключ і спеціальний алгоритм, абонент формує цифровий підпис — послідовність бітів, яка однозначно відповідає документу, що підписується. Перевірка відповідності підпису виконується за допомогою відкритого ключа.

Властивості управління інформаційною безпекою в банку

Зміни, що відбулися в банківському секторі протягом останнього десятиліття, призвели до об’єднання інформаційних та комп’ютерних мереж в єдиний інформаційний та кібернетичний простір. Інтеграційні процеси обумовили створення автоматизованих банківських систем (АБС), які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози у такому національному інформаційному ресурсі держави, як банківська інформація.

Почнемо з того, що підхід до організації інформаційної безпеки визначається трьома основними факторами. Перший – це особливості бізнес-процесів в у банківських установах. Другий – специфіка інформації, яка є в розпорядженні і обробляється. І третій – це коло осіб, допущених до оброблення інформації.

У найзагальнішому розумінні, банки оперують чужими грошима, щоб створити свій прибуток. Тому інцидент інформаційної безпеки в банку в більшості випадків призводить до реальних втрат реальних грошей, тобто до прямих збитків. Не будемо забувати і про репутаційні втрати, штрафні санкції, тощо. Постанова правління Національного банку від 28.08.2017 № 95 дає поняття "критичний бізнес-процес банку", навколо якого і повинна будуватися вся система управління інформаційною безпекою.

Банки оперують персональними даними клієнтів. У нашій реальності, мабуть, саме банки мають найбільший обсяг інформації про кожного з нас. Будучи клієнтом банку, ми всі даємо згоду на оброблення персональних даних, не замислюючись, хто і як буде їх обробляти і зберігати. Це теж завдання системи управління інформаційною безпекою.

Важливо пам’ятати, що в рамках роботи систем банку задіяні звичайні користувачі, далекі від питань безпеки. Відповідно, щоб уникнути можливих проблем і перебоїв в роботі систем для користувачів повинні бути розроблені єдині вимоги з управління обліковими записами, парольної політики, автентифікації тощо.

В кінцевому підсумку, банківська система – це частина критичної інфраструктури держави, збої в роботі якої можуть привести до жахливих наслідків для всієї фінансової системи.

Враховуючи те, що управління інформаційною безпекою в банківських установах має свої особливості, визначимо, що основними об’єктами захисту у системі управління інформаційною безпекою банку є:

– інформаційні ресурси, що містять комерційну та банківську таємницю, відомості обмеженого поширення, а також відкрита інформація, необхідна для роботи банку, незалежно від форми її подання;

– інформаційні ресурси, що містять конфіденційну інформацію, включаючи персональні дані фізичних осіб, а також відкрита інформація, необхідна для роботи банку;

– інформаційна інфраструктура банку, яка інформаційно-телекомунікаційні системи, системи і засоби захисту інформації і приміщень, в яких розміщено такі системи.

Постанова правління Національного банку України від 28.08.2017 № 95 зобов'язує банки упровадити систему управління інформаційною безпекою (СУІБ) згідно з ДСТУ ISO/IEC 27001:2015 для визначеної сфери застосування з урахуванням обов'язкових вимог щодо впровадження СУІБ, викладених у Положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого цією постановою.

Ця постанова також зобов'язує банк визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку. Банк має право розширити сферу застосування СУІБ банку відповідно до особливостей його діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

Стандарти Національного банку України базуються на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами, які вже висунуто в нормативних документах Національного банку України.

Впровадження СУІБ в банківських установах

Зобов'язання керівництва щодо управління інформаційною безпекою

Відповідно до стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 керівництво банку повинно забезпечити визначення завдань інформаційної безпеки, їх відповідність вимогам законодавства України, нормативно-правових актів Національного банку України та банку, інтегрованість у відповідні бізнес-процеси/банківські продукти, переглядати ефективність впровадження та

функціонування СУІБ, надавати ресурси, які потрібні для інформаційної безпеки та навчання персоналу з питань інформаційної безпеки.

Для вирішення цих завдань необхідно визначити організаційну структуру управління інформаційною безпекою, повноваження та відповідальність щодо розроблення, впровадження та функціонування СУІБ.

Керівництво СУІБ може здійснювати керівник банку або його заступник, або існуючий керівний орган, наприклад, рада з питань інформатизації з обов'язковим включенням до складу спеціалістів з питань інформаційної безпеки. Залежно від розміру банку ці обов'язки можуть бути покладені на створений спеціальний керівний орган з питань інформаційної безпеки з керівників підрозділів, відповідальних за критичні бізнес-процеси та банківські продукти.

Відповідно до стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010 діяльність банку із забезпечення інформаційної безпеки повинна бути узгодженою між представниками різних підрозділів банку, які відповідають та забезпечують функціонування критичних бізнес-процесів/банківських продуктів. Банки мають створювати єдину систему інформаційної безпеки для всіх бізнес-процесів та координувати дії різних підрозділів для забезпечення виконання загальних вимог щодо інформаційної безпеки. Для виконання цих обов'язків може бути створена окрема група з перехресними функціями з фахівців різних підрозділів. Якщо банк не створює окрему групу з перехресними функціями, то ці обов'язки повинні виконуватися спеціальним керівним органом або окремим керівником.

Банк має визначити всі підрозділи, які відносяться до сфери застосування СУІБ. Це підрозділи, які є власниками та учасниками критичних бізнеспроцесів, підрозділи, які супроводжують та забезпечують технічну підтримку програмно-технічних комплексів, користувачі програмно-технічних комплексів, служба безпеки, яка забезпечує фізичну безпеку приміщень банку, тощо. Наявність такого переліку підрозділів

дозволить чітко визначити обов'язки та відповідальності всіх причетних до виконання вимог безпеки сторін та планувати їх навчання у разі необхідності. Такий перелік може створюватися на основі структурної схеми підрозділів банку. Окрім того, у разі передавання частини послуг, пов'язаних з критичними бізнес-процесами/банківськими продуктами/ програмно-технічними комплексами, третім сторонам, ці організації також повинні бути включені до опису організаційної структури банку з приміткою, що вони не є структурними підрозділами банку.

Зрозуміло, що для проведення цих робіт потрібні ресурси, у тому числі наявність фахівців з питань інформаційної безпеки, наявність з боку керівництва банку повної підтримки та контролю, а також розуміння проблем, що виникають.

Система інформаційної безпеки повинна забезпечити безпечність та надійність функціонування бізнес-процесів/банківських продуктів банку. Впровадження та функціонування СУІБ стосується всіх підрозділів банку і, у першу чергу, керівників підрозділів – власників бізнес-процесів / банківських продуктів. Тому ці відповідальні особи повинні брати участь у вирішенні питань, що належать до сфери їх відповідальності, під час упровадження та функціонування СУІБ.

Зазвичай, координація інформаційної безпеки повинна стосуватися співробітництва і координації спільної діяльності менеджерів, користувачів, адміністраторів, розробників прикладних програм, аудиторів і персоналу безпеки, а також фахівців у таких галузях, як страхування, правові питання, людські ресурси, управління IT або ризиками.

Розроблення СУІБ банку повинно розроблятися на основі міжнародного стандарту ISO/IEC 27003:2010 «Information technology – Security techniques –Information security management system implementation guidance» (Настанова з впровадження системи управління інформаційною безпекою) з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки. Як

ми зазначали, управління інформаційною безпекою є циклічним процесом. Це фактично безперервний процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ. Саме тому методологічною **основою управління інформаційною безпекою, відповідно до стандартів серії ISO 27000**, є процесний підхід.

Для ефективної діяльності банківської установи необхідно ідентифікувати та управляти багатьма видами діяльності. Будь-яку діяльність, що використовує ресурси та підлягає управлінню з метою забезпечення перетворення вхідних даних у вихідні, можна розглядати як процес. Часто вихідні дані одного процесу є безпосередньо вхідними даними для наступного.

Застосування системи процесів у межах банку разом з ідентифікацією цих процесів та їх взаємодіями, а також управління ними можна розглядати як **процесний підхід**.

Процесний підхід до управління інформаційною безпекою виводить на перший план важливість:

– розуміння вимог інформаційної безпеки банку і необхідності розроблення політики та цілей інформаційної безпеки;

– впровадження заходів безпеки та забезпечення їх функціонування для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків банку;

– моніторингу та перегляду продуктивності та ефективності СУІБ та постійного вдосконалення, що базується на об’єктивному вимірюванні.

У межах такого підходу, для процесів СУІБ застосовується модель **“Плануй-Виконуй-Перевіряй-Дій” (“Plan-Do-Check-Act”),** наведена у вступі до стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010.

Порівняння СУІБ та процесу управління ризиками інформаційної безпеки можна описати у вигляді таблиці.

Фаза СУІБ	Процес управління ризиками інформаційної безпеки
Плануй (розробляй СУІБ)	Аналіз ресурсів СУІБ Оцінка ризиків План оброблення ризиків Прийняття залишкових ризиків
Виконуй (впроваджуй, забезпечуй функціонування СУІБ)	Впровадження плану оброблення ризиків
Перевіряй (здійснюй моніторинг та перегляд СУІБ)	Постійний моніторинг та перегляд ризиків
Дій (підтримуй та вдосконалюй СУІБ)	Підтримка та покращення процесу управління ризиками інформаційної безпеки

Відповідно до вимог стандартів Національного банку України **сферою застосування СУІБ, яка має бути впроваджена, є банк у цілому.** Тому дуже важливо чітко визначити бізнес-процеси/ банківські продукти, які працюють з інформацією з обмеженим доступом і повинні бути захищеними.

Відповідно до Положення про організацію операційної діяльності в банках України, затвердженого постановою Правління Національного банку України від 18.06.2003 № 254, банківський продукт – це стандартизовані процедури, що забезпечують виконання банками операцій, згрупованих за відповідними типами та ознаками.

Поняття бізнес-процесу є багатозначним і не існує загально прийнятого його визначення. Під бізнес-процесом у широкому значенні

розуміється структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу предмета діяльності. Кожен бізнес-процес має початок (вхід), вихід та послідовність процедур, які забезпечують виконання операцій, згрупованих за відповідними типами.

Для визначення бізнес-процесів/банківських продуктів, які має охоплювати СУІБ, необхідно проаналізувати всі бізнес-процеси/ банківські продукти банку та створити перелік критичних процесів, функціонування яких має великий вплив на успішну роботу банку. Оскільки в банку бізнес-процеси/банківські продукти взаємопов'язані, то рекомендується створити їх блок-схему з визначенням усіх взаємозв'язків. Така візуалізація значно спростить розуміння всього обсягу робіт, що виконуються банком.

Банк повинен створити перелік критичних бізнес-процесів/ банківських продуктів, які обробляють інформацію з обмеженим доступом, розголошення якої може нанести шкоду банку. До цього переліку повинні бути включеними всі бізнес-процеси/банківські продукти, що обробляють:

– платіжні документи,

– внутрішні платіжні документи,

– кредитні документи,

– документи на грошові перекази,

– персональні дані клієнтів та працівників банку,

– статистичні звіти,

– інші документи, які містять інформацію з обмеженим доступом.

Для кожного критичного бізнес-процесу/банківського продукту рекомендується надати перелік бізнес-процесів/банківських продуктів, з якими взаємодіє цей бізнес-процес/банківський продукт.

Перелік критичних бізнес-процесів/банківських продуктів повинен супроводжуватися коротким описом кожного бізнес-процесу/ банківського продукту з наданням інформації про програмно-технічні комплекси, які забезпечують його функціонування.

Короткий опис кожного бізнес-процесу/банківського продукту повинен містити таку інформацію:

-назва бізнес-процесу/банківського продукту;

– цілі бізнес-процесу/банківського продукту;

– гриф інформації з обмеженим доступом, яка обробляється бізнес-процесом/банківським продуктом;

– власник бізнес-процесу/банківського продукту;

– підрозділи банку, які забезпечують функціонування бізнес-процесу/банківського продукту;

– наявність зобов'язань перед третіми сторонами (угоди на розроблення, доопрацювання, супроводження та технічне обслуговування);

– вхідні та вихідні дані бізнес-процесу/банківського продукту;

– перелік процедур бізнес-процесу та блок-схема послідовності їх виконання з визначенням взаємозв'язків;

– вимоги щодо забезпечення безперервності бізнес-процесу/ банківського продукту;

– типи ролей (груп) для бізнес-процесу/банківського продукту;

– існування забороненого суміщення типів ролей;

– програмно-технічні комплекси, що забезпечують функціонування бізнес□процесу;

– кількість користувачів програмно-технічного комплексу;

– архітектура і технологія роботи;

– операційна система та тип бази даних програмно-технічного комплексу, які використовуються для функціонування бізнес-процесу/банківського продукту;

– географічне розміщення (серверів та робочих місць) програмно-технічного комплексу;

– засоби захисту, які вже існують у програмно-технічному комплексі;

– взаємодія з іншими програмно-технічними комплексами;

– принципи резервування обладнання та інформації програмно-технічного комплексу.

Дуже важливо визначити власника бізнес-процесу/банківського продукту, який повинен також бути власником програмно-технічного комплексу. Саме власник бізнес-процесу/банківського продукту / програмно-технічного комплексу повинен приймати рішення щодо надання доступу до інформації, яка обробляється в цьому бізнес-процесі/банківському продукту/програмно-технічному комплексі. Власником програмно-технічного комплексу не може бути підрозділ банку, який відповідає за інформаційні технології і забезпечує технічну підтримку роботи комплексу.

У разі якщо функціонування одного бізнес-процесу/банківського продукту забезпечується декількома програмно-технічними комплексами, тоді короткі описи кожного комплексу та їх взаємозв'язків повинні також бути надані.

У разі якщо один програмно-технічний комплекс забезпечує функціонування декількох бізнес-процесів/банківських продуктів, тоді визначається єдиний власник програмно-технічного комплексу або група власників бізнес-процесів, які надають та контролюють доступ до інформації, що обробляється різними модулями комплексу.

У разі відсутності централізованих програмно-технічних комплексів мають бути надані короткі описи програмно-технічних комплексів у структурних підрозділах банку та описаний взаємозв’язок між ними.

Для більшого розуміння зв’язків між бізнес-процесами/банківськими продуктами/програмно-технічними комплексами рекомендується створити блок-схему цих зв’язків із додаванням структурних підрозділів банку, які забезпечують ці бізнес-процеси/банківські продукти/програмно-технічні комплекси вхідною інформацією, та підрозділів банку, які використовують вихідні дані.

СУІБ, використовуючи як вхідні дані вимоги інформаційної безпеки та очікування зацікавлених сторін, за допомогою необхідних дій і процесів формує вихідні дані інформаційної безпеки, що відповідають цим вимогам та очікуванням.

РОЗДІЛ 7. БЕЗПЕКА В АВТОМАТИЗОВАНИХ СИСТЕМАХ БАНКУ

Захист інформації в інформаційних системах

Як інформаційний об’єкт банк є єдиним комплексом компонентів, пов’язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Ці компоненти в процесі функціонування банку можуть змінюватися, на них можуть здійснювати вплив різного роду внутрішні та зовнішні чинники, які складно прогнозувати та оцінювати. Велику кількість компонентів, які формують банк як об’єкт інформатизації, можна подати сукупністю **чотирьох груп: персонал, технічні засоби інформатизації, програмне забезпечення, документи.**

Ці групи зазнають впливу різного роду специфічних факторів і, взаємодіючи між собою, впливають одна на одну, формуючи відповідний стан інформаційної безпеки банку. Як показує практика, робота з кожною з цих груп щодо забезпечення інформаційної безпеки чи, зокрема, щодо захисту інформації призводить до покращення якостей безпеки по одних параметрах і погіршення по інших, що вимагає комплексного підходу до забезпечення інформаційної безпеки банку.

Забезпечення інформаційної безпеки і такої її складової, як захист інформації, неможливо здійснити лише організаційними чи технічними заходами, або, скажімо, програмними чи криптографічними. Дії щодо забезпечення інформаційної безпеки повинні бути регулярним процесом, що здійснюється на всіх напрямах діяльності банку на основі комплексного застосування всіх заходів і засобів безпеки. При цьому засоби, заходи та методи безпеки найбільш раціональним способом об’єднуються в єдиний цілісний механізм не лише для захисту від зловмисників, а й від некомпетентних, недобросовісних працівників банку

та різних непередбачуваних ситуацій. Тобто **забезпечення інформаційної безпеки як і кожної з її складових мусить мати системний та комплексний характер.**

Системність заходів інформаційної безпеки має передбачати таке:

– високий ступінь захищеності інформації банків як головну характеристику її якісного стану;

– заходами безпеки охоплюються всі інформаційні ресурси банку всієї його структури;

– діяльність щодо забезпечення інформаційної безпеки є безперервною і плановою, на основі єдиної концепції безпеки;

– забезпечення інформаційної безпеки здійснюється у тісній єдності з поточною діяльністю банку.

Комплексний характер системи забезпечує оптимізацію заходів і засобів, що використовуються нею задля створення необхідного балансу вимог і можливостей інформаційної безпеки банку. Комплексний підхід обумовлюється ще й тим, що загрози інформації банку мають різноманітний характер, перекриття яких потребує застосування багатьох, різних за призначенням заходів і засобів.

Більше того, забезпечення безпеки у сучасних умовах має здійснюватися як на технологічному, так і на логічному рівнях, що повинно забезпечувати урахування всіх факторів і особливостей, які впливають на безпеку банку, а також усіх компонентів інформаційної роботи: збирання, оброблення, зберігання, передавання, використання інформації. За таких умов системність та комплексність банківської безпеки, у тому числі й у сфері захисту інформації є обов'язковою умовою її високої ефективності.

Основними об'єктами захисту в банку є:

– фінансові ресурси (національна та іноземна валюта, коштовності, фінансові документи);

– персонал банку;

– матеріальні засоби;

– інформаційні ресурси банку з обмеженим доступом.

Важливе значення у захисті інформації має політика безпеки банку. Відповідно до прийнятої в банку політики безпеки проводяться організаційні заходи щодо створення системи захисту інформації.

Система захисту інформації банку – це організована сукупність об'єктів і суб'єктів захисту інформації, заходів, методів і засобів, що використовуються для захисту. **Основна мета створення системи захисту інформації** – забезпечення надійності зберігання і використання інформації в банку.

В банках напрацьовано відповідний алгоритм роботи з організації системи захисту інформації, який включає такі дії:

– визначення вразливості інформації банку;

– визначення мети, завдань та об'єктів захисту інформації;

– вибір форм, способів і засобів захисту інформації;

– формування елементів системи захисту інформації, її сил та засобів;

– створення нормативної бази банку з питань захисту інформації;

– планування функціонування системи, використання нею сил та засобів захисту інформації у відповідності до особливосте і діяльності банку;

– забезпечення взаємодії всіх елементів системи між собою та з іншими компонентами, які згідно з політикою безпеки можуть бути задіяні для захисту банківської інформації;

– забезпечення функціонування системи;

– контроль стану захищеності інформації, надійності функціонування системи та ефективності заходів, що вживаються нею.

Система захисту інформації платіжних систем банку повинна складатися з:

1) законодавчих актів України та інших нормативно-правових актів, а також внутрішніх нормативних актів суб'єктів переказу, що регулюють порядок доступу та роботи з відповідною інформацією, а також відповідальність за порушення цих правил;

2) заходів охорони приміщень, технічного обладнання відповідної платіжної системи та персоналу суб'єкта переказу;

3) технологічних та програмно-апаратних засобів криптографічного захисту інформації, що обробляється в платіжній системі.

Система захисту інформації платіжних систем банку має забезпечувати:

1) цілісність інформації, що передається в платіжній системі, та компонентів платіжної системи;

2) конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі;

3) неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання;

4) забезпечення постійного та безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

Зазвичай банки не передбачають захисту відкритої інформації. Але ж відкритість інформації не позбавляє її цінності, а цінна інформація, безумовно, має захищатися. Захист такої інформації здійснюється за допомогою реєстрації її носіїв, обліку, контролю наявності. Водночас захист відкритої інформації не повинен обмежувати її загальнодоступність, але доступ до неї має бут и контрольованим із дотриманням відповідних вимог щодо її збереження. Тобто відкрита інформація є об'єктом захисту, і стосовно неї мають проводитися певні заходи в системі захисту

інформації. Загальною ж основою для вибору об’єкта захисту є **цінність інформації.**

Критеріями цінності інформації можуть бути:

– необхідність інформації для правового забезпечення діяльності банку;

– необхідність інформації для здійснення виробничої діяльності банку;

– необхідність інформації для ефективного управління діяльністю банку, об’єктивного прийняття управлінських рішень, організації прибуткової діяльності банку;

– необхідність інформації для формування ресурсної бази банку та забезпечення його безпеки.

Система захисту інформації банку у своєму функціонуванні має конкретний характер і потребує однозначної конкретизації об’єктів захисту. Інформація, на яку спрямовуються зусилля системи захисту не існує сама по собі, а фіксується (відбивається) у відповідних матеріальних об’єктах або пам’яті людей, тобто вона існує на відповідних носіях. Таким чином, обираючи об’єкт захисту, ми маємо визначити певний перелік носіїв невідомої третім особам інформації, за рахунок якої банк отримує певні переваги у своїй діяльності. Захист цих об’єктів має здійснюватися регулюванням доступу до них, установленням від□повідного порядку їх використання (діяльності) та формуванням умов зберігання. Якраз ці заходи і складають структуру системи захисту інформації.

Особливим напрямком забезпечення інформаційної безпеки в банках є **захист банківських інформаційних систем**. Тому при розробленні архітектури та створенні інфраструктури банківської інформаційної системи слід забезпечити її захищеність від загроз. Вирішення цієї проблеми полягає в детальному аналізі таких взаємопов’язаних видів робіт, як проектування та впровадження банківської інформаційної системи, її атестація, аудит та обстеження на предмет безпеки. З метою

забезпечення збереженості конфіденційності, цілісності та доступності інформації, що циркулює в банківських установах, банки мають використовувати у своїй діяльності **спеціалізоване програмно-апаратне забезпечення.**

1) програмний захист від несанкціонованого входу на робочу станцію комп'ютерної мережі банківської установи;

2) організації локальної обчислювальної мережі на базі доменної структури. Це дасть змогу адміністратору такої мережі, по-перше, розмежувати права доступу всіх користувачів до певних класів інформації, по-друге, розписати для кожного користувача політику безпеки та організувати його власний профіль, по-третє, обмежити обсяг доступної для збереження інформації з метою збереження сервера від перевантаження та втрати основних властивостей інформації, по-четверте, організувати статистику роботи користувачів у мережі, та у разі необхідності виявити спробу несанкціонованого доступу зловмисника до інформації;

3) програмні модулі мережевого сканування для виконання деяких завдань. Це по-перше, сканування робочих станцій, які ввійшли в мережу, по-друге, виявлення несанкціонованої роботи не легалізованих робочих станцій в мережі, по-третє, виявлення нестандартних процесів, завантажених в оперативну пам'ять робочих станцій, по-четверте, виявлення несанкціонованого програмного забезпечення сканування мережі, тощо;

4) використання серверної платформа та програмні клієнтські модулі управління системою антивірусного захисту. Цей спосіб дає змогу налаштувати автоматичне сканування всієї локальної обчислювальної мережі. Всі основні налаштування, такі як автоматичне щоденне оновлення всіх частин системи антивірусного захисту, автоматичне сканування мережі та робочої станції, тощо, відбуваються на серверній частині програмного забезпечення;

5) криптозахист файлів електронної пошти банківської установи, які можуть зберігатись на спеціальному поштовому серверів. Використання всіх перелічених складових дасть змогу забезпечити надійний захист інформації, яка циркулює в автоматизованих системах банківської установи.

Криптографічний захист інформації

Криптографічний захист інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Зашифровані повідомлення передаються відкрито, приховується їхній зміст. Використання криптографічного захисту інформації під час побудови політики безпеки банківської on-line-системи значно посилює безпеку роботи системи, але за умови, що ця система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів.

Криптографічні методи захисту інформації – це методи захисту даних із використанням шифрування.

Шифрування — це технічний процес, за допомогою якого інформація перетворюється на секретний код, маскуючи дані, які ви надсилаєте, отримуєте чи зберігаєте. Шифрування інформації широко використовується в службах безпеки, банках та інших комерційних підприємствах, що містять дані з обмеженим доступом.

Головна мета шифрування (кодування) інформації – її захист від несанкціонованого читання.

Системи криптографічного захисту (системи шифрування інформації) для банківських on-line -систем можна поділити за різними ознаками:

– за принципами використання криптографічного захисту;

– за способом реалізації;

– за криптографічними алгоритмами, які використовуються;

– за цілями захисту;

– за методом розподілу криптографічних ключів тощо.

Вбудовані механізми криптографічного захисту входять до складу системи, їх створюють одночасно з розробленням банківської on-line-системи. Такі механізми можуть бути окремими компонентами системи або бути розподіленими між іншими компонентами системи.

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним.

Апаратна реалізація криптографічного захисту полягає в тому, що інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передавання в апаратуру може бути виконана за допомогою спеціально розроблених програм типу "вірус". Апаратна реалізація найбільш надійний спосіб, але й найдорожчий.

Програмна реалізація криптографічного захисту є значно дешевшою та гнучкішою в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення.

Крім того, можна використовувати **комбінацію апаратних і програмних механізмів криптографічного захисту**. Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, вибираючи апаратні засоби для зберігання криптографічних ключів, треба пам’ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптографічні алгоритми мають секретний алгоритм шифрування, а загальні криптографічні алгоритми характеризуються повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптографічного захисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхню висока криптостійкість доведено. Ці алгоритми оприлюднюють для обговорення, при цьому навіть визначається премію за успішну спробу його "зламування". Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою зі збільшенням довжини ключа.

Є дві групи загальних криптографічних алгоритмів: симетричні і асиметричні.

До **симетричних** криптографічних алгоритмів належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість оброблення як для апаратної, так і для програмної реалізації. Основним їх недоліком є труднощі, пов’язані з дотриманням безпечного розподілу ключів між абонентами системи.

Для **асиметричних** криптографічних алгоритмів шифрування і розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостійкості алгоритму і не дає можливості відновлення парного йому ключа.

Метою використання криптографічних методів є захист інформації від модифікації, викривлення або підроблення. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена.

Для симетричних алгоритмів шифрування така додаткова інформація – це код автентифікації, який формується за наявності ключа шифрування за допомогою криптографічних алгоритмів.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву **електронний цифровий підпис.**

Електронний цифровий підпис – сукупність даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, яка його підписала.

Останнім часом використання електронного цифрового підпису значно поширюється, у тому числі для регулювання доступу до конфіденційної банківської інформації та ресурсів системи, особливо для on-line-систем реального часу. Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів.

– **Метод базових/сеансових ключів**. Цей метод описано у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ і ключ шифрування даних. Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключів потребує значного часу і значних затрат.

– **Метод відкритих ключів**. Цей метод описано у стандарті ISO 11166 і його може бути використано для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує абсолютного захисту інформації, але гарантує, що вартість зламування у кілька разів перевищує вартість зашифрованої інформації.

Для використання системи криптографії з відкритим ключем потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів – через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат – це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Головним обмеженням криптографічних систем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна дізнатися напевне, хто саме його відправив. Постановою правління Національного банку України від 28.09.2017 № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" визначено **принципи криптографічного захисту інформаційних систем Національного банку України**:

– криптографічний захист інформації в інформаційних системах Національного банку України на ділянці зв'язку між учасником інформаційних систем Національного банку та Національним банком забезпечується застосуванням багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансів рівень базової еталонної моделі взаємодії відкритих систем (Open systems interconnection basic reference model, OSI/ISO) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку;

– для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовується криптографічний протокол захисту на транспортному рівні (Transport layer security, TLS), забезпечуються контроль цілісності та конфіденційність інформації. Для прикладного рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються такі механізми захисту: ідентифікація/автентифікація підписувача, контроль цілісності та конфіденційність на всіх етапах оброблення інформації;

– залежно від категорії інформації щодо критерію конфіденційності, для забезпечення ідентифікації та автентифікації, використовується односпрямований (криптографічний ключ лише на стороні сервера, сувора криптографічна

автентифікація сервера) або двоспрямований достовірний канал захисту на транспортному рівні (криптографічний ключ на стороні клієнта і на стороні сервера, сувора криптографічна автентифікація обох сторін з'єднання).

Цією постановою також визначено такі обов'язкові заходи щодо криптографічного захисту інформації в інформаційних системах Національного банку України:

– налаштувати системи криптографічного захисту інформації в інформаційних системах Національного банку згідно з вимогами, які

визначені у відповідній експлуатаційній документації кожної інформаційної системи Національного банку;

– забезпечити захист інформаційних систем банку від несанкціонованого доступу та дій, спрямованих на відмову в обслуговуванні.

У разі застосування криптографічного захисту банк зобов'язаний використовувати криптографічні алгоритми з такого переліку:

1) асиметричні алгоритми:

– алгоритм Діффі – Геллмана (алгоритм DH) для узгодження сеансових ключів шифрування;

– алгоритм цифрового підпису (алгоритм DSA) для цифрових підписів;

– алгоритм Діффі – Геллмана на еліптичних кривих (алгоритм ECDH) для узгодження сеансових ключів шифрування;

– алгоритм цифрового підпису на еліптичних кривих (алгоритм ECDSA) для цифрових підписів;

– алгоритм Ривест – Шаміра – Адлемана (алгоритм RSA) для цифрових підписів і узгодження сеансових ключів шифрування або аналогічних ключів;

– алгоритм цифрового підпису (ДСТУ 4145-2002 ―Інформаційні технології.

Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння для цифрових підписів;

2) алгоритми безпеки гешування SHA-224, SHA-256, SHA-384, SHA512, "Купина" (ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування") або більш криптостійкі;

3) алгоритми симетричного шифрування:

– алгоритм "Advanced encryption standard" (AES) із використанням довжини ключа 128, 192 і 256 біт або більше;

– алгоритм криптографічного перетворення (ДСТУ ГОСТ 28147:2009 "Система оброблення інформації. Захист криптографічний. Алгоритм криптографічного перетворення");

– алгоритм "Калина" (ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення").

Банк зобов’язаний використовувати останню версію протоколу захисту на транспортному рівні та реалізацію цього протоколу, що підтримує безпечне повторне погодження з’єднання для захисту з’єднань, які управляються протоколом Transmission control protocol (TCP). Якщо безпечне повторне погодження з’єднання не підтримується, то ця процедура має бути відключена.

РОЗДІЛ 8. БЕЗПЕКА МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ SWIFT

Основні поняття мережі передачі даних SWIFT

Мережа передачі даних SWIFT (Society for World-Wide Interbank Financial Telecommunication) забезпечує оперативне зберігання та пересилання банківських документів різного типу між банками, підключеними до мережі SWIFT, але не забезпечує виконання жодних розрахункових чи інших операцій з банківської обробки повідомлень. Головна мета створення SWIFT і її основна функція, полягають у забезпеченні користувачам цілодобової високошвидкісної передачі банківських даних за умови високого ступеня контролю даних та захисту від несанкціонованого доступу.

Дані передаються по мережі шляхом пакетної комутації у вигляді структурованих повідомлень кожне з яких призначене для виконання певної фінансової операції. Для кожного підключеного вузла (банку) мережа забезпечує індивідуальне підтвердження приймання повідомлення та його обробки.

Метою створення SWIFT було забезпечення всіх банків, що беруть участь у проекті, захищеної від несанкціонованого доступу, надійною, високошвидкісною і цілодобово працюючою системою для передачі банківської інформації.

Вартість передачі одного повідомлення в системі SWIFT виявляється менше, ніж вартість його передачі по телексу.

Особливістю SWIFT є використання єдиних для всіх користувачів правил і понять. Стандартизовані типи повідомлень мережі охоплюють сфери переміщень платежів клієнтів, міжбанківський рух платежів, дані про торгівлю грошима і валютою, виписки з платіжних рахунків банків, і т.п. Стандартизація типів повідомлень переданих по мережі SWIFT була виконана Міжнародним комітетом зі стандартизації. У 1974-80 рр.

розробку типових повідомлень було завершено. Наприкінці 1993 р. була додана група нових фінансових стандартів SWIFT Alliance, де визначаються інтерфейси для зв'язку з національними глобальними мережами комп'ютерів по телексу і факсу.

Застосування стандартних форматів повідомлень у рамках системи SWIFT дає наступні переваги:

– виключається можливість різної інтерпретації повідомлень відправником і одержувачем;

– можливий повний контроль за передачею інформації на основі постійної фіксації трансакцій у системі;

– банк-користувач системи може автоматично генерувати щоденний звіт по проведених операціях.

У цілому система SWIFT являє собою глобальну всесвітню мережу на основі комп'ютерних центрів, з'єднаних різними каналами зв'язку. Основні комп'ютерні центри розташовані в США і Голландії. Ці центри зв'язані з регіональними хост-комп'ютерами, що встановлюються в країнах, що вступили в співтовариство SWIFT. Повідомлення від банку-відправника надходить через модем по відповідних каналах (комутованих або виділених телефонних лініях) у регіональний хост-комп'ютер. Відповідальність за передачу повідомлення до регіонального хост-комп’ютер несе банк-відправник. У регіональному центрі системи SWIFT повідомлення перевіряються на відповідність стандартам, накопичуються, шифруються і передаються по призначенню. Структура мережі SWIFT має два рівні (рис.8.1).

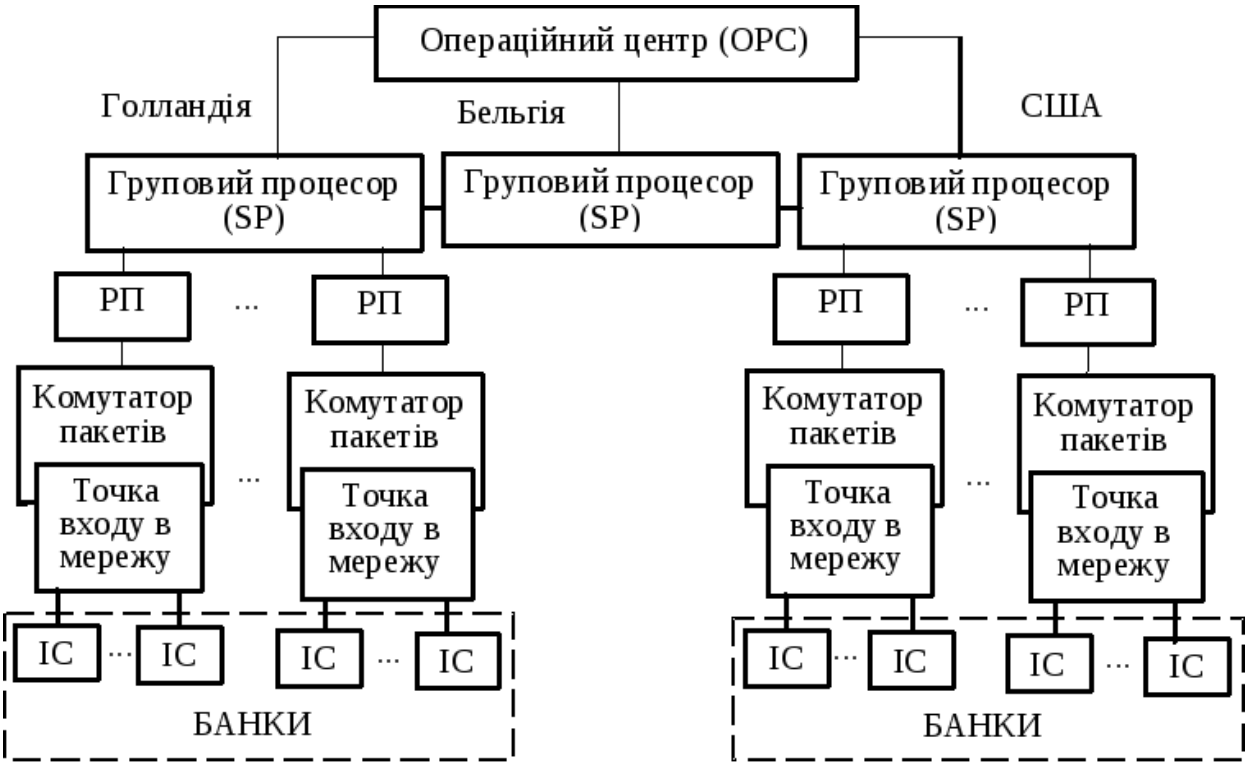

Рис. 8.1. Архітектура SWIFT

Система SWIFT має багаторівневу архітектуру. На нижньому рівні знаходяться банківські установи, де встановлені інтерфейсні системи (ІС), за допомогою яких вони підключаються до мережі. SWIFT пропонує своїм користувачам цілий спектр ІС. Користувачі можуть запропонувати свій варіант ІС, але вона обов’яз-ково погоджується з SWIFT.

Наступний рівень — це регіональні процесори (РП), що розміщені в більшості країн, банки яких вступили в SWIFT. До одного регіонального процесора може бути підключена довільна кількість інтерфейсних систем. Регіональні процесори виконують прийом та перевірку повідомлень користувачів системи і передають їх для подальшої обробки на груповий процесор (SP). Груповий процесор здійснює розподіл повідомлень за адресами по регіональних процесорах, виконує зберігання, архівування та пошук повідомлень, а також генерацію системних звітів. Обмін повідомленнями між РП і SP виконується через світові інформаційні

мережі пакетної комутації. Крім мереж з комутацією пакетів, SWIFT може використовувати більш сучасні технології ATM, Frame Relay і т.п.

На верхньому рівні знаходиться операційний центр, який складається з процесора повідомлень, процесора контролю та центра управління, які виконують моніторинг всіх повідомлень системи.

Говорячи про програмно-апаратну реалізацію системи SWIFT, слід зазначити той факт, що всі можливі варіанти такої реалізації теж чітко стандартизовані. Як інтерфейси різних рівнів для підключення до мережі SWIFT використовуються інтерфейси ST200, ST400 і ST500, які мають різну продуктивність і можуть бути реалізовані на основі різних комп'ютерних платформ.

Програмну реалізацію системи розглянемо на прикладі терміналів системи SWIFT-2. Для них можна використовувати різні модифікації програмного пакета TurboSWIFT фірми MIC Data Corp.

У системі SWIFT застосовується багаторівнева система захисту інформації, що забезпечує гарантії зберігання і конфіденційності переданих даних. Широко використовуються криптографічні методи, що відповідають стандартам ISO.

В силу специфічних вимог, які висуваються до конфіденційності переданої фінансової інформації, мережа SWIFT забезпечує високий рівень захисту повідомлень. SWIFT використовує широкий діапазон профілактичних наглядових заходів для забезпечення цілісності і конфіденційності її мережного трафіку, безперебійного забезпечення доступу до її послуг користувачам. Забезпеченню безпеки сприяє системний підхід, у рамках якого для забезпечення інтегральної безпеки системи приділяється увага всім компонентам: програмному забезпеченню, терміналам, технічній інфраструктурі, персоналу, приміщенням. При цьому враховується повний спектр ризиків від захисту від шахрайства до мінімізації вразливості фізичних ресурсів від наслідків неавторизованого доступу і навіть від природних і техногенних катастроф.

За організацію безпеки та за надійність роботи в мережі SWIFT несе відповідальність Генеральна Інспекція – група спеціалістів, до обов'язків якої входить перевірка діяльності в мережі. Крім цього, періодично проводяться перевірки зовнішніми аудиторами безпеки. Крім цілого ряду організаційних заходів для гарантування безпеки на програмному рівні мережа SWIFT автоматично виявляє випадки несанкціонованого доступу або необґрунтованого проникнення в роботу РП. Автоматично фіксуються і аномалії та відхилення від норм параметрів мережі. Додатково до цього кожному повідомленню при його вводі в мережу автоматично присвоюється послідовний вхідний номер, а при виводі – вихідний.

Всі пересилання повідомлень кодуються з використанням шрифтів, які змінюються через випадкові проміжки часу. Система контролю доступу до мережі включає в себе місцеві паролі для вузлів, журнальні файли, в яких зберігається інформація про кожне підключений до мережі та універсальну систему ідентифікації банків – BIC-код.

У SWIFT існує суворий поділ відповідальності між користувачами і Співтовариством за підтримку безпеки. Користувач відповідає за правильну експлуатацію, за фізичний захист терміналів, модемів і ліній зв'язку до пункту доступу і за правильне оформлення повідомлень. Вся інша відповідальність лежить на SWIFT, що відповідає за безупинне функціонування мережі, за захист від несанкціонованого доступу до неї, за захист повідомлень, що пересилаються, від усіх видів впливів після пункту доступу.

Один з важливих елементів забезпечення безпеки – фізична безпека приміщень. Доступ в усі будинки SWIFT суворо контролюється; в операційних центрах персонал має право пересуватися лише у визначених зонах. Розроблено спеціальні інструкції на випадок вторгнення, пожежі, збоїв харчування і т. д. Пункти доступу, які працюють без участі персоналу, контролюються спеціальними системами, що стежать за

входом і за приміщенням, за станом навколишнього середовища і станом устаткування.

Для захисту терміналів передбачене розмежування доступу користувачів на основі паролів, а з 1993 р. – на основі смарт-карток SWIFT висуває суворі вимоги до процедури підключення терміналів до мережі. З метою забезпечення безпеки термінал може бути автоматично відключений самою системою в тому випадку, якщо виявлена перешкода, перервана лінія, або виявлені кількаразові помилки при передачі, повідомлення з неправильним номером і ін. Системою ведеться файл, де автоматично фіксуються усі відключення кожного терміналу, для того, щоб виявити лінії низької якості і некваліфіковане обслуговування терміналів.

Для захисту повідомлень при їхній передачі по лінії зв'язку до пункту, допуску рекомендується використовувати схему підключення за допомогою спеціальних пристроїв шифрування, погоджених з SWIFT.

Безпека комунікацій SWIFT забезпечується шифруванням усіх повідомлень, переданих по міжнародним лініях зв'язку, що робить їх недоступними третім особам. Повідомлення запам'ятовуються також у зашифрованому виді, тому і персонал не може їх прочитати без спеціального доступу.

До програмно-технічних методів захисту відносяться:

– коди підтвердження дійсності повідомлення, створювані під час введення даних спеціальними алгоритмами, що базуються на змісті повідомлень. Хоча алгоритм відомий усім, ключ знає лише відправник і одержувач. Ключі рекомендується змінювати раз у півроку;

– контроль послідовності повідомлень. Повідомленням SWIFT присвоюються унікальні вхідні і вихідні номери в кожному сеансі зв'язку. Вхідні послідовності повідомлень обробляються онлайн процесорами, а вихідні – одержувачами, так що ці номери веріфікуються в процесі прийому і передачі і якщо вони не відповідають очікуваній послідовності,

то повідомлення не тільки не пропускаються, але і відключається термінал користувача. Цей механізм гарантує, що кожне повідомлення не буде знищене або продубльоване. Запобігання передачі помилкових повідомлень, що містять спотворені послідовності незахищені ключами автентифікації, є обов'язком користувача.

Захищеною є і сама архітектура системи (два операційний центри) у системі широко використовується резервування апаратних засобів. Усі канали зв'язку працюють лише з зашифрованою інформацією, а доступ до телекомунікаційного устаткування суворо обмежений.

Передані повідомлення захищаються від можливої втрати при збої в роботі устаткування, в центрах обробки інформації зберігаються копії всіх переданих повідомлень, а факт одержання кожного з них підтверджується індивідуально. При виникненні яких-небудь сумнівів користувач може запросити копію будь-якого відправленого на його адресу повідомлення. З огляду на використання ряду додаткових заходів, включаючи апаратні засоби захисту каналів зв'язку, мережа забезпечує надійний захист інформації від несанкціонованого доступу, втрати чи перекручування.

Безпрецедентні міри безпеки, використовувані в мережі SWIFT і багаторазове резервування технічних засобів дозволили дотепер уникнути будь-яких – серйозних аварійних ситуацій у мережі SWIFT і її несанкціонованого використання.

SWIFT та інформаційна безпека

З технічної точки зору мережа SWIFT собою міжнародну телекомунікаційну мережу, що дозволяє фінансовим організаціям з різних країн підключитися до неї, використовуючи комп'ютери і термінали різних типів, для передачі банківської та фінансової інформації. В системі ухвалений спеціальний формат банківських повідомлень – стандарт, який розвивається за допомогою робочої групи фахівців банків і організацією SWIFT. В системі SWIFT використовуються як міжнародні стандарти,

розроблені ISO, так і стандарти Міжнародної торгової палати (ICC). В результаті розвитку мережі SWIFT утворилася нова мережа – SWIFT-2, яка базується на 4-х рівневої мережевій архітектурі і на системі управління процесорами, що знаходяться в операційних центрах SWIFT.

Логічна архітектура системи SWIFT-2 підпорядковується основним принципам встановленим ISO (Міжнародна організація стандартизації) для взаємодії відкритих систем. Кожен активний компонент архітектури SWIFT-2 називається вузлом. Вузли можуть бути зв'язані між собою:

– прямими виділеними лініями;

– місцевими (міжнародними) комутованими лініями;

– локальними мережами;

– супутниковими каналами зв'язку.

Архітектура системи складається з чотирьох основних компонентів:

– SCP (процесор управління системою);

– SP (комутаційний процесор);

– RP (регіональний процесор);

– CP (процесор передачі).

Фактично вся система SWIFT-2 зосереджена в двох Центрах управління системою (SCC), які розташовані в Zoeterwoude недалеко від Leiden в Netherlands і в Culpeper (USA). SCC включає в себе дві ключові компоненти системи, а саме SCP і SP. Для поліпшення працездатності і захисту від збоїв в системі SWIFT-2 застосовується дублювання кожного SCP і резервування роботи кожного SP. У будь-який час тільки один SCP є активним і здійснює безпосереднє управління системою. Решта три SCP постійно знаходяться в резерві і безперервно оновлюють свої статки за даними конфігурації активного SCP.

Процесор управління системою SCP відповідає за функціонування всієї системи в цілому. Він постійно контролює і управляє всіма активними компонентами системи, також як і всім доступом до системи в цілому. У функції управління SCP входить:

– дозвіл відкриття нового сеансу і зберігання даних сеансу;

– поширення нового програмного забезпечення по системі;

– функціональний контроль всіх технічних і програмних засобів;

– збір діагностичної інформації про несправності;

– управління процесом відновлення після помилки;

– динамічний розподіл системних ресурсів.

Комутаційні процесори SP керують маршрутизацією і зберіганням повідомлень. Основні функції SP:

– маршрутизація повідомлень між користувачами через RP;

– надійне зберігання двох копій всіх оброблених даними SP повідомлень (на двох різних носіях) і відповідної їм передісторії доставки;

– формування підтверджень про зберігання, доставку оброблених даними SP повідомлень або їх недоставки;

– обробка вибірки повідомлень.

Регіональний процесор RP здійснює логічне підключення користувачів до мережі SWIFT-2 і, по суті, є вхідною і вихідною точкою системи. Програмне забезпечення RP, взаємодіючи з програмами користувача, здійснює точне і безпечне логічне підключення до SWIFT-2. У його функції входить:

– перевірка вхідних повідомлень до пересилання в SP;

– обробка протоколів прикладного рівня;

– контроль і перевірка номерів вхідної послідовності (ISN) всіх повідомлень;

– верифікація контрольних сум повідомлень;

– формування позитивних (ACK) і негативних (NAK) підтверджень прийому повідомлень.

Кожен RP обслуговує конкретну країну або територію і розташований в безпечних (з контролем доступу) центрах. Для кожного користувача системи, відомого по його фізичному адресою, призначається його основний RP, який і буде здійснювати обслуговування даного

користувача. Процесор передачі CP забезпечує зв'язок між RP і іншими вузлами системи, тим самим дозволяючи RP, підключеному до власного SP, приймати інформацію від інших SP.

Для того щоб отримати фізичний доступ до системи SWIFT-2, індивідуальні користувачі повинні мати комп'ютерний термінал (CBT), який підключається до системи SWIFT-2 через ряд місцевих вузлів підключення, відомих як точки доступу до системи SWIFT-2 (SAP) або віддалені точки доступу (RAP).

До складу SAP / RAP входять:

– процесор, що виконує функції управління лініями користувача і лініями підключення SAP / RAP до транспортної мережі SWIFT-2 (STN);

– порти надаються користувачам.

Доступ до послуг SWIFT-2 через SAP або RAP забезпечується STN, що працює під комунікаційним протоколом X.25. Різниця між SAP і RAP полягає в забезпеченні рівня безпеки, хоча вони забезпечують однакові доступи до послуг SWIFT-2 через SAP або RAP забезпечується STN, що працює під комунікаційним протоколом X.25. Різниця між SAP і RAP полягає в забезпеченні рівня безпеки, хоча вони забезпечують однакові операційні можливості по роботі з декількома окремо підключеними користувачами. Якщо через проблеми на лінії зв'язку або несправності SAP (RAP) користувач не може увійти в систему в його основний SAP (RAP), то альтернативний вхід в систему може бути проведений в інший SAP (RAP).

Підключення користувачів до мережі SWIFT-2 можливо через виділені лінії зв'язку, через Загальні мережі передачі даних (PDN) або через PSTN (комутовані лінії), підключені до точки доступу.

Підключення виділених ліній є у всіх SAP зі швидкістю передачі даних по лініях 2400,4800 і 9600 біт / сек. Для даного типу підключення характерно, що користувачеві виділяється окремий порт на точці доступу.

Для даного типу підключення за бажанням користувача може використовуватися шифрування.

Підключення через PDN можливо тільки зі швидкостями еквівалентними швидкостям виділених ліній. Підключення користувача до PDN забезпечується за допомогою виділених ліній з використанням протоколу X.25. Для даного типу підключення передбачається обов'язкове шифрування даних згідно з протоколом X.25.

В системі SWIFT-2 є два типи підключення через комутовані лінії (PSTN):

– через порти PSTN спільного використання, до яких всі користувачі мають доступ на основі суворої конкуренції. Швидкість роботи через ці порти не більше 2400 біт / с і засоби шифрування не застосовуються;

– через виділені порти (для кожного користувача свій) зі швидкістю передачі даних до 9600 біт / с і можливістю (за бажанням користувача) застосовувати засоби шифрування інформації.

Для реалізації комплексного підходу забезпечення інформаційної безпеки сукупність апаратно – програмних і організаційно – технічних засобів і заходів, що реалізують систему безпеки, повинні утворювати розподілений комплекс, що функціонує під управлінням центрів управління безпекою (ЦУБ) мережі.

Для функціонування ЦУБ необхідна розробка і реалізація програмно – технічних засобів управління мережею, розробка нормативно – технічної документації, інструкцій і правил, що визначають порядок дій з управління мережею і роботі користувачів в ній.

Конкретна реалізація зазначених принципів має забезпечувати захист:

– від порушення функціонування телекомунікаційного середовища шляхом виключення впливу на інформаційні канали; канали сигналізації, управління і віддаленого завантаження баз даних комутаційного обладнання, системне і прикладне програмне забезпечення;

– від несанкціонованого доступу до інформації шляхом виявлення і ліквідації спроб використання ресурсів мережі, що призводять до витоку інформації, порушення цілісності мережі та інформації, зміни функціонування підсистем розподілу інформації, доступності баз даних;

– від руйнування вбудованих і зовнішніх засобів захисту шляхом забезпечення шифрування та імітозахисту переданої і збереженої інформації, можливості доказу неправомірних дій користувачів і обслуговуючого персоналу мережі.

Також необхідно відзначити, що при побудові систем інформаційної безпеки в кредитно-фінансових організаціях необхідно враховувати наступні принципи, які в багатьох випадках послужать причинами відхилення організацій від методів і правил побудови аналогічних систем в державних структурах:

– витрати на побудову систем захисту не повинні перевищувати величину гіпотетично можливої шкоди;

– політика відкритості суперечить політиці забезпечення інформаційної безпеки.

Відділ Головного інспектора системи SWIFT-2 (CIO) управляє всіма питаннями, пов'язаними із забезпеченням безпеки роботи мережі SWIFT-2. Користувачам рекомендується забезпечувати належну безпеку процедур, що здійснюються в їх власних організаціях, наприклад, контроль доступу до терміналів SWIFT-2, управління їх підключенням і використанням.

РОЗДІЛ 9. БЕЗПЕКА ДАНИХ В МЕРЕЖІ БАНКОМАТІВ

Система банкоматів

Банкомат (скорочення від «банківський автомат», іноді АТМ, від англ. automated teller machine — «автоматичний касовий апарат») — електронний програмно-технічний комплекс з вмонтованим спеціалізованим комп'ютером, призначений для здійснення автоматизованих операцій видачі наявних грошових коштів, зокрема з використанням платіжних карток, передачі розпоряджень банку про перерахування грошових коштів з банківського рахунку клієнта та виконання інших операцій: оплати товарів, послуг; для автоматизованого складання документів, що підтверджують відповідні операції. Інколи банкомати можуть також мати функцію прийому грошових коштів, в такому випадку вони називаються депозитними банкоматами.

Принцип дії банкомату наступний, після завантаження карти в кардридер банкомата тримачу карти пропонується ввести секретний код (Пін-код) для авторизації картотримача. Далі пропонується вибір доступних операцій (при виборі операції також може запитуватися Пін-код; це залежить від конкретних налаштувань конкретного банкомата). Після вибору операції банкомат шифрує отриману інформацію (уміст магнітної смуги/чипа, уведений Пін-код, запитану операцію) і передає дані в процесинговий центр банку-банка-екваєра.

Банк-Екваєр відправляє в платіжну систему запит на проведення операції. Платіжна система маршрутизує запит у банк-емітент (банк, що видав карту) і, одержавши згоду або відмову (код авторизації), передає банкомату команди на виконання або відхилення запиту. При цьому всі дії по відправленню запиту, обробці відповіді на запит, видачі/прийманню грошей з касет фіксуються, що дозволяє провести розслідування у випадку, якщо операція оскаржена. Тому що Пін-код відомий тільки

тримачу карти, операції, підтверджені Пін-кодом, уважаються виконаними безпосередньо тримачем карти.

В останні роки, одночасно з розвитком банкоматної мережі, росте кількість випадків **банкоматного шахрайства** – неправомірного використання банкоматів для крадіжки грошей з рахунків тримачів пластикових карт.

Існує кілька десятків різних по організації й технологічному рівню способів неправомірного заволодіння грішми з карткового рахунку іншої людини за допомогою банкоматів. По даним APACS (Association for Payment Clearing Services — Асоціація систем клірингових платежів – Великобританія), найпоширеніші наступні:

– Використання украденої карти й Пін-коду, розголошеного тримачем.

– «Дружнє шахрайство». Використання карти шляхом вільного доступу членами родини, близькими друзями, колегами по роботі. Також припускає розголошення Пін-коду.

– Величезна черга біля банкомата, повна відсутність таємності введення Пін-коду.

– Підглядання Пін-коду через плече з наступною крадіжкою карти – найпростіший, але широко розповсюджений метод.

– «Ліванська петля». Блокується вікно подачі карти так, щоб карта застрягла. При спробі вставити карту в банкомат вона застряє. Зловмисник, що попередньо підглянув Пін-код, співчуває й рекомендує терміново йти й дзвонити в банк або сервісну службу. Як тільки власник відходить, злочинець витягає карту, звільняє вікно банкомата й знімає гроші.

– Фальшиві банкомати. Досить рідкий спосіб, що вимагає технічної оснащеності. Шахраї виготовляють фальшиві банкомати, які виглядають як справжні, або переробляють старі, і розміщають їх у людних місцях. Такий банкомат приймає карту, вимагає введення Пін-коду, після чого видає повідомлення про неможливість видачі грошей (під приводом

відсутності грошей у банкоматі або технічної помилки) і повертає карту. У банкоматі відбувається копіювання даних з карти й Пін-коду, що дозволяє шахраям згодом виготовити дублікат і зняти з його допомогою гроші з рахунку клієнта.

– Копіювання магнітної смуги (skimming) за допомогою підставних пристроїв зчитування. Такі пристрої встановлюють на банкомат (зчитувач — на щілину для приймання карти, додатковою клавіатурою накривають справжню). При користуванні таким банкоматом зчитувач зберігає дані з, що вставляються в банкомат карт, а клавіатура — Пін-коди. Як і в попередньому випадку, украдених даних досить для виробництва дубліката карти й зняття грошей з рахунку власника.

– Неправильний ПІН-ПАД (пристрій для введення Пін-коду в платіжних терміналах), або додатковий елемент на електронному замку в приміщенні з банкоматом, що відкривається за допомогою карти.

– Установка поруч із банкоматом мініатюрних телекамер для злодійства Пін-кодів. Така камера може бути замаскована встановленим рядом або прикріпленим до банкомата або стіни поруч із ним предметом.

Деякі із цих методів є апаратними закладками у банкоматах.

В 2011 році з'явилися повідомлення про ще один теоретично можливий спосіб злодійства Пін-кодів за допомогою банкомата: за допомогою високочутливої інфрачервоної камери. Зловмисник, що чергує в черзі, робить знімок клавіатури, на якій попередній користувач набирав Пін-код. Клавіші, до яких доторкалися, трохи тепліші, причому остання натиснута клавіша тепліше передостанньої і так далі. Успішність даного методу, втім, залежить від типу клавіатури (металеві клавіатури мають більшу теплопровідність і температура їх клавіш швидко вирівнюється) і від того, чи набирав клієнт що-небудь ще на клавіатурі (наприклад, суму). Для запобігання зняття Пін-коду по тепловому відбиткові досить після роботи із клавіатурою на короткий час покласти на неї долоню.

Поширеність

Масштаби банкоматного шахрайства у світі вже зараз дуже великі, втрати від нього в США склали 2,79 млрд доларів за рік на кінець травня 2005 року (Gartner), у Великобританії за 2006 рік— 61,9 млн ф.ст. У країнах Латинської Америки кількість злочинів, пов'язаних з банкоматами, з 2001 по 2005 р. виросло на 15 %. У Східній Європі й колишньому СРСР проблема стоїть менш гостро через менший обсяг використання електронних платіжних засобів, але, проте, рівень пов'язаних з електронними картами злочинів також росте. За офіційним даними, втрати від шахрайства на Україні становлять до 0,06 % річного обороту по картах (90 млн гривень в 2006). За неофіційними оцінками фахівців Національного банку України в реальності ця величина становить до одного відсотка всього обороту по картах, тобто фактичний обсяг злодійства за 2006 рік склав близько мільярда гривень.

Банкоматна мережа – це сукупність АТМ, установлених у філіях банків, торговельно-сервісних підприємствах або на території корпоративних клієнтів банків, і каналів передані даних, що зв'язують термінальні пристрої з процесинговим центром банків.

Є два шляхи, яких може дотримуватися банк, обираючи стратегію використання банкоматів:

– експлуатація незалежної власної мережі обслуговування;

– участь у спільній мережі обслуговування.

Перевага власної системи в тому, що власник зберігає над нею повний контроль. Крім того, вона забезпечує фінансовій установі престиж і незалежність від загальнонаціональних систем.

Недоліком є те, що створення мережі банківських автоматів-касирів і маркетинг вимагають значних витрат, обсяг її операцій обмежений, оскільки вона здатна обслуговувати лише операції власників карток певного виду, які проходять через цю установу.

Для підвищення економічності використання банківських автоматів банки об'єднують свої мережі і надають можливість клієнтам користуватися автоматами різних банків на великих територіях.

Спільна мережа банкоматів – це спільне підприємство кількох фінансових установ.

Учасники спільної мережі ставлять перед собою такі цілі:

– поділ витрат і ризику між учасниками мережі в разі впровадження нових послуг;

– зменшення вартості операцій для учасників.

Тож і для клієнта є два можливі варіанти використання банківських автоматів для видачі готівкових грошей і здійснення стандартних фінансових операцій. Клієнт за допомогою своєї картки може отримати гроші в автоматі, установленому банком, який його обслуговує. У цьому разі банк несе витрати тільки на обслуговування свого автомата, а з клієнта за цю операцію стягує невелику плату. Або клієнт одержує гроші в автоматі, що належить іншому банку, якщо існують міжбанківські зв'язки в цій сфері; у цьому разі банк, який видав картку, платить комісійний збір за "міжбанківський обмін", а пізніше стягує цю суму зі свого клієнта.

Використання банкоматів вимагає великих інвестицій, тому їх використовують переважно великі банки. Показником для оцінки ефективності використання банкоматів можна вважати кількість використовуваних платіжних карток на один банкомат.

"Безкоштовні" мережі банкоматів. Наявність сьогодні розвинутої мережі банкоматів вимагає стратегічного плану подальшого розвитку цього напряму банківської діяльності. Банківський ринок суттєво змінився – сьогодні, окрім банків, кредитні спілки і супермаркети також розвивають власні мережі банкматів. За прогнозами, уже найближчим часом відбудеться зниження обсягів трансакцій із розрахунку на один банкомат. Отже, надання послуг еквайрингу вже сьогодні не є великою конкурентною перевагою банків.

На противагу переважній кількості банків, які ввели комісійний збір для небанківських клієнтів для компенсації потенційних збитків, можна зіткнутися з принципом розгляду банкомата лише як зручності для клієнта, а не як джерела доходу або конкурентної переваги. Ідеться про "безкоштовні" мережі банкоматів – вигідні як для банків, так і для клієнтів.

Поняття безпеки банкоматів

Підсистема «АТМ-Інтелект» платформи «Інтелект» дозволяє включити в комплекс безпеки банку розподілену систему охорони банкоматів. У таку систему входять локальні відеоохоронні системи банкоматів і централізовані робочі місця, що дозволяють оперативно отримувати тривожні повідомлення від банкоматів, повідомлення про технічні неполадки локальних систем і відеокадри. Спеціалізований інтерфейс дозволяє вести претензійну роботу по операціях на будь-якому банкоматі віддалено, без виїзду на об'єкт. Одне з ключових переваг системи «АТМ-Інтелект» – здатність працювати за штатними захищеним низькошвидкісних каналах зв'язку банкоматів.

«АТМ-Інтелект» дозволяє ефективно вирішувати завдання, пов'язані з експлуатацією та безпекою мережі банкоматів:

– контроль стану обладнання банкомату і локальної системи безпеки в режимі реального часу;

– захист банкоматів від дій зловмисників і вандалів, оперативна реакція на тривоги;

– швидкий розбір інцидентів за операціями на банкоматі без виїзду на об'єкт для знімання архіву.

В структуру системи «АТМ-Інтелект» входять наступні компоненти:

– локальні відеоохоронні системи (ЛВОС) банкоматів;

– пульти дистанційного відеоконтролю (ПДВ);

– центральний пульт дистанційного відеоконтролю (ЦПДВ);

– пульт контролю технічного стану (ПКТС).

Локальна відеоохоронна система захисту банкоматів

Локальна відеоохоронні система (ЛВОС) встановлюється безпосередньо в банкоматі і здійснює запис з відеокамер банкомату. Ця система отримує від ПЗ банкомату інформацію про транзакції і сигнали від датчиків банкомату і синхронізує ці дані з відеозаписом. Система передає на пульт дистанційного відеоконтролю (ПДВ) і пульт контролю технічного стану (ПКТС) тривожні повідомлення, а також дані про технічний стан свого обладнання і устаткування банкомату. Локальна система отримує запити від ПДВ, виробляє відповідно до них пошук відеокадрів або відеофрагментів і передає їх на ПДВ.

Функції локальної відеоохоронні системи:

- Відеозапис:

  – безперервна;

  – по детектору руху;

  – по спрацьовуванню охоронних датчиків банкомату;

  – по сигналу від ПЗ банкомату.

- Інтеграція з ПЗ банкомату:

– синхронізація даних транзакцій з відеозаписом і віддалений доступ до архіву системи відеоспостереження;

– синхронізація часу банкомата і відеомагазину;

– можливість активації відеозапису при здійсненні транзакції;

– можливість перегляду відеозображення з камер безпосередньо на моніторі банкомату (опціонально).

- Прийом, обробка та реєстрація сигналів від датчиків банкомату:

  – датчик відкриття сервісної зони;

  – датчик відкриття сейфової зони;

  – термодатчик;

  – вібродатчик;

  – датчик відкриття сейфа під примусом.

- Прийом, обробка та реєстрація сигналів від антіскіммінгових пристроїв.
- Передача повідомлень на ПДВ і ПКТС:

  – передача повідомлень про стан компонентів;

  – передача на ПДВ відеокадрів або відеофрагментів за запитом;

  – робота по штатним захищеними каналами зв'язку банкомату.

Пульт дистанційного відеоконтролю (ПДВ) є робоче місце, на екрані якого відображається інформація від локальних відеоохоронні систем. ПДВ має спеціальний інтерфейс, який дозволяє на одному моніторі наочно відображати стан безлічі банкоматів. Також пульт дистанційного відеоконтролю дозволяє вести віддалений пошук відеозаписів в архівах підключених до нього ЛВОС за часом і за даними транзакцій, що використовується, зокрема, для ведення претензійної роботи. Функції пульта дистанційного відеоконтролю:

– Прийом, реєстрація та візуалізація тривожних повідомлень і відеокадрів, що надходять від ЛВОС;

– Прийом, реєстрація та візуалізація повідомлень про стан компонентів ЛВОС;

– Формування і передача запитів на пошук відеоінформації в архіві ЛВОС;

– Контроль технічного стану системи відеоспостереження банкомату.

Центральний пульт дистанційного відеоконтролю (ЦПДВ) – це робоче місце, на якому зберігається довідкова інформація про всі компоненти відеоохоронні системи безпеки. Через пульт дистанційного відеоконтролю можна звертатися до прецесингового центру банку для отримання звідти інформації про транзакції і завантаження нормативно-довідкової інформації. Тут можна отримувати статистичні звіти для аналізу роботи відеоохоронної системи і її окремих компонентів, а також для контролю роботи операторів ПДВ. Центральний пульт дистанційного

відеоконтролю дозволяє вести централізований пошук відеоданих в усіх локальних системах без виїзду на об'єкт, що забезпечує високу ефективність обробки запитів ЦСКО, МВС і служби інкасації.

Пульт контролю технічного стану – це робоче місце, на якому відображається тільки технічний стан компонентів відеоохоронної системи і не відображається відео. Тому пульт може розташовуватися і в відділенні банку, і в офісі сервісної організації, що займається обслуговуванням відеоохоронні системи безпеки. Це забезпечує високу швидкість і надійний контроль виконання заявок на усунення технічних неполадок.

Пульт контролю технічного стану забезпечує:

– Контроль технічного стану компонентів ЛВОС і ПДВ.

– Контроль розміру відеоархівів ЛВОС.

– Контроль справності каналів зв'язку.

– Контроль температури всередині банкоматів.

– Формування заявок на сервісне обслуговування компонентів ЛВОС і контроль їх виконання.

РОЗДІЛ 10. БЕЗПЕКА ДАНИХ В МОБІЛЬНИХ ПРИСТРОЯХ

Кібербезпека мобільних та дистанційних телекомунікацій

Широке застосування мобільних пристроїв і технології хмарних сховищ висуває підвищені вимоги до безпеки мобільних і дистанційних телекомунікацій, збереження і захисту корпоративних даних, в тому числі від несанкціонованого поширення цієї інформації. При використанні технології хмарних сховищ за моделлю на віддалених серверах і центрах опрацювання даних провайдера зберігається критично важлива для підприємства інформація, наприклад фінансовий звіт. Багато керівників дублюють її на своїх персональних мобільних пристроях, що знижує рівень інформаційної безпеки підприємства. В цьому випадку потрібно передбачити заходи щодо захисту або знищення цих даних при втраті або крадіжці мобільного пристрою. Передача інформації по незахищених каналах зв'язку також може привести до катастрофічних наслідків.

Мобільні засоби часто використовуються поза контрольованої зони корпоративного зв'язку. Вони є об'єктами крадіжки і зараження шкідливими програмами з метою викрадення грошових коштів або цінної інформації, здійснення хакерських атак, спрямованих на нанесення економічної або моральної шкоди компанії. Щоб захиститися від таких загроз, недостатньо антивірусних програм, що встановлюються на мобільні пристрої. Убезпечити може тільки комплексна система забезпечення інформаційної безпеки корпоративного класу.

Одним з рішень захисту трафіку мобільних пристроїв є послуга оператора зв'язку "Мобільний VPN". В цьому випадку весь трафік мобільних пристроїв передається по закритих каналах оператора зв'язку і не потрапляє в Інтернет, що виключає ризик перехоплення нею зловмисниками.

Для мобільних користувачів інформаційна безпека забезпечується:

– готовими рішеннями, які встановлюються на мобільний апарат, щоби обмежити можливість витоку інформації;

– засобами, що надають захищене взаємодія співробітників з офісом компанії;

– засобами, що дозволяють реалізувати віртуальне робоче місце на мобільному терміналі з можливістю централізованого управління його безпекою;

– ефективним застосуванням вже існуючих сертифікованих засобів захисту.

Як відповідь на серйозну і обґрунтовану стурбованість з приводу безпеки мобільних пристроїв з'явилися нові комплексні захисти всього периметра інформаційної інфраструктури з урахуванням мобільності.

Загрози втрати інформації з мобільних пристроїв

Перш за все, всім користувачам, які користуються мобільними телефонами, а особливо смартфонами, дуже важливо розуміти, що той пристрій, який вони носять у себе у кишені, це повноцінний комп’ютер з функцією постійного доступу до мережі Інтернет, мікрофоном, камерою, GPS-навігатором і приєднаним до нього одним або декількома різними гаманцями. Тобто, є власний мобільний рахунок у оператора і додатково прив’язана банківська карта. Всі ці рахунки можуть бути використані зловмисникам.

Хочу звернути Вашу увагу на те, що для смартфонів характерні ті ж самі загрози, що і для персональних комп’ютерів, оскільки телефон, по суті, і є комп’ютером. Це обумовлює і можливість запуску "троянських" програм, і шпигунство за Вами, і крадіжку конфіденційної інформації, крадіжку грошей з Ваших мобільних рахунків.

"**Троянські" програми.** На жаль, нам властиво не думати про безпеку мобільних пристроїв. І якщо на комп’ютері використання антивірусу є вже нормою, то на мобільних пристроях це все ж ще щось

екзотичне. Сьогодні існує величезна кількість загроз: віруси, троянські програми, мережеві хробаки, рекламні модулі орієнтовані на абсолютно різні платформи для мобільних пристроїв.

Шпигунські програми. Ці програми відносяться до класу легальних шпигунських програм. Зверніть увагу – «легальних» шпигунських програм. Це програми, що можна вільно придбати. У програм є технічна підтримка, власний сайт, офіційний власник, програму можна досить просто видалили з приладу. Тільки подумайте, подібну програму можна вільно придбати, встановити на пристрій користувача і спокійно за ним стежити. Тобто перехоплювати інформацію про всі здійснені дзвінки, показувати вміст sms-листування, показувати інформацію про відвідувані сайти, знімати за допомогою камери телефону оточуючу ситуацію, визначати Ваше місцерозташування, сканувати bluetooth чи Wi-Fi оточення, включати мікрофон і записувати інформацію про все навкруги. Встановлення подібного додатку на телефон користувача, по суті, дозволяє шпигувати за ним всюди, адже телефон практично завжди з нами. Слідкувати можна не лише в плані дій в самому телефоні, але і за безпосереднім оточенням користувача – реальним життям, де він перебуваєте, що бачить, що говорить.

Дещо про **історію розвитку мобільних вірусів**. Перші мобільні віруси не можна було навіть назвати повністю вірусами, це були більше шкідливі sms-повідомлення, тобто на телефон користувача приходило певне sms-повідомлення і якщо його відкрити – це призводило до збою роботи телефону і могла призвести до зависання телефону, була спроможна «обнулити» телефонну книгу, здійснити певний дзвінок, тобто телефон виконував певну не потрібну користувачу функцію. Далі з’явились реальні віруси і хробаки. Перші віруси з’явились ще для комунікаторів на операційних системах Palm OS, Windows CE, Windows Mobile. Далі їм на заміну прийшов Symbian, для якого також було створено досить багато шкідливих програм, повноцінних хробаків, що мали

можливість розповсюджуватись від одного пристрою до іншого використовуючи bluetooth з'єднання і виконувати шкідливі дії.

Цікаво, що тоді розповсюдження хробаків було в основному побудовано на методах соціальної інженерії. Наприклад смартфон на базі Symbian, заражений хробаком, що розповсюджується через bluetooth. Радіус дії bluetooth передачі 10-15 метрів, при цьому автоматичної передачі не відбувається. Тобто заражений смартфон сканував оточення знаходив інші телефони із увімкненим bluetooth і намагався їм розіслати копії себе. Що ж відбувалось на стороні яка приймала? Звичайний користувач перебував у метро чи кафе і бачив на телефоні пропозицію прийняти певний файл. Ця ситуація була не висвітлена у ЗМІ і звичайної цікавості вистачало щоби прийняти файл, тим більше він міг цікаво називатись. Людина приймала файл, відкривала його із цікавості і якщо приймаючий прилад був на базі Symbian, хробак активізовувався, заражав пристрій і потім заражав інших, виконуючи нову розсилку.

Перші модифікації вірусу просто розмножувались і наносили певну шкоду, блокуючи деякі додатки у смартфоні. Більш пізніші модифікації хробака вже намагались заробляти кошти зловмисникам, тобто вірус розповсюджувався так само через bluetooth, але вже мав нову функцію – відправка sms на платні номери. Для цього зловмисники реєстрували короткі платні номери при відправці sms-повідомлень, за відправлення яких з користувача знімаються певні кошти. І троянська програма з Вашого зараженого пристрою відправляла sms-повідомлення, а зловмисники таким чином отримували зиск.

У подальшому мобільні пристрої почали володіти все більшою можливістю з'єднання з Інтернет. З початку це були WAP та GPRS з'єднання, потім з'явились 3G мережі, далі повноцінні Wi-Fi точки. В теперішній час є дуже багато місць де не підключаючись через свого GSM-оператора можна отримати доступ до глобальної мережі через Wi-Fi, що присутній практично всюди: в офісах, метро, кафе, вдома і т.д. Маючи

доступ до Інтернет хробаки отримали можливість, перш за все, більш швидко розповсюджуватись через електронну пошту, веб-сайти і наносити більш суттєву шкоду, адже вони вже могли не тільки відправляти платні sms-повідомлення, але й красти дані кредитних карток про акаунти в соціальних мережах, електронній пошті і т.д. Віруси для мобільних пристроїв отримали всі ті властивості, що притаманні класичним шкідливим програмам для персональних комп'ютерів.

Для того щоби провести аналогію, можна зазначити, що існує багато "троянських" програм, що заражаючи телефон, перетворюють його на бота і формують цілу бот-мережу. Існують бот-нети на основі мобільних пристроїв.

Так, у 2012 році у Китаї був виявлений бот-нет, що складався із 1,5 мільйона заражених пристроїв. Кожен із цих пристроїв міг або відправити sms-повідомлення на певний номер, або провести DDoS-атаку, СПАМ-розсилку. Таким чином DDoS-атаки на сайти можуть проводитись не тільки з заражених комп'ютерів, але й з заражених смартфонів, які по суті є тими самими комп'ютерами, але які ми постійно носимо з собою.

Класичні віруси для мобільних пристроїв, в основному, не розробляються. Переважно для мобільних пристроїв розробляють троянські програми, рекламні модулі, бекдор програми.

Варто розуміти, що шкідливі програми створюються для всіх операційних систем, на які можна встановити додаткове програмне забезпечення. Тобто якщо у Ваш телефон можна встановити додаткові програми, значить туди може потрапити шкідлива програма. Якщо вона не потрапить туди самостійно, автоматично, то програма може зробити це з Вашою допомогою через методи соціальної інженерії. Наприклад, Вам запропонують встановити цікаву гру, а це виявиться і гра, і шкідлива програма. Або взагалі вона не буде маскуватись під гру, а просто почне надсилати sms-повідомлення на короткі номери. Тільки пристрої з повною забороною на встановлення додаткового ПЗ є захищеними. Віруси, у

широкому сенсі, для операційної системи iOS, на жаль, існують і у досить великій кількості.

Тут скоріше стоїть питання яким чином ці шкідливі програми можуть проникнути на Ваш мобільний пристрій. І в цьому плані служба App Store дійсно більш захищена ніж служба Google Play Market. Але тут є і зворотня сторона. Як правило, користувачі мобільнихпристроїв iPhone не готові до того що їх прилади можуть заражатись вірусами. Якщо для Android-пристроїв хоча б частина юзерів користуються антивірусами, то у разі виникнення епідемії вони можуть бути захищені набагато швидше. Користувачі ж операційної системи iOS пристроїв змушені будуть чекати поки служба Apple випустить оновлення операційної системи, що усуне вразливість.

Ще один аспект загроз для користувачів мобільних телефонів полягає у моделі роботи з платними послугами, що можуть бути не зовсім зрозумілі користувачу. Тобто Вас можуть ввести в оману попросивши набрати певний номер, надіслати sms-повідомлення. У всіх цих випадках з мобільного рахунку знімаються певні кошти. Також дуже популярною є послуга sms-підписок, коли користувачу пропонують підписатись на певний сервіс за допомогою sms-повідомлень. Це може бути все що завгодно: підписка на он-лайн гру, певний сайт, будь-який сервіс, який вимагає регулярну оплату. У подальшому користувач може забути про це. Оскільки він лише один раз погоджується, а потім ініціювання зняття коштів буде відбуватись вже оператором. З вашого рахунку періодично буде зніматись певна сума коштів і ви цього можете навіть не помічати. Інколи ми просто не пам’ятаємо на що підписалися, а, можливо, і взагалі цього не робили – бо це зробила "троянська програма". Тому варто бути дуже обережним під час використання коротких sms-повідомлень при замовленні послуг через них. Не дзвоніть на не знайомі номери і уважно контролюйте послуги, на які Ви підписуєтесь. Інколи підписка на послугу може коштувати 5 гривень, а вже за те, щоби відписатись потрібно

заплатити 25 грн. Тому, варто бути якомога більш уважними і не користуватись підозрілими сервісами.

РОЗДІЛ 11. ПОЛОЖЕННЯ ПРО ЗАХОДИ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ

Вимоги до кібербезпеки в банківській системі. Вимоги до банків, та до впровадження СУІБ

Виділяють такі вимоги до інформаційної безпеки в банківській системі України:

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

2) принципи управління інформаційною безпекою;

3) вимоги до інформаційних систем банку, що взаємодіють з інформаційними системами Національного банку України, з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах Національного банку.

У цьому Положенні терміни та поняття вживаються в таких значеннях:

1) багатофакторна автентифікація – автентифікація, яка здійснюється за допомогою захищених механізмів двох або більше типів;

2) зловмисний код – комп'ютерна програма/комплекс комп'ютерних програм або частина програмного коду інформаційної системи, що впроваджується за участю користувача або виконується автоматично, створює загрозу або умови для реалізації загрози порушення штатної роботи обладнання банку та/або порушення конфіденційності, цілісності, доступності інформації, яка обробляється в інформаційних системах банку;

3) критичні бізнес-процеси банку – бізнес-процеси діяльності банку, визначені банком критичними щодо інформаційної безпеки за результатом

їх оцінювання банком за такими критеріями: конфіденційність, цілісність, доступність;

4) мережа банку – комплекс технічних засобів телекомунікацій, призначених для маршрутизації, комутації, передавання та/або приймання інформації дротовим та/або бездротовим зв'язком між кінцевим обладнанням усередині периметра банку;

5) мінімальний рівень повноважень – повноваження та права доступу, 1мінімально необхідні для якісного виконання персоналом банку службових обов'язків;

6) пристрої уніфікованого управління загрозами (Unified threat management, UTM) – пристрої, які можуть виконувати кілька функцій безпеки з одного пристрою: міжмережевий екран, запобігання несанкціонованого доступу до мережі, антивірусний шлюз, антиспамовий шлюз, віртуальна приватна мережа (Virtual private network, VPN), фільтрація вмісту, балансування навантаження, запобігання витоку даних;

7) ризик-орієнтований підхід до забезпечення інформаційної безпеки – прийняття управлінських рішень на підставі аналізу порівняння поточних ризиків інформаційної безпеки з прийнятними.

Інші терміни, що вживаються в цьому Положенні, використовуються в значеннях, визначених законами України, нормативно-правовими актами Національного банку та ДСТУ ISO/IEC 27000:2015.

Вимоги до банків.

1. Вимоги цього Положення поширюються на банки. Вимоги розділу III цього Положення також поширюються на небанківські установи – учасників інформаційних систем Національного банку.

2. Принципи забезпечення інформаційної безпеки:

– підхід до забезпечення інформаційної безпеки має бути системним;

– процес удосконалення та розвитку інформаційної безпеки має бути безперервним і здійснюватися шляхом обґрунтування та реалізації

раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;

– заходи захисту від реальних та потенційних загроз інформаційній безпеці банку мають бути своєчасні й адекватні;

– забезпечення належного рівня інформаційної безпеки банку неможливе без підтримки та контролю з боку керівників банку;

– сталий розвиток систем інформаційної безпеки можливий лише в разі забезпечення достатності ресурсів, у тому числі фінансових.

3. Принципи криптографічного захисту інформаційних систем Національного банку:

– криптографічний захист інформації в інформаційних системах Національного банку на ділянці зв'язку між учасником інформаційних систем Національного банку та Національним банком забезпечується застосуванням багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансовий рівень базової еталонної моделі взаємодії відкритих систем (Open systems interconnection basic reference model, OSI/ISO) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку;

– для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовується криптографічний протокол захисту на транспортному рівні (Transport layer security, TLS), забезпечуються контроль цілісності та конфіденційність інформації. Для прикладного рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються такі механізми захисту: ідентифікація/автентифікація підписувача, контроль цілісності та конфіденційність на всіх етапах оброблення інформації;

– залежно від категорії інформації щодо критерію конфіденційності, для забезпечення ідентифікації та автентифікації, використовується

односпрямований або двоспрямований достовірний канал захисту на транспортному рівні;

– інформаційні системи Національного банку підтримують роботу криптографічного протоколу захисту на транспортному рівні останньої версії, але не нижче версії 1.2;

– інформаційні системи Національного банку використовують криптографічні набори захисту на транспортному рівні лише з шифруванням та застосовують симетричні криптографічні алгоритми з довжиною ключа не менше ніж 128 біт;

– Департамент безпеки Національного банку надає криптобібліотеки для криптографічних засобів захисту інформації, рекомендації щодо їх використання та програмне забезпечення генерації ключів.

4. Банк зобов’язаний упровадити систему управління інформаційною безпекою (далі – СУІБ) згідно з ДСТУ ISO/IEC 27001:2015 для визначеної сфери застосування з урахуванням обов’язкових вимог щодо впровадження СУІБ, викладених у розділі ІІ цього Положення

5. Передумовами впровадження СУІБ у банку є:

– упровадження процесного підходу до діяльності банку;

– упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку.

6. Банк зобов’язаний запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку. Банк має право самостійно визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки.

7. Банк зобов’язаний запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов’язкових вимог щодо організації заходів безпеки інформації, викладених у розділах IV і V цього Положення.

8. Банк зобов’язаний визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку. Банк має право розширити сферу застосування СУІБ банку відповідно до особливостей його діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

9. Національний банк має право здійснювати перевірку стану впровадження СУІБ банку та повноту виконання заходів безпеки інформації, що встановлені цим Положенням.

Вимоги щодо впровадження СУІБ:

1. Банк зобов’язаний сформувати колективний керівний орган з питань впровадження та функціонування СУІБ (далі – керівний орган СУІБ) або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити положення про керівний орган СУІБ банку з чітким визначенням його завдань, функцій та відповідальності.

2. Банк зобов’язаний включити до складу керівного органу СУІБ голову правління банку та/або його заступника, що відповідає за інформаційну безпеку банку, керівників підрозділів банку – власників критичних бізнес-процесів банку та керівника підрозділу банку з управління ризиками. Банк має право ввести до складу керівного органу СУІБ інших працівників банку відповідно до потреб, що обумовлені особливостями діяльності банку.

3. Банк зобов’язаний покласти на керівний орган СУІБ обов’язок виконання таких завдань:

– погодження та перегляд політики інформаційної безпеки, положення щодо застосовності та стратегії розвитку інформаційної безпеки банку;

– узгодження впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки банку та заходів інформаційної безпеки;

– розгляд, затвердження та контроль за виконанням проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ банку;

– визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;

– організація практичних заходів щодо підвищення обізнаності/навчання персоналу банку з питань інформаційної безпеки;

– забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.

4. Банк зобов'язаний розробити та впровадити політику інформаційної безпеки, яка має містити:

– цілі інформаційної безпеки;

– сферу застосування політики інформаційної безпеки;

– принципи, правила та вимоги інформаційної безпеки в банку;

– визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки.

5. Банк зобов'язаний забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік. Якщо за результатами перегляду зміни до політики інформаційної безпеки не вносяться, то повторне її затвердження не потрібно.

6. Банк зобов'язаний затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін.

7. Банк зобов'язаний розробити та затвердити стратегію розвитку інформаційної безпеки. Банк має право затвердити стратегію розвитку інформаційної безпеки банку в документі, яким затверджено загальну стратегію розвитку банку, у вигляді окремого розділу. Зміст стратегії має узгоджуватися з політикою інформаційної безпеки банку, основними стратегічними цілями банку, що пов'язані із впровадженням нових бізнес-

процесів/банківських продуктів з використанням технологій, які потребують захисту інформації, а також враховувати планування розвитку інфраструктури банку та заходів інформаційної безпеки для мінімізації ризиків інформаційної безпеки.

8. Банк зобов'язаний розробити та затвердити план забезпечення безперервності діяльності банку, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності банку.

9. Банк має право розробляти документи СУІБ у формі окремих документів або об'єднаних за типом (тематикою) в загальні документи, із зазначенням у них розділів, що відповідають визначеним напрямам (питанням) інформаційної безпеки

Вимоги до криптографічного захисту інформації в інформаційних системах Національного банку

1. Учасники інформаційних систем Національного банку зобов'язані налаштувати системи криптографічного захисту інформації в інформаційних системах Національного банку згідно з вимогами, які визначені у відповідній експлуатаційній документації кожної інформаційної системи Національного банку.

2. Банк зобов'язаний забезпечити захист інформаційних систем банку від несанкціонованого доступу та дій, направлених на відмову в обслуговуванні відповідно до вимог розділу IV цього Положення.

3. Банк зобов'язаний призначити відповідальну особу за інформаційну безпеку банку (Chief information security officer, CISO), яка має повноваження, достатні для прийняття управлінських рішень, та забезпечує:

– стратегічне керівництво з питань інформаційної безпеки банку;

– визначення напрямів розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку банку;

– відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів;

– контроль за впровадженням заходів безпеки інформації в банку.

4. Банк зобов’язаний сформувати підрозділ з інформаційної безпеки не менше як із двох працівників зі складу штатних працівників банку. Підрозділ з інформаційної безпеки банку має безпосередньо підпорядковуватися відповідальній особі за інформаційну безпеку банку.

5. Підрозділ з інформаційної безпеки банку має здійснювати:

– розроблення вимог щодо налаштувань безпеки інформаційних систем банку;

– розроблення або участь у розробленні документів банку щодо інформаційної безпеки;

– контроль за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях життєвого циклу інформаційних систем банку;

– розслідування інцидентів безпеки інформації;

– спільно з підрозділами інформаційних технологій (інформатизації, автоматизації) банку відновлення функціонування інформаційних систем банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

6. Працівникам підрозділу інформаційної безпеки/відповідальній особі за інформаційну безпеку банку забороняється мати повноваження з розроблення, упровадження, супроводження (адміністрування) та експлуатації інформаційних систем банку, крім тих, що використовуються для забезпечення безпеки інформації.

7. Підрозділу інформаційних технологій (інформатизації, автоматизації) банку забороняється бути власником інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності.

8. Банк зобов’язаний ознайомити працівників під час прийому на роботу з політикою інформаційної безпеки банку. Працівник банку

зобов’язаний ознайомитися з політикою інформаційної безпеки банку під підпис та надати зобов’язання про дотримання конфіденційності.

9. Банк зобов’язаний включити до трудового контракту/договору працівника та/або посадової інструкції працівника обов’язки працівника банку щодо виконання вимог із забезпечення безпеки інформації.

10. Банк зобов’язаний ознайомити працівників банку з внутрішніми документами банку, які встановлюють вимоги щодо безпеки інформації. Документи розробляються банком з урахуванням вимог цього Положення. Перелік документів для ознайомлення визначається банком самостійно, з урахуванням принципу мінімального рівня повноважень. Працівник банку зобов’язаний ознайомитися з такими документами під підпис.

11. Банк зобов’язаний упровадити програму підвищення обізнаності/навчання працівників банку з питань безпеки інформації з урахуванням досвіду, отриманого за результатами вирішення інцидентів безпеки інформації.

12. Банк зобов’язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації і мають містити положення щодо:

– контролю за використанням змінних носіїв інформації, уключаючи процедури їх обліку та виведення з експлуатації;

– категорії інформації, яка може оброблятися на змінних носіях інформації;

– ідентифікації змінних носіїв інформації, які використовуються в банку;

– обмежень використання змінних носіїв інформації;

– знищення інформації на змінних носіях інформації перед їх передаванням у користування іншому працівникові банку, третім сторонам або виведенням з експлуатації;

– обов’язковості перевірки змінних носіїв інформації на наявність зловмисного коду перед використанням у банку.

13. Банк зобов’язаний здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія.

14. Банк зобов’язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо використання, надання, скасування та контролю доступу до інформаційних систем банку і мають містити:

– вимоги до ідентифікації, автентифікації, авторизації користувачів;

– послідовність дій під час управління доступом, у тому числі в разі віддаленого доступу;

– перелік типових функцій та прав доступу до інформаційних систем банку;

– вимоги щодо здійснення заходів контролю доступу, уключаючи контроль за діями привілейованих користувачів;

– періодичність контролю наданих прав доступу;

– вимоги до протоколювання дій під час управління доступом.

15. Банк зобов’язаний забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку.

16. В інформаційних системах банку, які безпосередньо забезпечують автоматизацію банківської діяльності, забороняється суміщення в межах однієї функції (ролі) таких повноважень: розроблення та супроводження (адміністрування), розроблення та експлуатація, супроводження (адміністрування) та експлуатація, виконання операцій в таких системах та подальшого контролю за їх виконанням.

17. Банк зобов’язаний запровадити такі заходи контролю доступу до інформаційних систем банку:

– перевірку наявності у користувача дозволу керівництва та власника інформаційної системи на такий доступ;

– заборону одноосібного ініціювання заявки, підтвердження та надання доступу;

– перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень;

– періодичну перевірку відповідності наданих прав доступу користувачеві тим, що діють на момент перевірки.

18. Банк зобов’язаний використовувати механізми багатофакторної автентифікації під час надання доступу для виконання функцій адміністрування або супроводження САБ.

19. Банк зобов’язаний забезпечити блокування облікових записів користувачів в інформаційних системах банку в таких випадках:

– п’яти невдалих спроб автентифікації поспіль;

– відсутності реєстрації користувача в інформаційних системах банку протягом 90 календарних днів;

– звільнення користувача.

20. Банк зобов’язаний здійснювати протоколювання всіх дій щодо надання, скасування чи зміни доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, у захищених від несанкціонованої модифікації електронних журналах із забезпеченням їх збереження не менше ніж протягом трьох років.

21. Банк зобов’язаний забезпечити протоколювання, збереження та захист від модифікації інформації про події доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, та зберігання її не менше ніж протягом одного року.

22. Банк зобов’язаний розробити та впровадити політику використання криптографічних засобів для захисту інформації, яка має містити:

– цілі безпеки, для яких використовуються криптографічні заходи безпеки;

– положення щодо необхідності та застосування необхідного рівня захисту інформації за допомогою криптографічних засобів залежно від її класифікації за критерієм конфіденційності.

23. Банк зобов’язаний розробити та затвердити документи, що описують процес управління ключами, які мають містити положення щодо:

– процедури генерації ключів для різних криптографічних систем;

– розподілу ключів серед відповідальних осіб;

– зберігання ключів;

– заміни або оновлення ключів;

– поводження із скомпрометованими ключами;

– відкликання ключів;

– відновлення ключів, які зруйновано;

– процедури резервного копіювання або архівування ключів;

– знищення ключів;

– реєстрації та аудиту діяльності, пов’язаної з управлінням ключами.

24. Банк у разі застосування криптографічного захисту зобов’язаний використовувати криптографічні алгоритми з такого переліку:

1) асиметричні алгоритми:

– алгоритм Діффі – Геллмана для узгодження сеансових ключів шифрування;

– алгоритм цифрового підпису для цифрових підписів;

– алгоритм Діффі – Геллмана на еліптичних кривих для узгодження сеансових ключів шифрування;

– алгоритм цифрового підпису на еліптичних кривих для цифрових підписів;

– алгоритм Ривест – Шаміра – Адлемана для цифрових підписів і узгодження сеансових ключів шифрування або аналогічних ключів;

– алгоритм цифрового підпису "ДСТУ 4145-2002 – Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затверджений наказом Державного комітету України з питань технічного

регулювання та споживчої політики від 28 грудня 2002 року № 31 для цифрових підписів;

2) алгоритми безпеки гешування SHA-224, SHA-256, SHA-384, SHA-512, "Купина" або більш крип-тостійкі;

3) алгоритми симетричного шифрування:

– алгоритм "Advanced encryption standard" (AES) із використанням довжини ключа 128, 192 і 256 біт або більше;

– алгоритм криптографічного перетворення;

– алгоритм "Калина".

25. Банк, який застосовує алгоритм DH для узгодження сеансових ключів шифрування, зобов’язаний використовувати розмір модуля не менше ніж 2048 біт.

26. Банк, який застосовує алгоритм DSA для цифрових підписів, зобов’язаний використовувати розмір модуля не менше ніж 2048 біт.

27. Банк, який застосовує алгоритм на еліптичних кривих, зобов’язаний використовувати еліптичні криві з ДСТУ 4145-2002 або з Федерального стандарту оброблення інформації (США) (Federal information processing standards, FIPS186-4).

28. Банк, який застосовує алгоритм ECDH для узгодження сеансових ключів шифрування, зобов’язаний використовувати розмір поля/ключа не менший, ніж 160 біт.

29. Банк, який застосовує алгоритми ECDSA, ДСТУ 4145-2002 для цифрових підписів, зобов’язаний використовувати розмір поля/ключа не менший, ніж 160 біт.

30. Банк, який застосовує алгоритм RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов’язаний використовувати розмір модуля не менше ніж 2048 біт.

31. Банк, який застосовує алгоритм RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов’язаний

використовувати різні ключові пари для передавання ключів шифрування сеансу (або аналогічних ключів) та для цифрових підписів.

32. Банк зобов’язаний використовувати останню версію протоколу захисту на транспортному рівні та реалізацію цього протоколу, що підтримує безпечне повторне погодження з’єднання для захисту з’єднань, які управляються протоколом Transmission control protocol (TCP). Якщо безпечне повторне погодження з’єднання не підтримується, то ця процедура має бути відключена.

33. Банку забороняється використання анонімного (без автентифікації) алгоритму DH.

34. Банк, який застосовує стандарти для шифрування "Secure multipurpose internet mail extension" (далі – S/MIME), зобов’язаний використовувати цей стандарт не нижче версії 3.0.

35. Банк зобов’язаний використовувати набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу Інтернету (набір протоколів Internet protocol security, IPsec) у режимі ESP (Encapsulating security payload).

36. Банк зобов’язаний використовувати кабелі типу "вита пара" не нижче категорії 5E та/або оптично-волоконні кабелі для організації структурованої кабельної системи (далі – СКС).

37. Банк зобов’язаний забезпечити наявність та актуальність такої документації до СКС:

– схеми (креслення) розміщення обладнання СКС та кабельних каналів;

– схеми підключення обладнання СКС;

– таблиці маркування кабелів СКС та кабельних з’єднань.

38. Банк зобов’язаний забезпечити персоналізований та контрольований доступ до комутаційних вузлів СКС.

39. Банк зобов’язаний розробити та затвердити внутрішній документ, який установлює вимоги до забезпечення захисту від зловмисного коду та

описує організацію захисту від зловмисного коду в банку, який має містити положення щодо:

– вимог до безперервного забезпечення захисту від зловмисного коду;

– вимог до застосування засобів захисту від зловмисного коду, контролю за їх належним функціонуванням та періодичністю оновлення, з обов'язковим визначенням відповідальних осіб;

– застосування оновлень для засобів захисту від зловмисного коду та баз даних засобів захисту від зловмисного коду на робочих станціях та серверах, що не підключені до мережі банку;

– опису процедури централізованого розгортання та управління засобами захисту від зловмисного коду;

– вимог до проведення профілактичних заходів з виявлення зловмисного коду в інформаційних системах банку та їх періодичності.

40. Банк зобов'язаний використовувати виключно актуальні версії ліцензійних засобів захисту від зловмисного коду, для яких не припинено підтримку виробника.

41. Банк зобов'язаний здійснювати централізоване управління захистом від зловмисного коду та забезпечувати можливість:

– віддаленого встановлення, видалення, оновлення та конфігурації засобів захисту від зловмисного коду;

– реєстрації всіх подій засобів захисту від зловмисного коду та централізованого зберігання такої інформації (електронних журналів);

– контролю за наявністю та коректністю роботи агентів засобів захисту від зловмисного коду на робочих станціях та серверах банку.

42. Банк зобов'язаний забезпечити перевірку програмними та/або програмно-апаратними засобами захисту від зловмисного коду:

– усіх вхідних та вихідних повідомлень корпоративної електронної пошти, уключаючи вкладення до них;

– усього вхідного Інтернет-трафіку;

– усіх змінних носіїв інформації, що підключаються до робочих станцій або іншого обладнання інформаційних систем банку.

43. Банк зобов’язаний запровадити заходи, що забезпечують захист від несанкціонованого видалення, відключення та скасування оновлень засобів захисту від зловмисного коду, а також від зміни їх налаштувань та конфігурації.

44. Банк зобов’язаний обробляти факти ураження інформаційних систем банку зловмисним кодом в рамках процесу управління інцидентами безпеки інформації. Банк самостійно визначає критерії віднесення фактів вірусного ураження до інцидентів безпеки інформації.

45. Банк зобов’язаний здійснювати перевірку всіх переносних та/або стаціонарних носіїв інформації засобами захисту від зловмисного коду, які окремо або в складі пристрою були повернуті після їх використання третіми сторонами.

46. Банк зобов’язаний зберігати електронні журнали роботи засобів захисту від зловмисного коду не менше ніж три місяці.

47. Банк зобов’язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість:

– ідентифікації та автентифікації всіх користувачів операційної системи;

– розмежування доступу користувачів операційної системи;

– реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.

48. Банк зобов’язаний використовувати офіційні стабільні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.

49. Банк зобов’язаний визначити стандартне еталонне джерело часу та забезпечити синхронізацію з ним операційних систем.

50. Банк зобов’язаний забезпечити блокування або перейменування облікових записів користувачів операційних систем, що встановлюються

за замовчуванням, та відключення гостьових облікових записів. Банк зобов'язаний заблокувати вбудовані облікові записи локального адміністратора операційних систем або перейменувати такі вбудовані облікові записи та змінювати їх пароль не рідше ніж один раз на 30 діб.

51. Банк зобов'язаний забезпечити автоматичне блокування робочого стола операційної системи на робочій станції або сервері, якщо немає активності користувача протягом 15 хвилин, з наступною повторною автентифікацією користувача під час розблокування.

52. Банк зобов'язаний забезпечити централізоване розповсюдження налаштувань параметрів безпеки та інших параметрів конфігурації операційних систем.

53. Банк зобов'язаний створити та підтримувати в актуальному стані перелік програмного забезпечення, що використовується в банку.

54. Банк зобов'язаний забезпечити блокування можливості здійснення працівниками банку, яким не надано адміністративних прав у операційних системах, таких дій (налаштувань):

– самостійного встановлення програмного забезпечення, яке не внесено до переліку програмного забезпечення, що використовується в банку;

– автоматичного запуску програм із зовнішніх пристроїв та носіїв інформації;

– самостійного видалення встановленого програмного забезпечення, оновлень безпеки.

55. Банк зобов'язаний розробити та затвердити внутрішні документи, які містять опис процесу управління оновленнями. Процес управління оновленнями має містити такі стадії:

– підготовка тестового середовища (тестових клієнтів);

– підготовка переліку оновлень;

– застосування оновлень в тестовому середовищі;

– застосування оновлень на пілотній групі користувачів;

– застосування протестованих оновлень.

56. Банк зобов’язаний здійснювати налаштування програмного забезпечення систем управління базами даних (далі – СУБД) для роботи під окремим обліковим записом з дотриманням принципу надання мінімального рівня повноважень (необхідних для виконання функцій СУБД).

57. Банк зобов’язаний забезпечити блокування облікових записів адміністраторів СУБД, установлених за замовчуванням (або зміну їх паролів) та використання облікових записів адміністраторів СУБД виключно для вирішення адміністративних завдань.

58. Банк зобов’язаний забезпечити видалення/блокування неперсоналізованих і гостьових облікових записів користувачів СУБД та персоналізацію технологічних облікових записів СУБД.

59. Банк зобов’язаний забезпечити фізичне або віртуальне функціональне розділення серверів СУБД та серверів застосувань інформаційних систем банку.

60. Банк зобов’язаний розміщувати сервери баз даних в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

61. Банк зобов’язаний визначити привілейовані облікові записи для інформаційних систем банку, мережевого обладнання та серверів. Привілейовані облікові записи надаються користувачам згідно з внутрішніми документами банку, що встановлюють вимоги до використання, надання, скасування та контролю доступу до інформаційних систем банку.

62. Банк зобов’язаний забезпечити розташування робочих станцій, з яких виконуються дії щодо адміністрування та супроводження інформаційних систем банку, мережевого обладнання та серверів банку, використовуючи привілейовані облікові записи, в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

63. Банк зобов’язаний забезпечити надання доступу до портів адміністрування та супроводження інформаційних систем, мережевого обладнання та серверів банку виключно з IP-адрес (робочих станцій), які визначені банком для адміністрування та супроводження таких систем або обладнання.

64. Банк зобов’язаний забезпечити використання адміністраторами інформаційних систем банку, мережевого обладнання та серверів банку облікових записів без привілейованих повноважень для автентифікації на робочих станціях, які визначені банком для адміністрування та супроводження таких систем чи обладнання.

65. Банк зобов’язаний забезпечити використання виключно персоналізованих облікових записів для виконання адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів.

66. Банк зобов’язаний визначити та запровадити посилені вимоги щодо парольної політики для привілейованих облікових записів або застосовувати багатофакторну автентифікацію для таких облікових записів.

67. Банк зобов’язаний забезпечити централізоване управління мережею банку. Банк має право здійснювати локальне управління мережею банку на різних вузлах за умови централізованого управління такими функціями:

– вибір і монтаж кабельної системи мережі;

– підбір комутаційного обладнання мережі;

– підбір обладнання, що підключається до мережі банку, операційних систем, програмного забезпечення інформаційних систем банку, прикладного програмного забезпечення;

– управління мережевими адресами та ідентифікаторами обладнання і користувачів;

– розподіл мережі на сегменти.

68. Банк зобов’язаний забезпечити підтримання в актуальному стані документації мережі банку, документування всіх змін у конфігурації мережі банку та зберігання попередніх версій документації мережі строком не менше ніж один рік. Документація мережі банку має бути погоджена відповідальною особою за інформаційну безпеку банку та містити:

– фізичну схему мережі, уключаючи бездротові мережі, що відображає всі з’єднання в мережі;

– логічну схему мережі, уключаючи бездротові мережі, що відображає всі мережеві пристрої, критично важливі сервери та сервіси;

– конфігурацію мережевого обладнання, уключаючи бездротові мережі.

69. Банк зобов’язаний задокументувати порядок контролю змін у конфігурації мережі, у якому мають зазначатися вимоги щодо перегляду конфігурації мережі не рідше ніж один раз на рік з документуванням результатів перегляду.

70. Банк зобов’язаний здійснити розподіл мережі банку на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів.

71. Банк зобов’язаний забезпечити ідентифікацію обладнання, що підключається до мережі банку, та вжиття заходів, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

72. Банк зобов’язаний забезпечити програмне відключення портів на активних мережевих пристроях мережі банку, які не використовуються.

73. Банку забороняється використовувати облікові записи та паролі за замовчуванням на активних мережевих пристроях, які підключені до мережі банку.

74. Банку забороняється використовувати протокол Інтернету версії 6 (IPv6) у мережі банку.

75. Банку забороняється використовувати версії 1 або 2 простого протоколу керування мережею (Simple network management protocol, SNMP) для управління пристроями в мережі.

76. Банк зобов’язаний забезпечити синхронізацію всіх активних мережевих пристроїв з еталонним джерелом часу банку.

77. Банк зобов’язаний розробити та впровадити заходи безпеки інформації у разі використання бездротових мереж передавання даних.

78. Банк зобов’язаний розмістити бездротові мережі банку в окремій зоні безпеки мережі банку та розмежувати доступ із зони безпеки бездротових мереж до мережі банку з використанням міжмережевих екранів.

79. Банк зобов’язаний встановити ідентифікатори бездротових мереж (SSID), відмінні від встановлених виробником або інсталятором обладнання за замовчуванням. Банк зобов’язаний відключити трансляцію ідентифікаторів бездротових мереж.

80. Банк зобов’язаний забезпечити використання в бездротових мережах банку режиму безпеки WPA2-Enterprise та використання режиму безпеки WPA2-Personal для реалізації гостьових підключень.

81. Банк зобов’язаний застосовувати такі заходи безпеки інформації для організації віддаленого доступу до інформаційних систем банку:

– розміщення сервера (серверів) віддаленого доступу до інформаційних систем банку в демілітаризованій зоні (DMZ) мережі банку, з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами;

– шифрування каналів зв’язку для доступу до сервера віддаленого доступу до інформаційних систем банку;

– багатофакторна автентифікація користувачів.

82. Банк зобов’язаний забезпечити розмежування доступу між мережею банку і публічною мережею з використанням міжмережевих екранів та/або пристроїв уніфікованого управління загрозами.

83. Банк зобов’язаний обробляти виявлені атаки або вторгнення до мережі банку в рамках процесу управління інцидентами безпеки інформації. Банк самостійно визначає критерії віднесення таких атак або вторгнень до інцидентів безпеки інформації.

84. Банк зобов’язаний забезпечити доступ з публічної мережі до мережі банку виключно із застосуванням захищених з’єднань.

85. Банк зобов’язаний забезпечити розміщення в демілітаризованій зоні мережі банку серверів та обладнання, що забезпечує функціонування сервісів або банківських продуктів, які відкриті для доступу клієнтів з публічної мережі. З’єднання серверів та обладнання, що розміщено в демілітаризованій зоні, з серверами та обладнанням мережі банку захищаються міжмережевим екраном.

86. Банк зобов’язаний виконувати перевірку ефективності заходів щодо захисту периметра мережі банку шляхом виконання періодичних тестів на проникнення.

87. Національний банк визначає інформаційні задачі, у яких для забезпечення застосування електронного цифрового підпису обов’язковим є використання послуг електронного цифрового підпису від акредитованих центрів сертифікації ключів (далі – акредитовані ЦСК).

88. У випадках отримання послуг електронного цифрового підпису від зареєстрованих центрів сертифікації ключів взаємне визнання електронного цифрового підпису між учасниками електронної взаємодії визначається договірними засадами. Крім того, у договорі обов’язково мають обумовлюватися права, обов’язки та відповідальність сторін, розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, порядок вирішення спорів у разі їх виникнення.

89. Акредитовані ЦСК та зареєстровані ЦСК зобов’язані здійснювати свою діяльність відповідно до регламенту роботи, що визначає організаційно-методологічні та технологічні умови його діяльності в

процесі надання послуг електронного цифрового підпису підписувачам. Регламент роботи ЦСК має бути розроблений та погоджений відповідно до вимог чинного законодавства.

90. Банк зобов’язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації, технічного обслуговування, експлуатації факсимільних апаратів, багатофункціональних пристроїв, телефонів та/або телефонних систем та мають містити такі положення щодо:

– функцій та обов’язків персоналу банку стосовно підключення, технічного обслуговування та експлуатації систем та пристроїв зв’язку;

– категорій інформації за критерієм конфіденційності, що може передаватися пристроями зв’язку;

– обов’язковості очищення оперативної та постійної пам’яті факсимільних апаратів і багатофункціональних пристроїв перед передаванням їх третім сторонам або перед виведенням з експлуатації.

91. Банк зобов’язаний створити та підтримувати в актуальному стані перелік факсимільних апаратів і багатофункціональних пристроїв, який містить унікальні ідентифікатори обладнання та місце його розташування.

92. Банк зобов’язаний ознайомити своїх працівників із документами, які встановлюють вимоги щодо безпеки інформації, технічного обслуговування та експлуатації факсимільних апаратів, багатофункціональних пристроїв для друку, телефонів та/або телефонних систем.

93. Банк зобов’язаний розміщувати обладнання телефонної мережі (сервери, комутаційне та абонентське обладнання) в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

94. Банк зобов’язаний запровадити такі заходи безпеки в разі використання телефонного зв’язку на основі протоколу Інтернет (IP-телефонії):

– активувати вбудовані алгоритми шифрування трафіку між шлюзами, які забезпечують роботу телефонної системи банку, або між шлюзом та кінцевим абонентським обладнанням (телефоном);

– здійснювати розподіл унікальних ідентифікаторів мережевого рівня (IP-адрес) у телефонній мережі банку відповідно до стандарту RFC 1918 "Розподіл адрес у приватних IP-мережах".

95. Банк зобов’язаний розробити та затвердити документ щодо використання електронної пошти, який має містити положення щодо:

– обмежень під час пересилання інформації банку;

– категорії інформації, яка може надсилатись засобами електронної пошти;

– обмежень використання сторонніх сервісів електронної пошти, які не пов’язані з виконанням функціональних обов’язків персоналом банку.

96. Банк зобов’язаний розробити та впровадити заходи безпеки інформації для сервера електронної пошти, які включають:

– додаткові заходи безпеки операційної системи, на якій встановлено сервер застосувань електронної пошти;

– заходи безпеки сервера застосувань електронної пошти;

– налаштування правил доступу до сервера електронної пошти.

97. Банк зобов’язаний забезпечити перевірку програмними або апаратними засобами захисту всіх повідомлень, що обробляються сервером застосувань електронної пошти, на наявність зловмисного коду.

98. Банк зобов’язаний впровадити періодичне тестування захищеності та перегляд налаштувань параметрів безпеки операційної системи сервера застосувань електронної пошти та безпосередньо сервера застосувань електронної пошти.

99. Банк зобов’язаний розміщувати сервер застосувань електронної пошти на окремому фізичному або віртуальному сервері.

100. У разі використання віддаленого доступу до сервера застосувань електронної пошти банк зобов’язаний запровадити такі заходи безпеки інформації:

– сервер має бути розміщений в демілітаризованій зоні мережі банку з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами;

– доступ до сервера електронної пошти має надаватись лише шифрованими каналами зв’язку.

101. Банк зобов’язаний запровадити такі заходи безпеки інформації для сервера електронної пошти:

– використовувати міжмережевий екран операційної системи сервера електронної пошти для обмеження доступу до сервера;

– заблокувати отримання вхідних повідомлень від серверів мережі Інтернет, що розсилають спам;

– упровадити процес постійного моніторингу вразливостей сервера застосувань електронної пошти та клієнтського програмного забезпечення доступу до сервера застосувань електронної пошти, забезпечити встановлення відповідних оновлень, що усувають виявлені вразливості.

102. Банк зобов’язаний визначити та задокументувати вимоги безпеки інформації для інформаційних систем банку під час їх розроблення, модернізації або в разі придбання.

103. На стадії розроблення і тестування інформаційних систем банку та/або їх компонентів банк зобов’язаний використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента мережі банку. Як тестові дані банк має право використовувати виключно знеособлені дані.

104. Банк зобов’язаний розробити документацію для інформаційних систем банку та/або їх компонентів з обов’язковим описом реалізованих в інформаційних системах банку організаційних та технічних заходів

безпеки інформації, якщо така документація не надана розробником інформаційних систем банку.

105. Банк зобов’язаний на стадії експлуатації інформаційних систем задокументувати положення щодо:

– контролю функціонування реалізованих в інформаційних системах банку заходів безпеки інформації, уключаючи контроль реалізації організаційних заходів та контроль складу і параметрів налагодження технічних засобів безпеки інформації;

– контролю вразливостей в обладнанні та програмному забезпеченні інформаційних систем банку;

– контролю конфігурації програмного забезпечення інформаційних систем банку;

– відновлення всіх реалізованих заходів щодо забезпечення безпеки інформації в інформаційних системах банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

106. Банк зобов’язаний визначити функції та обов’язки, пов’язані з експлуатацією інформаційних систем і впроваджених в них заходів безпеки інформації, уключаючи внесення змін до параметрів їх налаштування.

107. Банк зобов’язаний задокументувати та впровадити порядок виведення з експлуатації обладнання інформаційних систем банку, який має містити опис процесу видалення інформації з таких систем, використовуючи алгоритми та/або методи, що забезпечать неможливість її відновлення.

108. Банк зобов’язаний упровадити процес управління інцидентами безпеки інформації та розробити і затвердити документи, які містять описи дій стосовно:

– виявлення інцидентів;

– інформування про інциденти, у тому числі відповідальної особи за інформаційну безпеку, підрозділу з безпеки інформації та працівників банку;

– класифікації інцидентів та оцінки негативного впливу (збитку), нанесеного банку інцидентом;

– реагування на інциденти;

– аналізу причин, що призвели до інцидентів та оцінки результатів реагування на інциденти;

– зберігання інформації щодо інцидентів, аналізу інцидентів та результатів реагування на інциденти.

109. Банк зобов’язаний визначити в посадових інструкціях працівників банку або організаційно-розпорядчих документах банку особисті функції та обов’язки з виявлення, класифікації, реагування і аналізу інцидентів безпеки інформації.

110. Банк зобов’язаний забезпечити документування інформації щодо інцидентів безпеки інформації та її зберігання не менше ніж один рік.

РОЗДІЛ 12. ЗАХИСТ ІНФОРМАЦІЇ В ПРИМІЩЕННЯХ БАНКІВ, У ЯКИХ ОБРОБЛЯЮТЬСЯ ЕЛЕКТРОННІ ДОКУМЕНТИ

1. Загальні положенння

1.1. Ці Правила розроблені відповідно до Законів України "Про Національний банк України" (679-14), "Про банки і банківську діяльність" (2121-14), "Про інформацію" (2657-12), "Про захист інформації в інформаційно-телекомунікаційних системах" (80/94-ВР).

1.2. Вимоги цих Правил поширюються на приміщення центрального апарату, структурних підрозділів і одиниць, територіальних управлінь, навчальних закладів Національного банку України (далі – Національний банк), банків України та їх відокремлених підрозділів (далі – банки), у яких обробляються електронні банківські документи, що містять відомості з грифом "Банківська таємниця", та інша електронна інформація, доступ до якої обмежений банком, а також на приміщення банків, що заново будуються, реконструюються або проектна документація на які не була затверджена до набрання чинності цим Положенням.

1.3. У цих Правилах терміни вживаються в таких значеннях:

– приміщення з обмеженим доступом – приміщення, у яких розташовані робочі місця з комп'ютерною технікою, обробляються електронні банківські документи, що містять відомості з грифом "Банківська таємниця", та інша електронна інформація, доступ до якої обмежений банком;

– комутаційні кімнати – приміщення, у яких розташовано телекомунікаційне обладнання, що забезпечує функціонування локальних і корпоративних мереж банку, а також зв'язок з іншими установами та мережами загального користування;

– серверні приміщення – приміщення, у яких розташовані сервери баз даних, сервери прикладних програм, файлові сервери тощо, на яких

обробляються та зберігаються електронні банківські документи і бази даних.

Інші терміни, що використовуються у цих Правилах, уживаються в значеннях, визначених нормативно-правовими актами з питань технічного захисту інформації.

1.4. Ці Правила встановлюють вимоги до систем електроживлення та заземлення, мережевого обладнання, приміщень з обмеженим доступом, комутаційних кімнат, серверних приміщень, приміщень, у яких зберігаються електронні архіви.

1.5. За порушення банками вимог цих Правил Національний банк має право застосувати заходи впливу відповідно до законодавства України.

2. Вимоги до приміщень з обмеженим доступом

2.1. Приміщення з обмеженим доступом визначаються внутрішнім документом банку з урахуванням особливостей організації робіт з електронними банківськими документами та із зазначенням прізвищ, імен та по батькові відповідальних працівників банку.

2.2. Приміщення з обмеженим доступом не можуть бути прохідними та мають розташовуватися таким чином, щоб унеможливити перебування інших осіб без супроводу відповідальних працівників банку.

2.3. Приміщення з обмеженим доступом слід обладнувати дверима з кодовим механічним замком або системою розмежування доступу та механічним замком.

2.4. Приміщення з обмеженим доступом слід обладнувати охоронною сигналізацією, виведеною на пост власної служби охорони банку та/або суб'єкта охорони банку.

2.5. Екрани дисплеїв комп'ютерів у таких приміщеннях слід розміщувати таким чином, щоб унеможливити ознайомлення з інформацією, яка виводиться на них, іншими особами (у тому числі крізь вікна, скляні огорожі тощо).

3. Вимоги до комутаційних кімнат

3.1. До комутаційних кімнат належать приміщення, у яких установлено комутаційне обладнання, що виконує функції управління мережами банку та зв'язком з іншими установами і мережами загального користування.

3.2. Комутаційні кімнати слід обладнувати як приміщення з обмеженим доступом.

3.3. Комутаційні кімнати не повинні містити робочі місця для працівників банку.

3.4. У кожній комутаційній кімнаті повинен вестися журнал на паперових носіях, у якому відображаються:

– дата та час відкриття і закриття кімнати;

– прізвище працівника, який відвідав кімнату;

– опис проведених робіт.

3.5. У разі розташування комутаційного обладнання в комутаційних шафах, які розташовані в коридорах або інших приміщеннях банку, такі шафи мають бути обладнані датчиками на відкриття і пожежними датчиками з виведенням їх сигналів на робочі місця осіб, які відповідають за мережеве обладнання, або на пульт служби централізованої охорони. Допускається обладнання комутаційних шаф замість датчиків на відкриття засобами для опечатування з обов'язковою перевіркою цілісності відбитків печаток не рідше одного разу на тиждень.

4. Вимоги до серверних приміщень і приміщень електронних архівів

4.1. Технічний захист інформації в серверних приміщеннях і приміщеннях електронних архівів здійснюється за допомогою екранування приміщення або використання екранованих шаф, екранованих сейфів (клас опору до злому не нижче II), екранованих кабін з метою запобігання витоку інформації через побічні випромінювання і наводки, а також від

порушення її цілісності внаслідок впливу зовнішніх електромагнітних полів.

4.2. Забороняється розміщення робочих місць працівників банку в серверних приміщеннях.

4.3. Допускається використання екранованих шаф (сейфів) для розміщення серверів баз даних, серверів прикладних задач тощо, а також електронних архівів у приміщеннях з обмеженим доступом. У разі використання екранованих шаф (сейфів) вони повинні мати сертифікат відповідності, виданий Державною службою спеціального зв'язку та захисту інформації України.

4.4. Серверні приміщення та приміщення електронних архівів рекомендується розташовувати у віддалених один від одного кінцях будівлі. Якщо є така змога, ці приміщення розташовують у внутрішній частині будівлі або з боку внутрішнього двору.

4.5. Серверні приміщення та приміщення електронних архівів рекомендується розташовувати в приміщеннях без вікон. Це не поширюється на старі приміщення, що реконструюються, та на екрановані приміщення, у яких установлені екрановані шафи (сейфи).

4.6. Для запобігання несанкціонованому доступу до серверних приміщень та приміщень електронних архівів їх двері повинні бути обладнані автоматизованою системою доступу або кодовим замком, не менше ніж двома рубежами охоронної сигналізації, кожний з яких підключений окремими кодами до приймально-контрольних приладів, установлених на посту охорони банку та/або суб'єкта охорони банку.

4.7. Серверні приміщення та приміщення електронних архівів мають бути обладнані системою оповіщення під час пожежі та автоматичною системою газового пожежогасіння. Внутрішні поверхні цих приміщень облицьовуються пожежобезпечними матеріалами, що відповідають санітарно-гігієнічним вимогам.

4.8. З метою недопущення проникнення через повітропроводи системи вентиляції та канали для введення кабелів і комунікацій до серверних приміщень і приміщення електронних архівів сторонніх речовин їх слід обладнати вогнетривкими пробками чи вогнетривкими аварійними заслінками.

4.9. Серверні приміщення та приміщення електронних архівів обладнуються централізованою або окремою системою припливно-витяжної вентиляції з очищенням від пилу та окремою системою автоматичного кондиціювання повітря з очищенням від пилу, які повинні забезпечувати в приміщенні температуру повітря 18-24 град. і відносну вологість не більше ніж 60% у будь-яку пору року.

4.10. У кожному серверному приміщенні та приміщенні електронних архівів повинен вестися журнал на паперових носіях, у якому відображаються:

– дата та час відкриття і закриття кімнати;

– прізвище працівника, який відвідав кімнату;

– опис проведених робіт.

5. Вимоги до екранованих приміщень

5.1. Екрановані приміщення повинні забезпечувати ефективність екранування не менше 20 дБ у діапазоні частот 0,15-1000 МГц.

5.2. Вимірювання ефективності екранування здійснюються юридичними особами, які мають ліцензію Державної служби спеціального зв'язку та захисту інформації України на провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації. Для підрозділів Національного банку вимірювання здійснюються підрозділом Національного банку, який має дозвіл Державної служби спеціального зв'язку та захисту інформації України.

5.3. Для виконання робіт з облаштування екранованих приміщень має розроблятися проект, який повинен містити:

– перелік матеріалів для побудови конструкції екрана екранованого приміщення, способи його з'єднання та кріплення до стін;

– конструкцію дверей;

– типи кабелів і комунікацій та способи їх уведення в екрановане приміщення;

– перелік і параметри обладнання, що розташовані в екранованому приміщенні;

– параметри систем вентиляції, кондиціювання і газового пожежогасіння.

5.4. Для виготовлення екрана мають використовуватися такі матеріали:

– сталь листова;

– листи мідні, латунні та з її сплавів;

– листи алюмінієві та з його сплавів;

– сітка металева з розміром вічка не більше ніж 6 х 6 мм.

5.5. Під час виготовлення екрана слід дотримуватися таких вимог:

-листи, що використовуються для виготовлення екрана, на всіх стиках зварюються внапуск суцільним швом або з'єднуються фальцем з подальшим пропаюванням місця з'єднання суцільним швом;

– полотна сітки з'єднуються внапуск за допомогою паяння чи зварювання суцільним швом;

– під час зварювання допускається використання переривчастого шва з проміжками між точками зварювання (паяння) не більше ніж 25 мм;

– деталі кріплення в місцях їх проходження через екран зварюються (спаюються) з ним по периметру.

5.6. Екран не повинен мати гальванічного контакту з металевими деталями будівельних конструкцій.

5.7. Екранування дверних або віконних прорізів виконується за допомогою металевих дверей або віконниць.

5.8. Для забезпечення електричного контакту дверей з коробкою по периметру встановлюють контактний пристрій: гребінчасті контакти з кроком гребінки не більше ніж 25 мм з корозієстійкого пружного матеріалу або сріблене чи луджене обплетення, які укладають на планку з корозостійкого матеріалу.

Дверну коробку з'єднують з екраном за допомогою зварювання чи паяння. По периметру прилягання дверей до дверної коробки на останній прокладається контактна планка з корозієстійкого матеріалу, яка призначена для електричного контакту з контактним пристроєм.

Гребінчасті контакти і планки ріпляться до зачищеної поверхні дверей (коробки) гвинтами з кроком не більше ніж 50 мм. Допускається встановлення контактного пристрою на дверній коробці, а контактної планки – на дверях.

5.9. Для забезпечення електричного контакту дверей з коробкою по периметру їх обладнують замковим пристроєм, конструкція якого забезпечує притискання дверей до коробки.

Замковий пристрій повинен мати з обох боків дверей рукоятки. Вісь, яка їх з'єднує, оснащується спеціальним контактним пристроєм, який забезпечує електричний контакт осі по її периметру з екранувальним полотном дверей, або ж вісь може бути виготовлена з діелектричного матеріалу та встановлена в патрубок, внутрішній діаметр якого не більше ніж 50 мм і довжина не менше двох діаметрів і який по периметру приварюється до екранувального полотна дверей.

Не рекомендується виготовляти двері з двох стулок тому, що в такому разі складніше забезпечити електричний контакт по периметру.

5.10. У разі реконструкції серверних приміщень, о мають вікна, для спрощення конструкції екранованого приміщення в результаті виключення з їх конструкції віконниць рекомендується між екраном і вікном залишити

технологічну зону завширшки не менше ніж 1 метр. У цій зоні можна розмістити допоміжне обладнання.

5.11. Неметалеві (діелектричні) труби вводять в екрановане приміщення через металеві патрубки, поперечний розмір яких не більше ніж 50 мм і довжина не менше ніж два поперечних розміри, які зварюють по периметру з екраном. Якщо площа перерізу такого патрубка недостатня, то трубу розривають і з'єднують за допомогою хвилеподібної стільникової решітки з поперечним розміром вічка не більше ніж 50 мм і завдовжки не менше ніж два поперечних розміри вічка. Цю стільникову решітку зварюють по периметру з екраном. Стільникову решітку можна виготовити з відрізків металевих кутиків із зварюванням усіх стиків або з патрубків з круглим перерізом, кінці яких з одного боку зварюються до листа з отворами по периметру кожного патрубка, або з патрубків з квадратним перерізом, кінці яких з одного боку зварені один одним по периметру кожного патрубка. Усі зварювальні шви мають бути суцільними. стільникова решітка зварюється по периметру з екраном. Замість стільникової решітки можна також використовувати сітку з вічком не більше ніж 6 х 6 мм, яка зварюється (спаюється) по периметру з екраном.

Якщо в неметалевій трубі циркулює провідна рідина, то вона може бути введена в екрановане приміщення через сталеву трубу з поперечним розміром не більше ніж 50 мм і завдовжки не менше ніж три метри, яка повинна по периметру введення вварюватися з екраном, або ж неметалева труба розривається і з'єднується через металевий штуцер, що проходить через екран і має з ним контакт по периметру.

5.12. У місцях уведення в екрановане приміщення металевих труб, що не є природними заземлювачами, їх зварюють по периметру до екрана, а якщо їх поперечний розмір перевищує 50 мм, о встановлюють хвилеподібну стільникову решітку або екранувальну сітку, яка зварюється (спаюється) по периметру з екраном. Для забезпечення легкої заміни руби рекомендується не зварювати її безпосередньо з екраном, а ввести через

патрубок, який одним кінцем зварюється з екраном, а другим – з трубою по периметру.

5.13. Металеві труби, що є природними заземлювачами, можуть бути введені в екрановане приміщення через сталеві труби з поперечним розміром не більше ніж 50 мм і завдовжки не менше ніж три метри, які по периметру введення повинні приварюватися до екрана. Ці сталеві труби повинні бути ізольовані від металевих труб, що вводяться. Металеві труби, якщо ними не циркулює провідна рідина, можуть бути розірвані та з'єднані за допомогою відрізка неметалевої труби, який вводиться в екрановане приміщення, як зазначено вище.

5.14. Усі інформаційні кабелі, які виходять з екранованого приміщення назовні, повинні бути не нижче п'ятої категорії екранованими, оптоволоконними або іншого типу, які забезпечують захист від електромагнітного випромінювання.

5.15. Кабелі електроживлення технологічного обладнання слід уводити через фільтри електроживлення.

5.16. Уведення всіх інших кабелів і проводів здійснюють через сталеві труби з поперечним розміром не більше ніж 50 мм і завдовжки не менше ніж три метри, які по периметру введення зварюються до екрана. Якщо ці заходи не забезпечать потрібної ефективності екранування, то рекомендується ці кабелі ввести через фільтри. Для інформаційних кабелів використовується феромагнітний порошок, який засипається в труби. Діелектричні оптоволоконні кабелі вводять через металеві патрубки поперечним розміром не більше ніж 50 мм і довжиною не менше ніж два поперечні розміри, які зварюють по периметру з екраном.

5.17. Слабкострумові та силові кабелі мають розміщуватися в різних пакетах.

5.18. Усередині екранованого приміщення прокладання кабельної мережі виконується в пластикових коробах. Коефіцієнт заповнення перетину короба чи труби не повинен перевищувати 65%.

5.19. Фільтри електроживлення рекомендується встановлювати із зовнішнього боку екранованого приміщення біля місця введення електричних проводів. Проводи між фільтром і екраном прокладають у металевій трубі або в екранувальному обплетенні, які з'єднані як з фільтром, так і з екраном по периметру.

5.20. Заземлювач екранованого приміщення потрібно розташовувати не ближче ніж за 10 м до межі території, що охороняється, та інженерних комунікацій, що виходять за неї. Для систем заземлення не використовуються природні заземлювачі.

5.21. Провідник захисного заземлення в місці введення в екроване приміщення зварюється по периметру з екраном. Провідник робочого заземлення, якщо воно ізольоване від захисного, потрібно вводити в екроване приміщення або через фільтр, або через сталеву трубу з поперечним розміром не більше ніж 50 мм і завдовжки не менше ніж три метри, яка по периметру введення зварюється з екраном.

5.22. Завершальний етап, саме етап здавання екранованого приміщення в експлуатацію, передбачає виконання таких заходів:

– перевірку ефективності екранування з уведеними в екранованому приміщенні кабелями та комунікаціями;

– дооснащення за потреби екранованого приміщення.

5.23. Після завершення робіт складаються акт про відповідність вимогам цих Правил і протоколи вимірювання ефективності екранування. Періодичність виконання вимірювань ефективності екранування виконується один раз на п'ять років.

6. Вимоги до систем заземлення банків та систем захисту від пошкодження блискавкою

6.1. Заземлення засобів комп'ютерної та іншої техніки для обробки інформації в банківській діяльності повинно мати електричний опір не більше ніж 4 Ом.

6.2. Захист від блискавки забезпечується:

– від наведеного електричного потенціалу – заземленням корпусів обладнання, металевих конструкцій і комунікацій, використанням елементів блокування перенапруги;

– від наведеної магнітної індукції – обмеженням площі незамкнених контурів системи заземлення.

7. Вимоги до систем електроживлення банків

7.1. Банк має підключатися до міської електромережі і мати два незалежних уведення від різних підстанцій. Кожне введення повинно забезпечувати передавання електроенергії необхідної потужності. Установлене електроустаткування має забезпечувати автоматичне та ручне переключення між уведеннями.

7.2. Одержання необхідної надійності та якості електроживлення локальних обчислювальних мереж, систем обробки та передавання інформації, електронної пошти, протипожежних установок, охоронної сигналізації та сигналізації загазованості забезпечується шляхом творення системи гарантованого електропостачання з використанням агрегату безперервного живлення подвійного перетворення із стандартним набором акумуляторних батарей, дизельної електростанції з автоматичним пуском пристроєм автоматичного переключення на дизельну електростанцію.

7.3. Силові та слабкострумові кабелі повинні розміщуватися в різних пакетах і прокладатися в металевих коробах або трубах, не утворюючи петель та замкнутих контурів. Якщо пакети прокладаються в неметалевих коробах, то відстань між силовими та слабкострумовими пакетами має бути не менше ніж 40 см. Перетин таких пакетів повинен виконуватися під кутом 90 град. До того ж екранувальні оболонки кабелів не повинні контактувати.

7.4. Живлення комп'ютерного обладнання має забезпечуватися за допомогою джерел безперебійного живлення з повним перетворенням

вхідної напруги (так звані on-line). Під час монтажу агрегату безперервного живлення вхідні та вихідні його проводи повинні прокладатися в окремих пакетах, відстань між якими має бути не менше ніж 40 см.

7.5. Головні розподільчі електрощити, джерело безперебійного живлення та апаратура автоматичного включення резерву повинні бути розташовані в спеціалізованому приміщенні з обмеженим доступом.

8. Рекомендації щодо побудови структурованих і локальних мереж

8.1. Локальні мережі банків повинні будуватися використанням екранованих витих пар не нижче п'ятої категорії (STP, FTP, SFTP), оптоволоконним кабелем або іншими кабелями, які забезпечують захист від електромагнітного випромінювання.

8.2. Під час розведення проводів кабелів у коробах слід передбачити 20% вільного місця для їх додаткового укладення (у разі потреби).

РОЗДІЛ 13. WESTERN UNION. ВИМОГИ ДО ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕКАЗІ КОШТІВ ЧЕРЕЗ СИСТЕМУ WESTERN UNION

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів застосовуються для забезпечення захисту такої інформації:

– інформації про залишки коштів на банківських рахунках;

– інформації про вчинені перекази грошових коштів, в тому числі інформації, що міститься в повідомленнях (підтверджень), що стосуються прийому до виконання розпоряджень Учасників, а також в повідомленнях (підтверджень), що стосуються виконання розпоряджень Учасників;

– інформації, що міститься в оформлених в рамках застосовуваної форми безготівкових розрахунків розпорядженнях клієнтів Учасників, розпорядженнях Учасників, розпорядженнях платіжного клірингового центру;

– інформації про платіжні клірингових позиціях;

– інформації, необхідної для посвідчення клієнтами права розпорядження грошовими коштами, в тому числі даних власників платіжних карт;

– ключової інформації засобів криптографічного захисту інформації, використовуваних при здійсненні переказів грошових коштів;

– інформації про конфігурацію, яка визначає параметри роботи автоматизованих систем, програмного забезпечення, засобів обчислювальної техніки, телекомунікаційного обладнання, експлуатація яких забезпечується Учасником, Оператором Послуг Платіжної Інфраструктурою, банківським платіжним агентом (субагентом), і

використовуються для здійснення переказів грошових коштів, а також інформації про конфігурацію, яка визначає параметри роботи технічних засобів по захисту інформації;

– інформації обмеженого доступу, в тому числі персональних даних та іншої інформації, що підлягає обов'язковому захисту відповідно до законодавства України, що обробляється при здійсненні переказів грошових коштів.

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів включають в себе:

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при призначенні і розподілі функціональних прав і обов'язків осіб, пов'язаних із здійсненням переказів грошових коштів;

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації, модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури;

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури, включаючи вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації від несанкціонованого доступу;

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації від впливу програмних кодів, що призводять до порушення штатного функціонування засобів обчислювальної техніки;

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при

використанні інформаційно-телекомунікаційної мережі Інтернет при здійсненні переказів грошових коштів;

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при використанні ЗКЗІ;

– вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів з використанням взаємопов'язаної сукупності організаційних заходів захисту інформації та технічних засобів захисту інформації, що застосовуються для контролю виконання технології обробки інформації, що захищається при здійсненні переказів грошових коштів;

– вимоги до організації та функціонування підрозділу (працівників), відповідального (відповідальних) за організацію і контроль забезпечення захисту інформації;

– вимоги до підвищення обізнаності працівників Учасника, Агента (субагентів), який є юридичною особою, Оператора Послуг Платіжної Інфраструктури і клієнтів у сфері забезпечення захисту інформації;

– вимоги до виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, і реагування на них;

– вимоги до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів;

– вимоги до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

– вимоги до доведення Учасником, Оператором Послуг Платіжної Інфраструктури до Оператора інформації про забезпечення в Платіжної Системі Вестерн Юніон захисту інформації при здійсненні переказів грошових коштів;

– вимоги до вдосконалення Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури захисту інформації при здійсненні переказів грошових коштів

Виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів забезпечується шляхом:

– вибору організаційних заходів захисту інформації; визначення у внутрішніх документах Учасника, Агента (субагентів), Оператора, Оператора Послуг Платіжної Інфраструктури порядку застосування організаційних заходів захисту інформації; визначення осіб, відповідальних за застосування організаційних заходів захисту інформації; застосування організаційних заходів захисту; реалізації контролю застосування організаційних заходів захисту інформації; виконання інших необхідних дій, пов'язаних із застосуванням організаційних заходів захисту інформації;

– вибору технічних засобів захисту інформації; визначення у внутрішніх документах Учасника, Агента (субагентів), Оператора, Оператора Послуг Платіжної Інфраструктури порядку використання технічних засобів захисту інформації, що включає інформацію про конфігурацію, визначальну параметри роботи технічних засобів захисту інформації; призначення осіб, відповідальних за використання технічних засобів захисту інформації; використання технічних засобів захисту інформації; реалізації контролю за використанням технічних засобів захисту інформації; виконання інших необхідних дій, пов'язаних з використанням технічних засобів захисту інформації

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при призначенні і розподілі ролей осіб, пов'язаних із здійсненням переказів грошових коштів, включаються такі вимоги.

1) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують реєстрацію осіб, що володіють правами:

– по здійсненню доступу до інформації, що захищається;

– з управління криптографічними ключами;

– по впливу на об'єкти інформаційної інфраструктури, яке може привести до порушення надання послуг по здійсненню переказів грошових коштів, за винятком банкоматів і платіжних терміналів.

2) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують реєстрацію своїх працівників, що володіють правами щодо формування електронних повідомлень, що містять розпорядження про здійснення переказів грошових коштів.

3) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують реалізацію заборони виконання однією особою в один момент часу наступних ролей:

– ролей, пов'язаних зі створенням (модернізацією) об'єкта інформаційної інфраструктури та експлуатацією об'єкта інформаційної інфраструктури;

– ролей, пов'язаних з експлуатацією об'єкта інформаційної інфраструктури в частині його використання за призначенням і експлуатацією об'єкта інформаційної інфраструктури в частині його технічного обслуговування і ремонту.

4) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують контроль і реєстрацію дій осіб, яким призначено ролі, визначені в цьому пункті.

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації, модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури, включаються такі вимоги.

1) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують включення в технічні завдання на створення (модернізацію) об'єктів інформаційної інфраструктури вимог до

забезпечення захисту інформації при здійсненні переказів грошових коштів.

2) Учасник, Агент (Субагент), який є юридичною особою, Оператор Послуг Платіжної Інфраструктури, участь служби інформаційної безпеки в розробці і узгодженні технічних завдань на створення (модернізацію) об'єктів інформаційної інфраструктури.

3) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури, оператор послуг платіжної інфраструктури забезпечують:

– наявність експлуатаційної документації на використовувані технічні засоби захисту інформації;

– контроль виконання вимог експлуатаційної документації на використовувані технічні засоби захисту інформації протягом усього терміну їх експлуатації;

– відновлення функціонування технічних засобів захисту інформації, що використовуються при здійсненні переказів грошових коштів, у випадках збоїв і (або) відмов у їх роботі.

4) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують реалізацію заборони використання інформації, що захищається на стадії створення об'єктів інформаційної інфраструктури.

5) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури на стадіях експлуатації та зняття з експлуатації об'єктів інформаційної інфраструктури забезпечують:

– реалізацію заборони несанкціонованого копіювання інформації, що захищається;

– захист резервних копій інформації, що захищається;

– знищення інформації, що захищається в випадках, коли зазначена інформація більше не використовується, за винятком інформації, що захищається, переміщеної в архіви, ведення і збереження яких передбачено законодавчими актами України, нормативними актами НБУ, Правилами та

(або) договорами, укладеними Учасником, Агентом (субагентами), Оператором, Оператором По□слуг Платіжної Інфраструктури;

– знищення інформації, що захищається, в тому числі міститься в архівах, способом, що забезпечує неможливість її відновлення.

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації з використанням технологічних заходів захисту інформації, включаються такі вимоги.

1) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують облік і контроль Оператор визначає порядок застосування організаційних заходів захисту інформації та (або) використання технічних засобів захисту інформації, що використовуються при проведенні операцій обміну електронними повідомленнями та іншою інформацією при здійсненні переказів грошових коштів. Учасник і Оператор Послуг Платіжної Інфраструктури забезпечують виконання зазначеного порядку.

2) Розпорядження клієнта, розпорядження Учасника та розпорядження ЦПКК в електронному вигляді може бути посвідчений електронним підписом, а також відповідно до пункту 3 статті 847 Цивільного кодексу України (Відомості Верховної Ради України, 1996, N 5, ст. 410) аналогами власноручного підпису, кодами, паролями та іншими засобами, що дозволяють підтвердити складання розпорядження уповноваженою на це особою.

3) При експлуатації об'єктів інформаційної інфраструктури Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують:

– захист електронних повідомлень від спотворення, фальсифікації, переадресації, несанкціонованого ознайомлення та (або) знищення, помилкової авторизації;

– контроль (моніторинг) дотримання встановленої технології підготовки, обробки, передачі та зберігання електронних повідомлень і інформації, що захищається на об'єктах інформаційної інфраструктури;

– автентифікацію вхідних електронних повідомлень;

– взаємну (двосторонню) автентифікацію учасників обміну електронними повідомленнями;

– відновлення інформації про залишки коштів на банківських рахунках і даних власників платіжних карт в разі умисного (випадкового) руйнування (спотворення) або виходу з ладу засобів обчислювальної техніки;

– звірку вихідних електронних повідомлень з відповідними вхідними і обробленими електронними повідомленнями при здійсненні розрахунків в платіжній системі Вестерн Юніон;

– виявлення фальсифікованих електронних повідомлень, в тому числі здійснення операцій, пов'язаних із здійсненням переказів грошових коштів, зловмисником від імені авторизованого клієнта (підміна авторизованого клієнта) після виконання процедури авторизації.

Кібербезпека при здійсненні переказів грошових коштів з використанням ЗКЗІ

Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ здійснюється в наступному порядку.

1) Роботи щодо забезпечення захисту інформації за допомогою СКЗІ проводяться відповідно до закону України "Про електронний підпис" (Відомості Верховної Ради України, 2011, N 15, ст. 2036; N 27, ст. 3880), Положенням про розробку, виробництво, реалізацію та експлуатацію шифрувальних (криптографічних) засобів захисту інформації (Положення ПКЗ-2005), затвердженим наказом служби безпеки України та технічною документацією на ЗКЗІ.

2) У випадку якщо Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури застосовують ЗКЗІ російського виробника, зазначені ЗКЗІ повинні мати сертифікати уповноваженого державного органу.

Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури застосовують ЗКЗІ, які:

– допускають вбудовування ЗКЗІ в технологічні процеси здійснення переказів грошових коштів, забезпечують взаємодію з прикладним програмним забезпеченням на рівні обробки запитів на криптографічні перетворення і видачі результатів;

– поставляються розробниками з повним комплектом експлуатаційної документації, включаючи опис ключової системи, правила роботи з нею, а також обґрунтування необхідного організаційно-штатної забезпечення;

– підтримують безперервність процесів протоколювання роботи ЗКЗІ і забезпечення цілісності програмного забезпечення для середовища функціонування ЗКЗІ, що представляє собою сукупність технічних і програмних засобів, спільно з якими відбувається штатне функціонування ЗКЗІ і які здатні вплинути на виконання пропонованих до ЗКЗІ вимог.

3) У разі застосування ЗКЗІ Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури визначають у внутрішніх документах і виконують порядок застосування ЗКЗІ, що включає:

– порядок введення в дію, включаючи процедури вбудовування ЗКЗІ в автоматизовані системи, які використовуються для здійснення переказів грошових коштів;

– порядок експлуатації ЗКЗІ;

– порядок відновлення працездатності ЗКЗІ у випадках збоїв і (або) відмов у їх роботі;

– порядок внесення змін до програмного забезпечення ЗКЗІ і технічну документацію на ЗКЗІ;

– порядок зняття з експлуатації ЗКЗІ;

– порядок управління ключовою системою;

– порядок поводження з носіями криптографічних ключів, включаючи порядок застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації, призначених для запобігання несанкціонованого використання криптографічних ключів, і порядок дій при зміні і компрометації ключів.

4) Криптографічні ключі виготовляються клієнтом (самостійно), Оператором Послуг Платіжної Інфраструктури і (або) Учасником.

5) Безпека процесів виготовлення криптографічних ключів ЗКЗІ забезпечується комплексом технологічних заходів захисту інформації, організаційних заходів захисту інформації та технічних засобів захисту інформації відповідно до технічної документації на ЗКЗІ.

6) Оператор визначає необхідність використання СКЗІ, якщо інше не передбачено законами та іншими нормативними правовими актами України.

РОЗДІЛ 14. ІНФОРМАЦІЙНА ЗЛОЧИННІСТЬ

Основні поняття інформаційної злочинності

Інформаційний злочин (Кіберзлочин) – дія, що порушує закон, який вчинено з використанням інформаційно-комунікаційних технологій (ІКТ) і/або націлене на мережі, системи, дані, веб-сайти і/або технології, або сприяє вчиненню злочину.

Кіберзлочин відрізняється від традиційного злочину тим, що він «не визнають фізичні або географічні кордони» і можуть відбуватися з меншими зусиллями, більшою легкістю і з більшою швидкістю, ніж традиційні злочини.

Коли ІКТ є частиною способу вчинення злочину, кіберзлочинність включає в себе традиційний злочин, вчинення якого тим чи іншим чином сприяють мережа Інтернет та цифрові технології.

Кіберзлочини вчиняються фізичними особами, групами осіб, комерційними організаціями і державами. Хоча ці суб'єкти можуть застосовувати схожі тактичні методи і атакувати схожі цілі, вони мають різні мотиви і наміри при здійсненні кіберзлочинів.

Зловмисники, які здійснювали кіберзлочини, націлювалися на фізичних осіб і вимагали від них невеликі суми грошей, але потім стали націлюватися на комерційні підприємства, компанії і організації і, нарешті, на інших суб'єктів в приватному і державному секторах, що надають важливі послуги.

Кіберзлочинність є одним з видів транснаціональної злочинності, виконавці і жертви якої можуть перебувати в будь-якій точці світу, де є підключення до мережі Інтернету. У зв'язку з цим слідчим, який веде розслідування кіберзлочинів, найчастіше потрібен транскордонний доступ до даних і обмін ними. Це завдання може бути виконано у разі, якщо запитувані дані зберігаються постачальниками послуг і приймаються

заходи, що дозволяють правоохоронним органам отримувати доступ до даних.

Основними правовими проблемами при розслідуванні кіберзлочинів і судових переслідуваннях кіберзлочинців є:

– різні правові системи, існуючі в різних країнах;

– відмінності в національних законодавствах про кіберзлочинність;

– відмінності в нормах доказового права і кримінального судочинства;

– відмінності в охопленні та географічної застосовності регіональних і багатосторонніх договорів про боротьбу з кіберзлочинністю;

– відмінності в підходах до захисту даних і дотримання прав людини.

Кіберзлочинці часто використовують як технічні, так і соціальні підходи до скоєння злочинів. Деякі види кіберзлочинів важко запобігти, однак користувачі технологій можуть робити певні дії, щоб захистити себе від кіберзлочинності. Інтерпол розміщує численні керівництва з інформування громадськості та профілактики злочинності на своєму веб-сайті. Проте, навіть маленькі дії здатні привнести великі зміни.

Поради, які слід враховувати при підключенні до мережі Інтернет:

– Регулярно оновлюйте операційну систему і встановлене програмне забезпечення.

– Регулярно видаляйте програмне забезпечення, яке ви більше не використовуєте.

– Використовуйте антивірусну програму, розроблену компанією з надійною репутацією.

– Не завантажуйте програмне забезпечення, фільми або музику з сайтів загального доступу – вони часто мають шкідливу програму.

– Не завантажуйте вкладення і не натискайте на посилання від невпізнаних відправників.

– Не надавайте особисту інформацію на невідомих веб-сайтах.

– Підтвердіть правильність адресу веб-сайту при введенні фінансової інформації.

Кіберзлочинність в Україні

Сучасні процеси цифрової трансформації економіки пов’язані з розвитком бізнес-моделей, що використовують цифрові платформи. Фактично протягом останнього десятиріччя відбувається революція платформ. Особливістю цифрових платформ є об’єднання різних груп споживачів, виробників, власників ресурсів на одному віртуальному майданчику. Вітчизняний цифровий капітал перебуває на стадії формування, але вже спостерігається велика кількість позитивних прикладів, оскільки можливості розвитку цифрової економіки в Україні пов’язані з розширенням використання цифрових платформ, що є точками зростання сучасної інформаційної економіки, при цьому перспективним напрямом розвитку цифрових платформ виступає технологія блокчейн.

Організована кіберзлочинність може бути асоційована не тільки з проблемами інформаційної безпеки, але й із загрозами для державної безпеки, військово-промислового і виробничого комплексів, інфраструктури життєзабезпечення. Характеризуючи стан організованої злочинності у сфері економіки, доцільно виділяти її в окрему категорію для вивчення злочинності саме у сфері «цифрової економіки». Оцінка впливу цифрової економіки на національну та світову економіку дозволяє констатувати, що актуальним залишається суцільна модернізація злочинності, що постійно вдосконалюється у рамках активної суцільної електронізації та цифровізації суспільства.

Найбільш поширеними напрямами загроз інформаційній безпеці є шахрайські шкідливі платіжні програми, що ускладнюють, порушують або блокують роботу банківських терміналів, використовуються для крадіжки даних громадян, взлому паролей від банківських карток для заволодіння коштами цих громадян, шахрайства у сфері електронної комерції та

застосування інших кримінальних інструментів і послуг в різноманітніших сферах злочинної діяльності.

Зростання ділової активності із застосуванням хмарних технологіях, придбання товарів через мережу Інтернет, Інтернет-банкінгу, он-лайн розрахунки сприяють зростанню економічних злочинів із застосуванням ІТ-технологій.

До ефективних засобів протидії злочинності у сфері інформаційної безпеки пропонується розробка, створення та впровадження сучасних систем захисту інформації, а також вдосконалення існуючої законодавчої та нормативно-правової бази, здатної забезпечити протидію сучасним кіберзагрозам.

Для підвищення ефективності боротьби з кіберзлочинністю, розвинені країни світу ведуть відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Інциденти в сфері кібербезпеки позначаються на життєдіяльності споживачів інформаційних і багатьох інших послуг та кібератаки, націлені на різноманітні об’єкти інфраструктури систем електронних комунікацій чи управління технологічними процесами.

Забезпечення кібербезпеки можливо тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації. З метою вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та військових цілях країна має активізувати участь в організації спільних міжнародних проєктів з нарощування кібернетичного потенціалу.

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, що здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО.

Важливо підвищувати рівень обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання відповідних освітніх програм. За умов небезпек, що склалися нині у кіберпросторі, організаціям потрібно змінити ставлення до інформаційної безпеки. А для цього треба підвищувати обізнаність про важливість інвестування у кібербезпеку як невід'ємну складову будь-якої національної стратегії розвитку ІКТ.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України CERT-UA функціонує для взаємодії з Cisco Talos Intelligence Group та іншими державами-членами CERT щодо питань подолання наслідків кібератак на інформаційну інфраструктуру, виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектору України та іноземних партнерів. Відповідно до закону "Про основні засади забезпечення кібербезпеки України" (2017), CERT-UA та Центр реагування на кіберзлочини координують заходи, спрямовані на оперативне реагування на кібератаки, а також контролюють впровадження контрзаходів, що передбачають мінімізацію вразливості систем зв'язку.

Україна бере участь у роботі Агентства ЄС з кібербезпеки, Європейського центру з досліджень і компетенції в сфері кібербезпеки, а також у навчаннях з реалізації Спільної оперативної схеми реагування ЄС і держав-членів на кібератаки.

Загалом усі заходи, що проводить світова спільнота у сфері кібербезпеки, – це спроба допомогти країнам вдосконалити цю сферу, а також мотивувати їх на вжиття заходів для покращення їхнього рейтингу, допомагаючи у такий спосіб підвищити загальний рівень кібербезпеки в усьому світі. Рейтинг "Глобального індексу кібербезпеки" допомагає аналізувати та використовувати найкращі засоби боротьби в ІТ-сфері для

подолання та упередження кіберзлочинів та зростання стану їх кібербезпеки.

Потреба координації та переорієнтації наукових досліджень і розробок у сфері інформаційної безпеки, вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробка технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливу атаку та локалізацію джерел загрози є актуальною.

Ця проблема потребує ефективного і комплексного вирішення питань на національному, регіональному та міжнародному рівнях для запобігання кіберзлочинів. Лише співпраця між державами для запобігання постійним загрозам в Інтернеті і подолання проблем кібербезпеки забезпечить належний рівень захисту від сучасних інформаційних загроз.

Виходячи з міжнародного досвіду, оцінкою вартості інформаційного капіталу може бути ринкова капіталізація цифрових платформ, що поступово впроваджуються в Україні. Актуальним є питання безпеки особистих даних, збір великих масивів даних, дистанційна праця.

Сучасні світові тенденції поширення кіберзлочинності та посилення кібератак свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що у свою чергу зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Ситуація, що склалася на сьогоднішній день з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами, розробки інформаційних систем та методів, спрямованих на забезпечення кібербезпеки країни.

Необхідними задачами є розробка національної стратегії з кібербезпеки, що міститиме тактичні та стратегічні пріоритети і завдання у

даній сфері для державних органів. Отже, питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, а тому потребує подальшого розгляду.

Боротьба із інформаційною злочинністю

Від комп'ютерних злочинів страждають всі країни світи. Національна кібербезпека України найбільше стикається з комп'ютерними злочинами в економічній, інформаційній та фінансово-кредитній сферах. Застосування сучасної системи електронного управління повітряним, автомобільним, залізничним, річковим та морським рухом, поширення телекомунікаційної мережі в освіті, науці і практиці, впровадження системи електронних платежів, використання комп'ютерів у діяльності органів законодавчої, виконавчої, судової влади, правоохоронних органів та керуванні військами, розширили сферу діяльності для хакерів, кракерів (хто порушує безпеку системи), кібершахраїв та кібертерористів.

Із розвитком глобальних електронних комп'ютерних мереж набула поширення практика електронного промислового шпигунства. Саме тому проблеми розробки систем захисту та збереження приватної, державної, службової і комерційної таємниці набувають сьогодні особливого значення. Багато питань виникає у зв'язку з крадіжками різного роду послуг, зокрема, вторгнення до телефонних мереж та незаконна торгівля послугами зв'язку. Мережа Інтернет широко використовують торговці піратським програмним забезпеченням, порнографією, зброєю та наркотиками для вчинення власних злочинних дій, обміну інформацією, координації дій тощо. Електронні комп'ютерні мережі, можуть стати й об'єктом нападу кібершахраїв та кібертерористів.

Сьогодні особлива увага приділяється саме питанням міжнародного співробітництва при запобіганні, протидії й розслідуванні комп'ютерних злочинів. У багатьох країнах світу для запобігання і протидії цим видам злочинів створені спеціалізовані кіберпідрозділи, що займаються

виявленням, розслідуванням комп'ютерних злочинів та збором іншої інформації з цього питання на національному рівні. Саме спеціалізовані національні поліцейські підрозділи утворюють головне ядро сил протидії міжнародній комп'ютерній злочинності. Такі підрозділи вже створені і діють тривалий час у Сполучених Штатах Америки, Канаді, Великобританії, Німеччині, Індії, Китаї, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі, Японії та багатьох інших країнах світу.

Законом «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року законодавчо закріплені доктринальні засади забезпечення кібербезпеки нашої країни, а також закладені правові основи діяльності Національного координаційного центру кібербезпеки. Згідно з положеннями цього Закону Національний координаційний центр кібербезпеки є робочим органом Ради національної безпеки і оборони України, який здійснює координацію та контроль за діяльністю суб'єктів сектора безпеки й оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

У Законі «Про основні засади забезпечення кібербезпеки України» передбачено створення урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA. Основними її завданнями є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, що провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України, у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Забезпечення функціонування діяльності CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог чинного законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Слід зазначити, що в багатьох провідних країнах світу вже сформовані і діють загальнодержавні системи кібернетичної безпеки критичної інфраструктури — як найбільш оптимальні організаційні структури, здатні в короткий проміжок часу швидко акумулювати сили та засоби різних державних і правоохоронних органів та установ приватного

сектора для протидії кіберзагрозам, кібератакам, кіберзлочинам, кібершпигунству, кібертероризму. В США, Великій Британії, Канаді довгий час діють потужні кіберполіцейські структури (NIPS, FBI, FATF і тощо). Сьогодні в Сполучених Штатах Америки, Польщі та інших країнах світу створено кібервійська.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена Законом «Про основні засади забезпечення кібербезпеки України» та іншими законами України. Загальна декларація прав людини, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України фактично закладають міцний міждержавний правовий, організаційний, процедурний фундамент забезпечення кібербезпеки інформаційного простору в Україні, Європі і світі.

РОЗДІЛ 15. НОРМАТИВНО-ПРАВОВІ АКТИ З ПИТАНЬ БЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

Положення про захист інформації електронних банківських документів з використанням засобів захисту інформації Національного банку України

1. Це Положення визначає принципи побудови системи захисту інформації та порядок отримання і повернення ЗЗІ організаціями.

2. Безпосередні учасники СЕП отримують ЗЗІ для використання в СЕП та інформаційних задачах незалежно від моделі обслуговування консолідованого кореспондентського рахунку банку в СЕП. Опосередковані учасники СЕП та організації, які не є учасниками СЕП, отримують ЗЗІ для використання їх в інформаційних задачах Національного банку України. Організації взаємодіють за всіма поточними питаннями роботи із ЗЗІ з Департаментом інформаційної безпеки Національного банку України та отримують ЗЗІ в територіальних управліннях Національного банку України за місцем їх розташування. Організації міста Києва і Київської області отримують ЗЗІ в Департаменті інформаційної безпеки.

3. Організації, які використовують ЗЗІ, зобов'язані виконувати організаційні заходи інформаційної безпеки щодо використання, зберігання, обліку ЗЗІ

згідно з Правилами організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженими постановою Правління Національного банку від 26 листопада 2015 року N 829.

4. Департамент інформаційної безпеки здійснює перевірку дотримання вимог Правил в організаціях відповідно до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших

установах, які використовують засоби захисту інформації Національного банку України, затвердженого постановою Правління Національного банку від 26 листопада 2015 року N 829.

5. Організація зобов'язана узгоджувати з Департаментом інформаційної безпеки питання, які можуть виникати під час роботи із ЗЗІ і які не передбачені Правилами.

6. Керівник організації забезпечує дотримання вимог щодо інформаційної безпеки в ній, визначених цим Положенням. II. Принципи побудови системи захисту інформації

7. Система захисту інформації створена для забезпечення конфіденційності та цілісності інформації в електронній формі на будь-якому етапі її оброблення, а також суворої автентифікації учасників СЕП, учасників інформаційних задач і фахівців організацій, які беруть участь у підготовці й обробленні електронних документів.

8. Для забезпечення цілісності інформації, суворої автентифікації та безперервного захисту електронних банківських документів з часу їх формування система захисту інформації використовує механізми формування (перевірки)

ЕЦП на базі несиметричних алгоритмів RSA та ДСТУ 4145-2002.

9. Організація для забезпечення захисту інформації зобов'язана мати трибайтний унікальний ідентифікатор, перший символ якого є літерою на позначення відповідної території, на якій вона розташована, другий і третій символи утворюють унікальний ідентифікатор організації в межах цієї території. Унікальний ідентифікатор має бути узгоджений з адресою організації в системі електронної пошти Національного банку. Унікальний ідентифікатор записується в ПМГК та АКЗІ, які надаються організації, та не може бути нею змінений, що забезпечує захист від підроблення ключової інформації від імені іншої організації. Ідентифікатори ключів криптографічного захисту, що використовуються організацією, складаються з шести символів, з яких перші три є унікальним

ідентифікатором організації, четвертий символ визначає тип робочого місця учасника СЕП (операціоніст, бухгалтер тощо) або тип інформаційної задачі, п'ятий і шостий – ідентифікатор робочого місця або відповідальної особи.

10. Організація забезпечує захист електронних банківських документів, шифрування/дешифрування і накладання/перевірку ЕЦП за допомогою таких криптографічних ЗЗІ:

– апаратно-програмних ЗЗІ, до складу яких входять АКЗІ, СК, програмне забезпечення керування АКЗІ, що вбудоване в АРМ-СЕП і не може бути вилучене або використане окремо, з відповідними ТВК та криптобібліотеками;

– програмних ЗЗІ, до складу яких входять програмний модуль для шифрування, вбудований в АРМ-СЕП, ПМГК з незаповненими ТВК, носіїв ТК, відповідними ТВК та криптобібліотеками.

11. Національний банк забезпечує побудову ключової системи криптографічного захисту для СЕП та інформаційних задач. Ця система складається з ключів програмних ЗЗІ, що генеруються в організаціях за допомогою наданих ПМГК, і ключів апаратних ЗЗІ, які генеруються безпосередньо АРМ-СЕП за допомогою АКЗІ.

12. Основними ЗЗІ в АРМ-СЕП є АКЗІ. Адміністратор АРМ-СЕП здійснює генерацію ключової пари (ТК та ВК) для АКЗІ на комп'ютері, де розміщується АРМ-СЕП, за допомогою програмного забезпечення керування АКЗІ, що вбудоване в АРМ-СЕП. Генерація здійснюється відповідно до алгоритму, визначеного в національному стандарті України ДСТУ 4145-2002. Для забезпечення безперебійної роботи АРМ-СЕП з апаратурою захисту адміністратор АРМСЕП повинен записувати ТК на дві СК (основну та резервну). Ключова інформація під час роботи АКЗІ використовується виключно на рівні АКЗІ, що унеможливлює підроблення та перехоплення ключової інформації. У разі виходу з ладу АКЗІ адміністратор АРМ-СЕП здійснює перехід до роботи з програмними ЗЗІ.

13. За допомогою ПМГК організація має право генерувати ключову пару (ТК та ВК) відповідно до несиметричного алгоритму RSA для всіх робочих місць, де працюють з електронними банківськими документами. Кожен ТК робочого місця захищений особистим паролем відповідальної особи, яка працює з цим ключем.

Для забезпечення захисту ключової інформації від несанкціонованої модифікації адміністратор інформаційної безпеки надсилає ВК до Департаменту інформаційної безпеки для сертифікації.

Департамент інформаційної безпеки здійснює сертифікацію ВК та надсилає засобами системи електронної пошти Національного банку на адресу організації відповідні сертифікати ВК. Організація вживає заходів щодо своєчасного оновлення ТВК відповідно до експлуатаційної документації для АРМ-СЕП, АРМ-НБУ-інф, САБ та інформаційних задач.

16. Департамент інформаційної безпеки надає криптобібліотеки безкоштовно всім організаціям, які використовують ЗЗІ, для вбудовування в програмне забезпечення САБ або інше відповідне програмне забезпечення.

17. В організації використовуються такі ЗЗІ:

– АКЗІ (для безпосереднього учасника СЕП) 1

– СК (для безпосереднього учасника СЕП) 2

– ПМГК 1

– Копія ПМГК 1

– ТКАРМ-СЕП (для безпосереднього учасника СЕП) 1 + копія

– ТК АРМ-НБУ-інф 1 + копія

– ТК АРМ бухгалтера САБ (для безпосереднього учасника СЕП). За кількістю відповідальних осіб, але не більше 5

– ТК технолога (для безпосереднього учасника СЕП). За кількістю відповідальних осіб, але не більше 5

– ТК операціоністів (для безпосереднього учасника СЕП). За кількістю відповідальних осіб

– ТК інших робочих та технологічних місць для інформаційних задач. За вказівками Національного банку

16. Центральна розрахункова палата Національного банку надає консультації щодо супроводження АРМ-СЕП/АРМ-НБУ-інф, а також технологічного процесу проходження електронних платежів у СЕП та електронних документів в інформаційних задачах. ІІІ. Порядок отримання і повернення ЗЗІ

17. Умовами для отримання ЗЗІ є:

– лист-звернення від організації-замовника до Департаменту інформаційної безпеки про укладення договору із зазначенням для цієї організації-замовника та її філій, якщо такі існують, унікального ідентифікатора, коду банку, назв інформаційних задач, з якими планують працювати, а також орієнтовної дати початку роботи в цих задачах;

– укладення договору про використання засобів захисту інформації Національного банку України між організацією-замовником та Національним банком;

– забезпечення відповідності приміщень, у яких будуть оброблятися електронні банківські документи, використовуються та зберігаються ЗЗІ, вимогам, визначені Правилами;

– призначення посадових осіб, відповідальних за зберігання та використання ЗЗІ;

– лист-доручення (довіреність) про отримання конкретних ЗЗІ особі, відповідальній за отримання ЗЗІ для організації.

18. Департамент інформаційної безпеки проводить перевірку готовності організації замовника, її філій до включення в СЕП та інформаційні задачі відповідно до розділу ІІІ Положення про порядок перевірки.

19. Департамент інформаційної безпеки від імені Національного банку та організація замовник укладають між собою договір відповідно до зразка, викладеного в додатку 1 до цього Положення. Організація-

замовник здійснює оплату Національному банку всіх послуг, наданих Національним банком за цим договором як організації-замовнику, так і її філіям.

Організація-замовник зобов'язана внести зміни до договору в разі:

– переходу на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку банку на іншу;

– зміни місцезнаходження філії з однієї області України на іншу;

– появи нових філій або закриття наявних. Організація-замовник зобов'язана переукласти договір у разі зміни свого місцезнаходження з однієї області України на іншу і отримати ЗЗІ з новим ідентифікатором, який відповідає новому місцезнаходженню.

20. Департамент інформаційної безпеки в разі відсутності недоліків за результатами перевірки готовності включення організації в СЕП та/або інформаційні задачі:

– виготовляє ЗЗІ для цієї організації;

– надає ЗЗІ організації через територіальне управління за місцезнаходженням організації або безпосередньо для міста Києва та Київської області.

21. Відповідальна за отримання ЗЗІ особа організації зобов'язана прибути до територіального управління за місцем розташування організації з документом, який засвідчує особу, та листом-дорученням або довіреністю, які надають право на отримання/заміну ЗЗІ, для отримання ЗЗІ з оформленням акта про приймання-передавання апаратних засобів захисту інформації Національного банку України (додаток 2).

22. Департамент інформаційної безпеки разом з документом на отримання/заміну ЗЗІ зберігає один примірник, а організація – другий примірник акта про приймання передавання апаратних засобів захисту інформації Національного банку України, за яким АКЗІ та смарт-картки передаються в організацію, а також зберігає копію супровідного листа, а

організація – супровідний лист, згідно з яким ПМГК передається в організацію.

Департамент інформаційних технологій Національного банку постачає криптобібліотеки, необхідні для роботи АРМ-СЕП і АРМ-НБУ-інф, разом з цими АРМ, у тому числі в разі їх оновлень – разом з оновленнями програмного забезпечення цих АРМ. Криптобібліотеки та програмний модуль криптографічного захисту інформації, вбудований в АРМ-СЕП, обліку і поверненню не підлягають.

Криптобібліотеки, призначені для вбудування в САБ або інше програмне забезпечення, постачаються за окремим листом Департаменту інформаційної безпеки або за запитом від організації.

23. Для завершення підготовки до включення в СЕП організація зобов'язана виконати генерацію ключів для АРМ-СЕП та отримати їх сертифікати за один робочий день до включення до Довідника учасників СЕП.

24. Організація, яка отримала ЗЗІ, не має права:

– передавати їх третім особам, установам чи організаціям, а також іншим установам однієї юридичної особи;

– використовувати їх за іншим місцезнаходженням, ніж це зазначено в договорі;

– використовувати їх в інших платіжних системах банків, у територіально відокремлених відділеннях (філіях) банків.

25. Організація зобов'язана повернути ЗЗІ до Департаменту інформаційної безпеки через територіальне управління в разі:

– ліквідації;

– припинення роботи із ЗЗІ, а саме: виключення з учасників СЕП;

– переходу на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку банку на іншу;

– зміни місцезнаходження з однієї області України на іншу;

– виходу з ладу ЗЗІ;

– на вимогу Департаменту інформаційної безпеки в разі виявлення суттєвих порушень в організації захисту електронних банківських документів.

26. Організація зобов'язана повернути АКЗІ разом із СК до Департаменту інформаційної безпеки через територіальне управління в разі виходу АКЗІ з ладу або отримання від Департаменту інформаційної безпеки листа з вимогою повернення ЗЗІ протягом трьох робочих днів з укладенням акта про приймання-передавання апаратних засобів захисту інформації Національного банку України, один примірник якого зберігає Департамент інформаційної безпеки, другий – організація.

27. Організація у випадках, передбачених підпунктами 1 і 2 пункту 27, зобов'язана:

– повідомити Департамент інформаційної безпеки про передбачувані строки і порядок виключення з учасників СЕП, переходу на іншу модель обслуговування консолідованого кореспондентського рахунку банку або зміни місцезнаходження, погодити перелік ЗЗІ, що підлягають поверненню до Департаменту інформаційної безпеки;

– ужити заходів щодо повернення до Департаменту інформаційної безпеки, знищення на місці і передавання до архіву організації ЗЗІ, справ, журналів обліку зі складанням відповідного акта (додаток 3);

– повернути до Департаменту інформаційної безпеки через територіальне управління ЗЗІ з актом, зазначеним у підпункті 2 цього пункту, один примірник якого зберігає Департамент інформаційної безпеки, другий -організація.

28. Організація, яка використовує ЗЗІ, зобов'язана виконувати організаційні вимоги щодо їх отримання, використання та зберігання і своєчасної заміни відповідних ключів до них. Департамент інформаційної безпеки має право вилучати з організації ЗЗІ в разі невиконання вимог щодо використання та зберігання ЗЗІ і вимог до приміщень.

Заходи інформаційної безпеки в СЕП

29. Технологічні засоби контролю, вбудовані в програмно-технічні комплекси СЕП, не можуть бути відключені. У разі виявлення нестандартної ситуації, яка може свідчити про підозру щодо несанкціонованого доступу до СЕП від імені певного учасника СЕП, ЦОСЕП автоматично припиняє приймання початкових електронних розрахункових документів та повідомлень від цього учасника.

30. Основним засобом шифрування файлів (пакетів) СЕП є АКЗІ. Робота АКЗІ контролюється вбудованими в ЦОСЕП і АРМ-СЕП програмними ЗЗІ і забезпечує апаратне шифрування (розшифрування) інформації за алгоритмом, визначеним у національному стандарті України ДСТУ ГОСТ 28147:2009.

Як резервний засіб шифрування в СЕП використовується вбудована в ЦОСЕП і АРМ-СЕП функція програмного шифрування.

31. Засоби шифрування ЦОСЕП і АРМ-СЕП (як АКЗІ, так і програмне шифрування) забезпечують сувору автентифікацію відправника та отримувача електронного банківського документа, цілісність кожного документа в результаті неможливості його підроблення або несанкціонованого модифікування в шифрованому вигляді. АРМ-СЕП і ЦОСЕП у режимі реального часу забезпечують додаткову сувору взаємну автентифікацію під час установлення сеансу зв'язку.

Під час роботи АРМ-СЕП створює журнали програмного та апаратного шифрування і захищений від модифікації протокол роботи АРМ-СЕП, у якому фіксуються всі дії, що ним виконуються, із зазначенням дати та часу оброблення електронних банківських документів. Наприкінці банківського дня журнали програмного та апаратного шифрування і протокол ро□боти АРМ-СЕП підлягають обов'язковому збереженню в архіві.

32. Департамент інформаційної безпеки надає банкам (філіям) інформаційні послуги щодо достовірності інформації за електронними

банківськими документами в разі виникнення спорів на основі копії архіву роботи АРМ-СЕП за відповідний банківський день.

Департамент інформаційної безпеки розшифровує копію цього архіву та визначає:

– ідентифікатор банку – учасника СЕП, який надіслав (зашифрував) електронний банківський документ;

– ідентифікатор банку – учасника СЕП, якому адресовано електронний банківський документ;

– дату, годину та хвилину виконання шифрування електронного банківського документа;

– дату, годину та хвилину розшифрування електронного банківського документа;

– відповідність усіх електронних цифрових підписів, якими був захищений від модифікації електронний банківський документ.

Під час використання АКЗІ додатково визначаються:

– номер АКЗІ, на якій виконувалося шифрування або розшифрування електронного банківського документа;

– номер СК, якою користувалися під час шифрування або розшифрування електронного банківського документа.

33. Департамент інформаційної безпеки надає послуги щодо розшифрування інформації за електронними банківськими документами, якщо між учасниками СЕП виникли спори з питань, пов'язаних з електронними банківськими документами, у разі:

– невиконання автентифікації або розшифрування електронного банківського документа;

– відмови від факту одержання електронного банківського документа;

– відмови від факту формування та надсилання електронного банківського документа;

– ствердження, що одержувачу надійшов електронний банківський документ, а насправді він не надсилався;

– ствердження, що електронний банківський документ був сформований та надісланий, а він не формувався або було надіслане інше повідомлення;

– виникнення спору щодо змісту одного й того самого електронного банківського документа, сформованого та надісланого відправником і одержаного та правильно автентифікованого одержувачем;

– роботи з архівом роботи АРМ-СЕП під час проведення ревізій тощо.

Департамент інформаційної безпеки надає учасникам СЕП письмові відповіді щодо порушених питань.

Внутрішній контроль за станом інформаційної безпеки в організації.

34. Організація зобов'язана інформувати Департамент інформаційної безпеки впродовж одного робочого дня телефоном та протягом трьох робочих днів листом засобами системи електронної пошти Національного банку в таких випадках:

– виконання (спроби виконання) фіктивного платіжного документа;

– компрометація ЗЗІ;

– пошкодження ЗЗІ;

– несанкціоноване проникнення в приміщення з АРМ-СЕП/АРМ-НБУ-інф ;

– проведення правоохоронними органами та іншими органами державної влади перевірки діяльності організації, унаслідок якої створюються умови для компрометації ЗЗІ;

– виникнення інших аварійних або надзвичайних ситуацій, що створюють передумови до розкрадання, втрати, пошкодження тощо ЗЗІ.

35. Внутрішній контроль за станом інформаційної безпеки відповідно до вимог нормативно-правових актів Національного банку в діяльності організації забезпечують:

-керівник організації;

-заступник керівника організації або особа, яка за своїми службовими обов'язками чи за окремим внутрішнім документом організації призначена відповідальною особою за організацію інформаційної безпеки.

36. Адміністратор інформаційної безпеки забезпечує поточний контроль за дотриманням вимог інформаційної безпеки під час використання та зберігання ЗЗІ в організації.

37. Службові особи організації, які відповідають за інформаційну безпеку, зобов'язані надавати письмові або усні відомості про стан ЗЗІ та їх використання, стан захисту інформації в програмному забезпеченні САБ та інших системах, на які поширюються вимоги Національного банку щодо інформаційної безпеки, технологію оброблення електронних банківських документів в організації та систему захисту інформації під час їх оброблення на вимогу Департаменту інформаційної безпеки.

Список використаних джерел

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
2. Закон України “Про захист персональних даних” (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України “Про національну безпеку (2018)
5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
15. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с.
16. А.М. Гребенюк, Л.В. Рибальченко. Основи управління інформаційною безпекою: навч. Посіб. Дніпро: Дніпроп. держ. ун□т внутріш. справ, 2020. – 144 с.
17. Головань СМ., Васюков І.В., Давиденко А.М., Хорошко В.О., Щербак Л.М. Основи організації електронного документообігу: У 2 т./ – К.: ДУІКТ, 2008. – Т. 1. – 230 с., Т. 2. – 233 с.
18. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М. Конфіденційне діловодство. Практикум: Навч. Посіб. – Луганськ: СНУ ім. В.Даля, 2010. – 180 с.
19. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.
20. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
21. 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.
22. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою / В. В. Домарєв, Д. В. Домарєв, С. Б Гордієнко. // Вісник Державного університету інформаційно-комунікаційних технологій. – 2012. – Т. 10, № 2. – С. 102-104.
23. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
24. Зубок М. І. Безпека банківської діяльності: навч. посібник / Зубок . І. — К. : КНЕУ, 2002. — 190 с.

25. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник.-К. ДУІКТ, 2010. - 316 с.
26. Лужецький В.А. Захист персональних даних. Навчальний посібник./ Лужецький В.А., Войтович О.П., Дудатьєв А.В – Вінниця: ВНТУ, 2009. –487 с.
27. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-СУМ-Вінниця, 2009. – 240 с.
28. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О.Хорошка – К.: Видавництво НАУ, 2002. – 208с.
29. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
30. Юдін О. К. Захист інформації в мережах передачі даних: підруч. / Г. Ф. Конахович, О. Г. Корченко, О. К. Юдін. — К.: Вид-во ТОВ НВП «ШТЕРСЕРВІС», 2009. — 714 с.
31. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. — К. : НАУ, 2011. — 640 с.
32. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ ―НВП‖ІНТЕРСЕРВІС‖, 2009. – 716 с.

Усік Павло Сергійович

Буравченко Костянтин Олегович

БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ

Навчальний посібник

© РВЛ ЦНТУ, просп. Університетський, 8, м. Кропивницький, 25006.

Тел. (0522) 559-245, www.kntu.kr.ua