ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

В.М. Ахрамович

КУРС ЛЕКЦІЙ

з навчальної дисципліни

КІБЕРБЕЗПЕКА БАНКІВСЬКИХ та КОМЕРЦІЙНИХ СТРУКТУР

Навчальний посібник

В.М. Ахрамович

КУРС ЛЕКЦІЙ

з навчальної дисципліни

«Кібербезпека банківських та комерційних структур»

Київ 2019

ISBN 978-5-9614-4112-3.

УДК 336.71

ББК 32. 884
А95
Схвалено Вченою радою Навчально-наукового інституту захисту інформації. Державного університету телекомунікацій
(протокол № 6 від 21 січня 2019 р.).

Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» /В.М.Ахрамович. Державний університет телекомунікацій. – К.:ДУТ, 2019. – 163 с. іл. – Бібліограф.: 166 с.

ISBN 978-617-571-028-9

Основна частина курсу лекцій присвячена розв'язку теоретичних та практичних завдань з ознайомлення й дослідження особливостей кіберзахисту програмного й апаратного забезпечення в сучасних мережах фінансових установ. Вивчення лекцій покликано поставити студента в ситуацію схожу з виробничою, коли потрібно налагодити й підтримувати обчислювальні мережі, а також середовище їх функціонування в рамках підрозділу, банку, підприємства. Лекції знайомлять студента не тільки із правильними сценаріями розв'язку того або іншого завдання, але й дозволяють побачити основні ознаки й симптоми вразливостей можливого некоректного налагодження політики безпеки, мережевого встаткування й програмного забезпечення в результаті тих або інших розповсюджених помилок.

В лекціях послідовно розкриті питання: основні положення кібербезпеки банків та комерційних установ; поняття банківської таємниці; вразливості , ризики, управління ризиками кібербезпеки банків; політика безпеки банківських установ; системи управління кібербезпекою в банківських установах; кібербезпека в автоматизованих системах банківських установ; основні положення кібербезпеки в мережі передачі даних SWIFT; основні положення кібербезпеки даних в мережі банкоматів; положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України; правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи; вимоги до захисту інформації при здійсненні переказів грошових коштів в Платіжній Системі Вестерн Юніон; нормативно-правові акти з питань інформаційної безпеки в банках.

У всіх лекціях наведені посилання на стандарти та інші нормативно - правові акти з безпеки банків та фінансових установ.

УДК 336.71

ББК 32. 884
ISBN 978-5-9614-4112-3.

© В.М. Ахрамович 2019

© Державний університет телекомунікацій (ДУТ), 2019

Зміст

Вступ

В умовах широкого застосування обчислювальної техніки і засобів обміну інформацією поширюються можливості її просочення 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. Останнім часом у засобах масової інформації з'явилося безліч сенсаційних повідомлень про факти злочинних впливів на автоматизовані системи обробки, зберігання і передачі інформації, особливо в кредитно-банківській діяльності.

За деякими даними, в промислово розвинених країнах середній збиток від одного злочину в сфері комп`ютерної інформації близький до 450 тис. дол., а щорічні сумарні втрати в США і Західній Європі, за даними, що наводять Гайкович В та Прешин А., досягають 100 млрд. і 35 млрд. дол. В останні десятиріччя зберігалася стійка тенденція до зросту збитків, пов'язаних з злочинністю в сфері комп'ютерної інформації. В пресі та літературі наводиться багато подібних прикладів.

Комерційним і фінансовим установам доводиться реалізовувати широкий набір заходів, щоб захистити себе від таких злочинів. Наслідки недооцінки питань безпеки можуть виявитися вельми сумними. Досить згадати про великі суми, викрадені за допомогою підробних авізо. На жаль, досвід західних фірм дає небагато підстав сподіватися, що цей перелік не буде продовжений у майбутньому в нашій країні.

Найбільшу небезпеку для банків представляє кібернетична незахищеність, тому при вирішенні даної проблеми банку необхідно враховувати те, що однією з головних умов стабільного функціонування кожного банку - є обмін інформацією. Розглянемо питання інформаційної безпеки більш детально.

З метою протидії злочинам у сфері комп`ютерної інформації або зменшення збитків від них необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації від просочування та несанкціонованого доступу до неї. 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 набагато більш уразливої.

Кібербезпека банку досягається організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу в банку, аналітичної обробки інформації; організацією системи інформаційного забезпечення рішень керівництва банку; визначенням категорій банківської інформації та виробленням відповідних заходів щодо її захисту; дотриманням відповідних режимів діяльності банку; виконан-

ням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів втрати інформації.

Проведений аналіз та практичний досвід показують, що в якості базової змістовної моделі забезпечення безпеки інформації необхідно використовувати модель, що визначається міжнародним стандартом ISO/IEC 15408 «Єдині критерії оцінки безпеки систем інформаційних технологій» та ISO/IEC 15446 «Керівництво з розробки профілю захисту та проекту безпеки». Функціональні вимоги інформаційної безпеки згруповані на основі 11 функціональних класів (в трьох групах), 66 сімейств, 135 компонентів.

Визначення порядку захисту інформації, організації роботи з нею здійснюється відповідно до Положення про організацію роботи з інформацією, що становить банківську і комерційну таємницю та є конфіденційною. Положення передбачає: права співробітників банку та інших осіб щодо отримання інформації з обмеженим доступом, обов'язки посадових осіб і службовців банку щодо роботи з грифованими документами, виробами та засобами, правила ведення конфіденційних переговорів за допомогою засобів зв'язку, спілкування з клієнтами та відвідувачами; правила оформлення доступу до інформації з обмеженим доступом, порядок розроблення, зберігання, пересилання та руху грифованих документів в установах банку; загальні обов'язки персоналу банку щодо зберігання його таємниць; порядок доступу на засідання і наради, де обговорюються питання, в яких присутня інформація з обмеженим доступом; інші питання, що регулюють правила доступу до інформації з обмеженим доступом. Окремим наказом по банку може оголошуватись список осіб, яким у повному обсязі може доводитись інформація, що становить банківську і комерційну таємницю та є конфіденційною.

Конспект лекцій має передусім спонукати читачів до самостійного пошуку практичних заходів із протидії сторонньому кібернетичному впливу за тих чи інших конкретних умов.

.

Лекція 1 Основні положення кібербезпеки банків та комерційних установ (3 год)

План лекції

1. Інформаційна безпека банківської установи. Суть, мета, завдання.
2. Національний банк України як суб'єкт вітчизняної системи кібербезпеки
3. Безпека автоматизованих систем обробки інформації банку
4. Міжнародна співпраця з кібербезпеки.

1. Інформаційна безпека банківської установи. Суть, мета, завдання.

Розглянемо спочатку коротко поняття безпеки банку взагалі. А далі в цьому контексті будемо розглядати управління інформаційною безпекою банківської установи.

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

Тому у процесі розроблення концепції управління банківською діяльністю варто виділити основні процеси функціонування банку і виключити можливість витоку інформації, її несанкціонованого використання, нанесення збитків, упущення вигоди з боку всіх зацікавлених сторін і в напрямі досягнення основних цілей банківської діяльності. Реалізація цих положень гармонійно вписується в концепцію корпоративного управління банківською діяльністю, до якої сьогодні залучаються дедалі більше банків.

Управління інформаційною безпекою банку і повинно стати частиною цієї концепції.

Головним **критерієм ефективності та якості інформаційної безпеки** банку є стійкість його фінансового та економічного розвитку згідно з планами і завданнями незалежно від зміни ситуації.

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 (слабкість одного або декількох активів, яка може бути використана однією або декількома загрозами);

- запобігання інцидентам інформаційної безпеки;
- нейтралізація або мінімізація загроз інформаційній безпеці банку.

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

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

У структурі інформаційної безпеки банківської установи виділяють такі основні складові:

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

Інформаційні ресурси банківської установи – це взаємозв'язана, упорядкована, систематизована інформація, 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: телерадіо-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 (підприємства, установи) є індивідуальним.

Зазначимо, що для **банківських установ процеси забезпечення інформаційної безпеки регламентовано краще, ніж для багатьох інших галузей**: існують закони і стандарти забезпечення належного рівня інформаційної безпеки, якими банки повинні керуватися у своїй діяльності, зокрема: Закони Украї-

ни “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.

Застосування стандартів з управління інформаційною безпекою в практиці банківської діяльності дає можливість:

- оптимізувати вартість побудови та підтримання системи управління інформаційною безпекою;
- постійно відстежувати та оцінювати ризики з урахуванням цілей діяльності банків;
- ефективно виявляти найкритичніші ризики та зменшувати ймовірність їх реалізації;
- створювати ефективні стратегії інформаційної безпеки та дотримуватись її виконання;
- ефективно розробляти, впроваджувати та тестувати банківські інформаційні системи та сучасні інформаційно-комунікаційні технології підтримки банківської діяльності;
- забезпечити управління процесами підтримки інформаційної безпеки в банках і в загальній банківській системі тощо.

Міжнародні стандарти управління інформаційною безпекою серії ISO 27000, дотримання яких є обов’язковим у банківській системі України, щодо інформаційної безпеки організації використовують такі основні терміни і поняття:

інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, спостережність, неспростовність та надійність (при цьому для банків України автентичність, спостережність, неспростовність, надійність та автентифікація користувачів та інформаційних ресурсів є обов`язковими вимогами інформаційної безпеки);

засоби оброблення інформації (information processing facilities) – будь-яка система оброблення інформації, послуга чи інфраструктура, чи місце, де вони фізично розміщені (для банків України засобами оброблення інформації можуть бути власні програмно-технічні комплекси або автоматизовані робочі місця державних/міжнародних платіжних/ інформаційних систем);

система управління інформаційною безпекою (СУІБ) (information security management system ISMS) – 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 (information security event) – ідентифікована подія системи, служби або мережі, яка вказує на можливе порушення полі-

тики інформаційної безпеки або відмову засобів захисту чи раніше невідому ситуацію, яка може мати відношення до безпеки;

інцидент інформаційної безпеки (information security incident) – одна або серія небажаних чи непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації бізнес-операцій і загрози інформаційній безпеці;

загроза (threat) – потенційна причина небажаного інциденту, який може призвести до шкоди для системи або організації;

вразливість (vulnerability) – слабкість ресурсу СУІБ або групи ресурсів СУІБ, якою можуть скористатися одна або більше загроз;

ризик (risk) – 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 (risk evaluation) – процес порівняння кількісно оціненого ризику із заданими критеріями ризику для встановлення його значимості;

управління ризиком (risk management) – скоординовані дії в організації щодо регулювання та контролю ризику (управління ризиком зазвичай містить оцінку ризику, оброблення ризику, прийняття ризику і доведення ризику до відома);

заходи безпеки (control) – засоби управління ризиком, які включають політику, процедури, настанови, практику або організаційні заходи, які можуть бути адміністративного, технічного, управлінського або правового характеру;

політика (policy) – 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 (під час оцінювання ризику ідентифікують загрози ресурсам СУІБ і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу);

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.

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

- закони України;
- нормативно-правові акти Національного банку України;
- стандарти Національного банку України;
- вимоги платіжних систем та систем переказу коштів;
- внутрішні нормативні документи банку;
- умови угод та договорів з третіми сторонами тощо.

Важливим є те, що вимоги з інформаційної безпеки для платіжних систем та систем переказів коштів висуваються платіжною організацією платіжної системи та системи переказу коштів, тому вони можуть відрізнятися від вимог Національного банку України (крім Системи електронних платежів (СЕП) та Національної платіжної системи “Український платіжний простір” або “Простір” (НПС “Простір”), які є платіжними організаціями Національного банку України).

Особливу увагу слід звернути на умови угод та договорів з третіми сторонами. Відповідно до п. 6.2 стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010 безпека інформації та засобів оброблення інформації банку не повинна знижуватися через уведення в експлуатацію продуктів або послуг зовнішньої сторони. Якщо є бізнес-потреба в роботі із зовнішніми сторонами, яка може вимагати доступу до інформації або засобів оброблення інформації банку, або в отриманні від зовнішньої сторони чи наданні їй продукту та послуги, тоді банк повинен викону-

вати оцінку ризику для визначення вимог щодо заходів безпеки та наслідків порушення безпеки. Заходи безпеки мають бути погоджені та визначені в угоді із зовнішньою стороною. Ці питання розглядаються не тільки для договорів про надання послуг клієнтам банку (системи типу "клієнт-банк", Інтернет-банкінг, мобільний банкінг тощо), а також при отриманні послуг зовнішніх сторін (розроблення та супроводження програмного забезпечення, придбання та технічне обслуговування обладнання, надання послуг зв'язку тощо).

Оцінювання інформаційної безпеки банківської установи здійснюється з позицій основних **сервісів інформаційної безпеки**, до яких належать:

- конфіденційність (confidentiality);
- цілісність (integrity);
- доступність (availability);
- спостережність (accountability) – 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/банківського продукту, програмно-технічного комплексу банку. Слід зазначити, що для різних бізнес-процесів/банківських продуктів 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 / банківських продуктів банку.

2. Національний банк України як суб'єкт вітчизняної системи кібербезпеки

Відповідно до **Стратегії кібербезпеки України** на Національний банк України покладено завдання із формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері.

Крім того, згідно з Законом України «Про Національний банк України», НБУ визначає напрями розвитку сучасних електронних банківських технологій, створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених ним платіжних та облікових систем, встановлює для банків правила захисту інформації, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації.

НБУ має у своєму складі окремий структурний підрозділ – **Департамент безпеки**, однією з основних функцій якого є «розроблення та реалізація стратегії і політики інформаційної безпеки НБУ, упровадження новітніх технологій у частині забезпечення ефективного і цілеспрямованого захисту інформації в інформаційній інфраструктурі НБУ та банківської системи України».

В НБУ використовуються сучасні системи кібербезпеки такі як: Intrusion Prevention System, Wireless Intrusion Protection System, Security information and event management, Vulnerability scanner, Secure Web Gateway, Network firewall.

Водночас, у зв'язку із відсутністю в НБУ необхідних ресурсів, залишається не вирішеною проблема сертифікації засобів криптографічного захисту інформації, що використовуються Нацбанком. Зазначене потребує врегулювання цього питання із Держспецзв'язку, як державним органом, відповідальним за проведення державної експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації в державі.

Надійне функціонування електронних банківських платіжних систем, їх захищеність від потенційних кіберзлочинців є важливою складовою банківської системи, адже не тільки забезпечує права і законні інтереси громадян і держави у фінансовій сфері та гарантує її стабільний розвиток, а й формує рівень довіри громадськості та бізнесу до вітчизняного банківського сектору, зокрема, до електронних платіжних систем та безготівкових розрахунків. Зазначене є вкрай важливим з огляду на обраний нашою країною курс на інформатизацію та розширення безготівкового грошового обігу.

Водночас, останнім часом кількість кібератак на банківській сектор України критично зростає. Банківська система України є однією зі сфер, де найбільш широко та **активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет**. А враховуючи, що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більшу увагу злочинців.

Наслідком значної кількості кіберзлочинів у вказаній сфері є зниження довіри громадян в цілому до надійності фінансової системи, інституту банківської таємниці, надійності захисту персональних даних, а також до фінансових операцій, що проводяться з використанням новітніх технологій. При цьому недовіра населення до ринків фінансових послуг не дає можливості активно використовувати вільні кошти громадян як інвестиційні ресурси, що спрямовуються на розвиток економіки.

Значна частина кіберзлочинів стає можливою завдяки необізнаності населення те недотриманню основних правил безпеки, у зв'язку з цим, значну користь у попередженні кіберзлочинності, мають інформаційно-просвітницькі заходи щодо нових ризиків та загроз в інформаційних та комп'ютерних системах. Національним банком України з метою попередження шахрайства з платіжними картками розроблено Рекомендації держателям платіжних карток щодо їх використання, які розміщені на офіційній сторінці Національного банку України в мережі Інтернет у розділі «Платіжна система» (http://www.bank.gov.ua/doccatalog/document?id=70904).

Крім того, у 2011 році Департамент інформатизації НБУ на виконання пункту 2 постанови Правління Національного банку України від 28.10.2010 N 474 «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України» розробив Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. Згадана іні-

ціатива була спрямована на підвищення захисту інформаційно-телекомунікаційних систем банків України відповідно до міжнародних стандартів та зменшення їх операційних ризиків. Для ефективної протидії кібератакам на банки України потрібно терміново організувати обмін інформацією про атаки між учасниками банківського ринку, а також налагодити обмін такою інформацією з подібними центрами за кордоном. Центр реагування на інциденти кібербезпеки у банківський системі та платіжному просторі України (CERT-NBU), а також визначити порядок взаємодії CERT-NBU з командами реагування на комп'ютерні інциденти інших суб'єктів забезпечення кібербезпеки, правоохоронними органами та банками України.

Водночас, для вдалої реалізації будь-яких ініціатив НБУ у сфері кіберзахисту банківського сектору необхідно не просто формальний підхід до розроблення, впровадження, функціонування системи управління безпекою власних ІТС з боку керівництва і працівників банків, а реальна зацікавленість у підвищенні рівня її кіберзахисту. Адже за відсутності правового механізму, який би зобов'язував приватні банківські установи забезпечувати належний кіберзахист власних інформаційних систем та повідомляти НБУ про будь які кібератаки чи кіберінциденти, функції НБУ у сфері кіберзахисту банківської сфери фактично зводились до розроблення рекомендацій банкам України щодо захисту власних ІТС.

Саме з метою запровадження такого механізму у вересні 2017 р. і було прийнято з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». Вказане Положення встановлює:

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.

3. Безпека автоматизованих систем обробки інформації банку

Під безпекою автоматизованих систем обробки інформації банку необхідно розуміти таку їх властивість, що полягає у спроможності протидіяти спробам завдання збитків власникам і користувачам системи, тобто захищеності від спроб розкрадання чи руйнування її компонентів.

Таким чином, 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 банківських автоматизованих системах 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 аутентифікація 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. Наприклад, контроль за доступом, тобто обмеження можливостей використання ресурсів системи програмами, процесами і користувачами згідно з політикою безпеки забезпечує захист не тільки від зовнішніх і внутрішніх зловмисників, але в тому числі дозволяє захиститися від помилок персоналу, що призводять до втрат еквівалентним реалізації атаки зловмисником.

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. Аутентифікація – встановлення автентичності. Нові можливості дозволяють використовувати багатофакторну посилену ідентифікацію при авторизації в банківській системі. Така аутентифікація 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, тобто захист від несанкціонованої модифікації суб'єктів системи. Це фактично – 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 криптографічний 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 алгорит-

мів 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 модель власно діючого підпису в електронному вигляді певної посадової особи. 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. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, що є фундаментом реалізації багатьох з них і останньою захисною межею.

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) в трьох сферах безпеки: інформаційної безпеки, безпеки інформації та кібернетичної безпеки (рис. 1).

Рис. 1. Модель тріади CIA для комплексних АБС

У даній моделі під «інформаційною безпекою» розуміється процес забезпечення конфіденційності, цілісності і доступності інформації клієнтами банку. 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. Прикладом такого комплексу є «АванГард». Ціллю 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.

Сенс запропонованого підходу може бути представлений в вигляді деякої умовної фігури. Дані методи дозволять, визначити і класифікувати загрози і, відповідно до вірогідності наступу негативних наслідків та їх можливої тяжкості для Банку, організувати систему захисту.

4. Міжнародна співпраця з кібербезпеки.

Асоціація ISACA (www.isaca.org) об’єднує більше 115 000 членів у 180 країнах світу, допомагає лідерам у сфері управління та інформаційних технологій забезпечувати корисність і довіру до інформації та інформаційних систем. Із часу заснування асоціації у 1969 році ISACA є надійним джерелом знань, стандартів, співробітництва та підвищення кваліфікації для фахівців у галузі ауди-

ту, підтвердження достовірності, безпеки, управління ризиками, конфіденційності та управління інформаційними системами. ISACA пропонує фахівцям із кібербезпеки широкий набір ресурсів Cybersecurity Nexus™ і настанови COBIT®2, що допомагають організаціям в управлінні та контролі за інформацією та технологіями. Асоціація також розвиває та підтверджує найбільш важливі для бізнесу навички та знання рис. 2), поширюючи сертифікації, що визнаються у міжнародному масштабі: CISA®3, CISM®4, CGEIT®5 і CRISC™6. ISACA має понад 200 відділень по всьому світу.

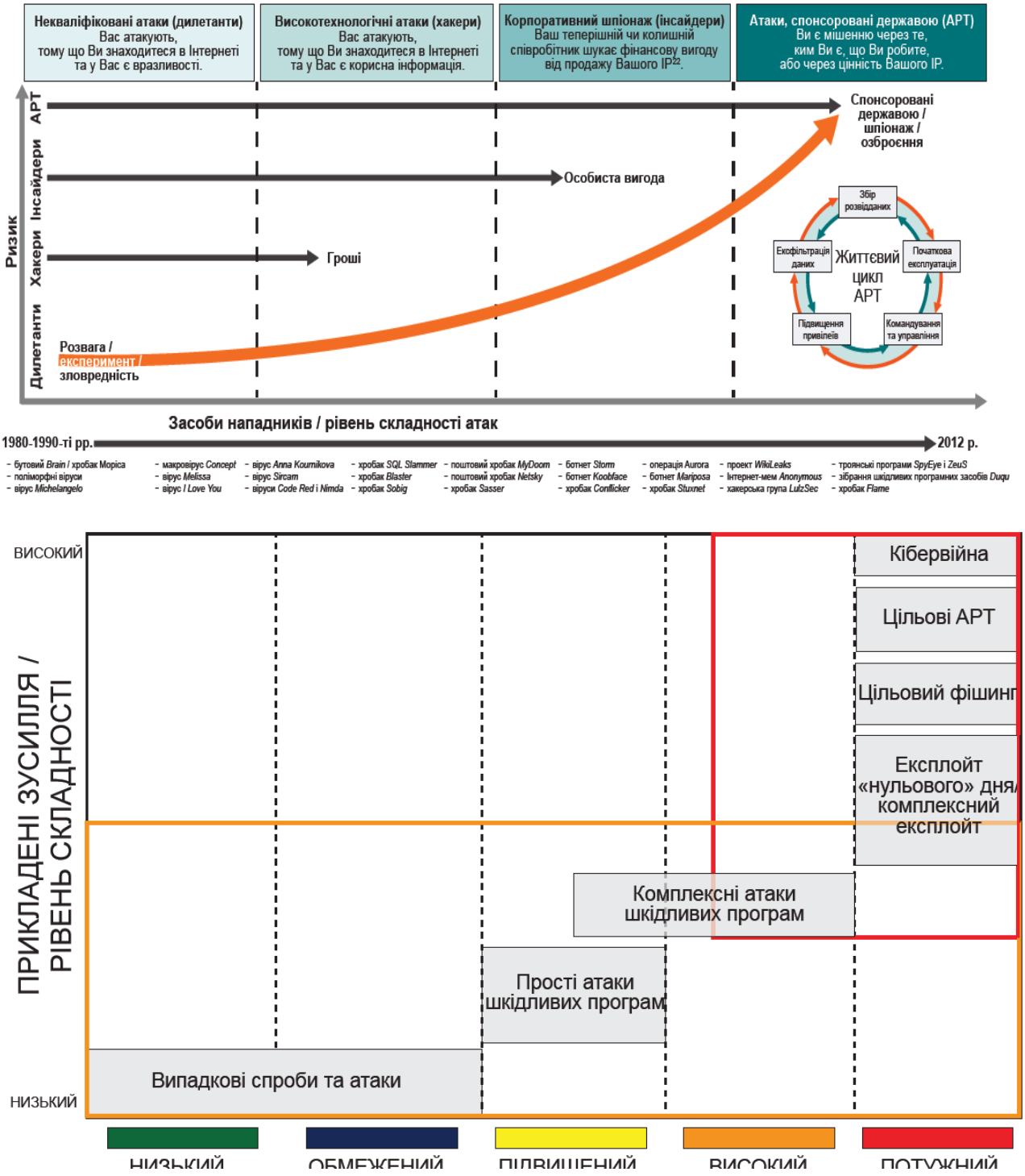

Рис. 2 Засоби нападників і рівень складності атак

Лекція 2 Поняття банківської таємниці

(2год.)

План лекції

1. Правове регулювання захисту банківської таємниці
2. Відповідальність за посягання на банківську таємницю
3. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж

1. Правове регулювання захисту банківської таємниці

У зв'язку із зверненнями правоохоронних органів та банків щодо порядку та обсягів розкриття банками інформації, що становить банківську таємницю, за рішенням суду та використовуючи закріплені у пункті 1 статті 66 Закону України «Про банки і банківську діяльність» повноваження щодо адміністративного регулювання діяльності банків, Національний банк України вважає за необхідне висловити наступні рекомендації стосовно діяльності банків.

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** (за винятком, якщо така інформація складає державну таємницю), 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 (чи його заступника), 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.

Довідки по рахунках (вкладах) у разі смерті їх власників надаються банком особам, зазначеним власником рахунку (вкладу) в заповідальному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, іноземним консульським установам по справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів).

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 (способи) 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 (масова інформація та інформація, що публічно поширюється через друковані та аудіовізуальні канали, закони, нормативні акти, що стосуються свобод і законних інтересів громадян та ін.).

Ураховуючи відкритий доступ до зазначеної інформації, необхідно пояснити таке. 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.

2. Відповідальність за посягання на банківську таємницю

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 (одержання) таких відомостей у будь-який спосіб: вилучення (викрадення), 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.

Незалежно від вирішення питання про притягнення до кримінальної відповідальності і покарання злочинця зазначені санкції не передбачають відшкодування суб'єкту підприємницької діяльності завданих злочином збитків - їх відшкодування може бути здійснене шляхом використання норм цивільного законодавства.

Цивільна відповідальність ґрунтується на цивільно-правових відносинах, за яких одна сторона зобов'язана відшкодовувати другій збитки, завдані протиправними (і не завжди кримінально караними) 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 (чи його заступника), 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.

Довідки по рахунках (вкладах) у разі смерті їх власників надаються банком особам, зазначеним власником рахунку (вкладу) в заповідальному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, іноземним консульським установам по справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів).

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 (способи) 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 (масова інформація та інформація, що публічно поширюється через друковані та аудіовізуальні канали, закони, нормативні акти, що стосуються свобод і законних інтересів громадян та ін.).

Ураховуючи відкритий доступ до зазначеної інформації, необхідно пояснити таке. **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.

3. Злочини у сфері використання електронно-обчислювальних машин (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.

П р і м і т ка. 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 (розрахункові документи, документи на переказ готівкових коштів, а також ті, що використовуються при проведенні міжбанківського переказу та платіжного повідомлення інші).

Лекція 3 Вразливості , ризики, Управління ризиками кібербезпеки банків (3 год.)

Зміст

1. Загрози інформаційній безпеці банківської установи. Вразливості.

2. Управління ризиками кібербезпеки банків

1. Загрози інформаційній безпеці банківської установи. Вразливості.

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

Як свідчить досвід, основними способами реалізації таких загроз є:

- маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації);
- порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправне збирання і використання інформації;
- руйнування та використання з протиправною метою чужих інформаційних ресурсів;
- інформаційний тероризм (поширення комп'ютерних "вірусів", установлення програмних та апаратних пристроїв, призначених для несанкціонованого отримання інформації, упровадження радіоелектронних приладів перехоплення інформації, незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем, нав'язування фальшивої інформації, оприлюднення компрометуючої інформації та ін.).

Джерелами загроз інформаційній безпеці банку можуть бути як зовнішніми, так і внутрішніми. До внутрішніх загроз безпеці банківської установи можна віднести:

- втрату інформації,
- некомпетентність персоналу,
- розголошення конфіденційної інформації,
- незаконне використання банківської інформації,
- знищення інформації,
- викривлення інформації,
- викрадення конференційної інформації,
- витік інформації;
- помилки обслуговуючого персоналу та користувачів;
- втрату чи руйнування інформації, обумовлена неправильним збереженням архівних даних на магнітних носіях;

- випадкове знищення чи зміна даних;
- збої обладнання електроживлення;
- збої кабельної системи;
- перебої в електроживленні.
- До зовнішніх загроз безпеці банківської установи відносять:
- модифікацію змісту даних,
- порушення конфіденційності банківської інформації,
- порушення логічної цілісності банківської інформації,
- порушення прав власності на інформацію,
- порушення фізичної цілісності банківської інформації;
- несанкціонований доступ сторонніх осіб, що не належать до числа працівників, до конфіденційної інформації і мережевих ресурсів;
- розкриття і модифікація інформації і програм;
- копіювання інформації і програм;
- розкриття чи модифікація або підміна трафіку передачі інформації мережею;
- поширення комп'ютерних вірусів;
- введення в програмне забезпечення логічних бомб;
- руйнування архівної інформації або навмисне її знищення;
- фальсифікація повідомлень, переданих каналами зв'язку.

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. Воно може здійснюватися через повідомлення, передавання, пересилання, публікації, втрати чи іншим способом оприлюднення зазначених відомостей.

Викраденням інформації є таємне вилучення носіїв інформації (документів, електронних носіїв, відео- та аудіозаписів) з метою подальшого їх використання іншою особою чи передання їх такій особі.

Знищенням є приведення носіїв інформації (документів, електронних носіїв, аудіо-, відеозаписів та інших носіїв, що мають матеріальний характер) 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 (комп'ютерних програм), 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.

Зазначені загрози мають загальний характер і однаково стосуються всіх видів інформації: документованої, електронної, знань та ін.

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. У результаті відбувається відтік інвестицій та міграція клієнтів та конкурентів.

По друге, інциденти такого роду можуть призвести до втрати конкурентоздатності банку, якщо, наприклад, інтелектуальна власність або база клієнтів попадуть до конкурентів.

Отже, наслідком витоку конфіденційної інформації є втрата клієнтів, погіршення іміджу, зниження конкурентоздатності та прямі фінансові збитки банків. З проблемою витоку інформації можна боротись, але перемогти її повністю неможливо, оскільки ні апаратні, ні технічні засоби не можуть забезпечити необхідного захисту, бо техніка безсила проти витонченого розуму людини.

Загрози можуть бути навмисними, випадковими, природними і можуть бути результатом втрати будь-яких сервісів.

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.

Приклади таких загроз наведено у таблиці 1.

Таблиця 1

Приклади загроз та їх джерела

Джерело загрози	Загроза
Хакери, кракери	Хакерські дії Соціальна інженерія Втручання до системи, злом Неавторизований доступ до системи
Комп’ютерні злочинці	Комп’ютерні злочини Шахрайські дії Продаж інформації Спуфінг Втручання у систему Руйнування інформаційної системи
Тероризм	Кібертероризм Інформаційна війна Атаки на систему (наприклад, розподілена

	відмова в обслуговуванні) Підробка системи Фінансування терористичних організацій
Дії конкурентів	Політична перевага Економічні дії Крадіжка інформації Вручання в особисте життя Соціальна інженерія Проникнення у систему Неавторизований доступ до системи
Персонал	Напад на персонал “Чорна пошта” Перегляд інформації з обмеженим доступом Комп’ютерні зловживання Шахрайство і крадіжка Продаж інформації Фальсифікація та підробка даних Перехоплення Зловмисні коди (віруси, логічні бомби, троянські коні, тощо) Продаж персональної інформації Дефекти системи Втручання у систему Системний саботаж Неавторизований доступ до системи

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.

Таким чином, у банківському секторі загрози інформаційній безпеці пов’язані з потенційною можливістю завдання шкоди ресурсам банківської системи, зокрема, інформації, працівникам банків, клієнтам банків, обладнанню, процесам банківської діяльності, банківським програмно-технічним комплексам, бізнес-процесам/банківським продуктам тощо. Деякі загрози можуть впливати на кілька ресурсів банківської системи. У такому випадку вони можуть чинити різний вплив на різні ресурси.

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 (у тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії тощо).

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.

Конкретними заходами ліквідації загроз безпеці інформаційної інфраструктури банківської установи мають бути:

- створення цілісності засобів захисту, технічного і програмного середовища, що полягає у фізичному збереженні засобів інформатизації, незмінності програмного середовища, виконанні засобами захисту передбачених функцій, ізольованості засобів захисту від користувачів;
- захист інформації від витоку внаслідок наявності фізичних полів за рахунок акустичних та побічних електромагнітних випромінювань і наводок на комунікаційні мережі та конструкції будівель;
- використання криптографічного захисту найбільш цінної інформації при її обробці в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку підприємства;
- надання диференційованого доступу працівникам для здійснення конкретних операцій (створення, читання, запис, модифікація, видалення) за допомогою програмно-технічних засобів, а також розмежування доступу користувачів до даних в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку банківської установи різного рівня та призначення;
- ідентифікація користувачів та здійснюваних ними процесів в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку установи на основі використання паролів, ключів, магнітних карт, цифрового підпису, а також біометричних характеристик особи як при доступі до інформаційно-телекомунікаційних систем;
- реєстрація (з фіксацією дати і часу) дій користувачів з інформаційними та програмними ресурсами в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах, зокрема протиправних спроб доступу;
- попередження передавання інформації з обмеженим доступом по незахищених лініях зв'язку;
- запобігання впровадженню в інформаційно-телекомунікаційні системи програм-вірусів;
- регулярна перевірка технічних засобів і приміщень для виявлення наявності в них пристроїв несанкціонованого доступу до інформації;
- обладнання спеціальних приміщень для захисту мовної інформації при проведенні конфіденційних переговорів тощо.

Суттєвим наслідком реалізації загроз інформаційній безпеці є підрив ділового іміджу банківської установи, виникнення проблем у взаємостосунках з реальними та потенційними клієнтами, конкурентами, контролюючими та правоохоронними органами, спричиненими передусім поширенням недостовірної, заздалегідь неправдивої інформації про банківську установу, здійсненням негативних інформаційних впливів на його керівництво, працівників тощо.

Вразливості, які можуть стати причиною негативної дії загроз інформаційній безпеці банківської установи можуть розглядатися на таких рівнях:

- банківська система в цілому,
- банк,
- процеси та процедури банківської діяльності,
- системи управління;
- банківські інформаційні системи,
- інформаційно-комунікаційні технології підтримки банківської діяльності,
- персонал,
- конфігурація програмно-технічних комплексів,
- залежність від зовнішніх організацій тощо.

При цьому некоректно запроваджені чи недієві заходи безпеки є одним із видів вразливостей, що знижують рівень безпеки банку в цілому і кожного бізнес-процесу/банківського продукту окремо.

Розглянемо окремо вразливість інформації.

Вразливість інформації є одним із головних показників стану її захищеності. Тому визначення ступеня вразливості інформації у процесі організації її захисту має досить суттєве значення. Суть заходів із визначення вразливості інформації показано на рис. 1.

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.

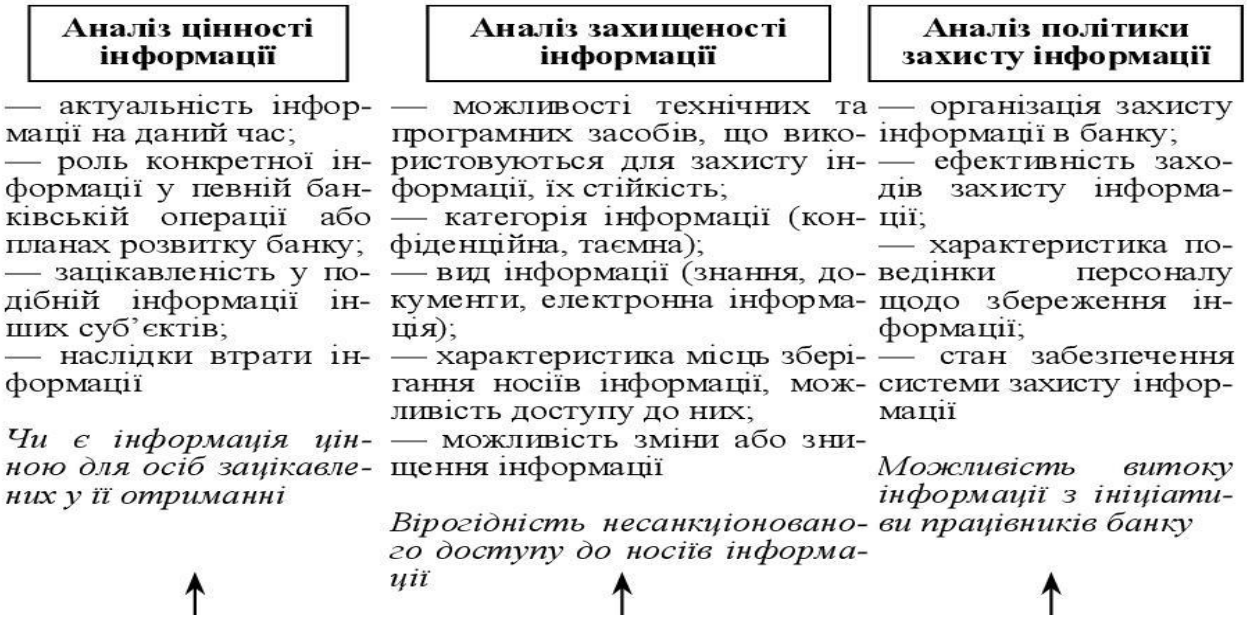

Рис. 1. Визначення вразливості інформації з обмеженим доступом в банку

2. Управління ризиками кібербезпеки банків

Оскільки сучасна діяльність банків 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 (витоком, руйнуванням, знищенням) 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 (можливо, як підсистему управління інформаційною безпекою банку).**

Зазначена система управління 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 (банківська, комерційна таємниці, конфіденційна інформація), та те, що банки є єдиними (крім державних режимних установ) серед суб'єктів підприємницької діяльності, на кого в законодавчому порядку покладено захист чужих таємниць (клієнтів банків), питання аналізу, контролю та мінімізації втрати інформації для банків є доволі важливими. Звідси головним в аналізі ризиків втрати інформації є виявлення способів несанкціонованого доступу до інформації банку та її найбільш уразливих носіїв.

Під час проведення такого аналізу слід виходити з того, що інформація банку зосереджена переважно в двох групах її носіїв: комп'ютерній інформаційній мережі та у працівників банку. Тобто несанкціонований доступ до інформації може бути здійснено, з одного боку, через технічні і програмні засоби, а з іншого – за допомогою засобів інтелектуального та психологічного характеру. Оскільки поведінка людей, зокрема працівників банку, є доволі непередбачуваною, а телекомунікаційні системи банку в умовах значного розвитку штучного інтелекту є уразливими, можна говорити, що ризики втратити банками їх інформацію зосереджені головним чином на таких її носіях, як персонал і телекомунікаційні системи.

Оцінювання ризиків втрати інформації в банку передбачає визначення вартості інформаційних ресурсів, щодо яких існує ризик втрати, та самого ризику як імовірності реалізації певної загрози, у цьому разі пов'язаної з втратою інформації. Вартість інформації оцінюється через її комерційну цінність, яка, у свою чергу, визначається через розміри збитків (шкоди), які можуть настати у зв'язку з її втратою, обсягом (перспективами) вигоди, яку може отримати банк, використовуючи наявну в нього інформацію, а також витрати, пов'язані з виробленням, отриманням і захистом такої інформації. Щодо банківської таємниці, то її цінність може бути визначена через обсяги залучених коштів від клієнтів банку, інформацію про комерційну та фінансову діяльність яких він зберігає.

На оцінювання власне ризику як імовірності реалізації певної загрози щодо відповідної інформації банку впливає кілька показників. Головними серед них є привабливість інформації для суб'єктів загроз, її цінність, актуальність, доступність, рівень захисту. Через ці показники визначається рівень критичності інформації. Скажімо, для інформації про фінансову діяльність клієнтів банку рівень критичності може бути доволі високий, незважаючи на вжиття банком заходів її захисту. Це насамперед пов'язане з тим, що доступ до такої інформації має значна кількість осіб (операціоністи, бухгалтерські працівники, працівники кредитного та інших підрозділів банку, працівники його телекомунікаційних систем, служби безпеки), а в проведенні платежів задіяно дуже багато технічних засобів та інформаційних мереж, за допомогою яких така інформація передається. Ризик доступу до зазначеної інформації буде тим вищим, чим активніше здійснює свої фінансові операції клієнт (проведення платежів, отримання кредитів, операції з цінними паперами, валютою, пластиковими платіжними засобами). Крім того, береться до уваги ділова активність клієнта, його роль і місце на ринку, конкурентна поведінка. У цьому разі інформація про клієнта банку буде доволі привабливою для його конкурентів і вони намагатимуться її отримати.

Питання мінімізації ризику втрати інформації є доволі серйозним для банків, однак чи всі ризики необхідно мінімізувати, і якщо так, то до якого ступеня? З досвіду відомо: хоч як банки чи інші суб'єкти намагалися виключити ризик втрати інформації, зробити це майже неможливо. Крім того, 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 втра-

ти 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.

Водночас для зниження (мінімізації) ризику втрати інформації банки мають вживати відповідних заходів, диференціюючи 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, а також інформації, яка існує у вигляді 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, насамперед працівниками банку, стосовно дотримання ними встановленого режиму захисту інформації, своєчасне реагування на всі збої в захисті інформації, що зберігається та функціонує в інформаційних мережах банку;
- запровадження надійної системи документообігу в банку (службового та спеціального діловодства), яка виключала б можливість несанкціонованого доступу до банківських документів, їх втрати, знищення чи модифікації;
- 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, наприклад, страхувальників, постачальників.

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 (ймовірність і наслідки ризику мають бути зрозумілими);
- 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 може бути виконано з різним ступенем деталізації залежно від критичності ресурсів СУІБ/бізнес-процесів/банківських продуктів, відомих вразливостей і попередніх інцидентів інформаційної безпеки.

Аналіз ризиків передбачає їх визначення та оцінювання. Під час визначення ризиків установлюють, які саме інформаційні ризики можуть існувати чи існують в діяльності суб'єкта господарювання (у нашому випадку 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.

Стандарти Національного банку України, які базуються на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням до них вимог із захисту інформації, обумовлені конкретними вимогами сфери банківської діяльності і вимогами чинного законодавства України. Ключовим моментом цих документів є те, що вони розглядають принципи управління інформаційною безпекою банку, найбільш важливим з яких є **оцінювання ризиків інформаційної безпеки банків**.

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. У цьому випадку значення ризику обчислюється окремо для кожної загрози, і у загальному випадку представляється як добуток ймовірності реалізації загрози на величину потенційного збитку від цієї загрози. Значення збитку визначається власником банківської інформації, а ймовірність реалізації загрози обчислюється групою експертів, які проводять аудит системи управління інформаційною безпекою.

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

Таким чином, методологія оцінювання ризиків може бути кількісною або якісною, або також їх комбінацією. На практиці **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.

Якісна методика оцінювання ризиків використовує шкалу атрибутів для опису величини потенціальних наслідків реалізації загроз і вірогідність того,

що такі наслідки виникнуть. Перевагою якісної методики є її простота розуміння всім персоналом; недоліком такої методики є залежність від суб'єктивного вибору шкали атрибутів.

Для отримання якісної оцінки ризиків необхідно розглянути оцінки наслідків реалізації загроз разом із вразливостями, з використанням яких ці загрози можуть реалізуватися, та оцінки ймовірності їх реалізації для кожного бізнес-процесу/банківського продукту, мережі, обладнання, програмного забезпечення, які забезпечують функціонування цього бізнес-процесу/банківського продукту, мережі банку в цілому, фізичного середовища, персоналу тощо, з урахуванням попереднього аналізу.

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.

Порівняння СУІБ та процесу управління ризиками інформаційної безпеки банку можна подати у вигляді таблиці:

Фаза СУІБ	**Процес управління ризиками інформаційної безпеки**
Плануй	Аналіз ресурсів СУІБ. Оцінювання ризиків. План оброблення ризиків. Прийняття залишкових ризиків
Виконуй	Впровадження плану оброблення ризиків
Перевіряй	Постійний моніторинг та перегляд ризиків
Дій	Підтримка та покращення процесу управління ризиками інформаційної безпеки

Процес управління ризиками інформаційної безпеки 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.

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

Лекція 4 Політика безпеки банківських установ

(2 год)

План лекції

1. Політика інформаційної безпеки банківських установ
2. Перегляд політики інформаційної безпеки банків
3. Реалізація політики інформаційної безпеки банківської установи
4. Приклад Політики інформаційної безпеки

1.Політика інформаційної безпеки банківських установ

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 [2, с. 567-568]:

- «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, навпаки, детальним аналізом усієї наявної схеми зберігання та обробки інформації. Першим етапом цього методу є, як і завжди, 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 (незмінності). 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, аутентифікація, 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 (стан інформаційної безпеки банку).

Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене постановою правління Національного банку України від 28 вересня 2017 року № 95 зобов'язує банки:

•розробити та впровадити політику інформаційної безпеки, яка має містити:

1) цілі інформаційної безпеки;

2) сферу застосування політики інформаційної безпеки;

3) принципи, правила та вимоги інформаційної безпеки в банку;

4) визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки;

•забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік;

•затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін;

•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.

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.

Політика інформаційної безпеки банківської установи визначає стратегію і тактику побудови системи захисту інформації.

Питанню впровадження політики безпеки в банківських установах приділяють увагу дослідники у сфері ІБ, усі вони дають своє визначення політики інформаційної безпеки взагалі і банків зокрема. Розглянемо деякі з них.

Домарєв В. В. у статті "Обґрунтування основних функцій системи управління інформаційною безпекою" зазначає, що **під політикою інформаційної безпеки** слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Бондаренко М. Ф. у статті " Визначення та обґрунтування суті політики інформаційної безпеки" дає таке визначення: "політика **інформаційної безпеки банку** є сукупністю 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".

Бодюл Є. М. під поняттям "**політика інформаційної безпеки банківської установи**" розуміє науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення задач інформаційного захисту банківської установи від протиправних дій.

Узагальнюючі ці визначення, під поняттям "**політика інформаційної безпеки банківської установи**" будемо розуміти сукупність правил, обмежень і рекомендацій, прийнятих керівництвом банку, які спрямовані на захист інформації від внутрішніх та зовнішніх загроз.

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.

Головною метою діяльності у сфері інформаційної безпеки є забезпечення властивостей кожного активу:

- доступності (можливість користування деякими ресурсами інформаційної системи й інформацією в будь-який момент);
- конфіденційності (недоступність інформації чи сервісів для користувачів, яким апріорно не надано можливість використання зазначених сервісів або інформації);
- цілісності (незалежність властивостей інформації і ресурсів у будь-який момент часу від моменту їх появи чи введення в систему);

Серед **основних об'єктів політики інформаційної безпеки банківських установ** доцільно виокремити такі:

- фінансові ресурси – національна та іноземна валюта, банківські операції та угоди банку, коштовності, фінансові документи;
- персонал банку – керівництво і вищий менеджмент банку, особи, які мають доступ до конфіденційної інформації, банківської та комерційної таємниці, інші працівники банку;
- матеріальні засоби – апаратні засоби інформаційних технологій, носії даних, будівлі, приміщення, меблі, транспорт тощо;
- сервісні ресурси та підтримуюча інфраструктура – обслуговуючі засоби обчислювальної техніки, енергопостачання, забезпечення необхідних умов експлуатації і тощо;
- програмне забезпечення – прикладне, системне чи сервісне програмне забезпечення тощо, яке використовується співробітниками банківської установи для роботи з системами і клієнтами;

- інформаційні ресурси – будь-яка інформація банку, що обробляється та зберігається в інформаційній системі банківської установи (бази даних, файли, електронні документи).
- Оцінювання ймовірності появи ймовірних загроз і очікування розмірів втрат – складний і тривалий процес, але коректно визначити вимоги до системи захисту банківської установи є ще складнішим, тому **політика інформаційної безпеки банку має визначатися такими заходами:**
- ідентифікація користувачів;
- перевірка дійсності та контроль доступу користувачів до об'єкту, що захищається, у приміщення, до ресурсів інформаційної системи;
- розподіл повноважень користувачів, що мають доступ до обчислювальних ресурсів;
- реєстрація та облік роботи користувачів;
- реєстрація спроб порушення повноважень;
- шифрування або кодування конфіденційної інформації на основі криптографічних алгоритмів високої стійкості;
- застосування цифрового підпису для передавання інформації каналами зв'язку;
- забезпечення антивірусного захисту та відновлення інформації, зруйнованої вірусними впливами;
- контроль цілісності програмних засобів та інформації, що обробляється;
- відновлення зруйнованої архівної інформації, навіть при значних втратах;
- наявність адміністратора захисту інформації в системі;
- розроблення та виконання необхідних організаційних заходів;
- застосування технічних засобів, що забезпечують безперебійну роботу обладнання.
- дотримання 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 (у тому числі віддаленого) до інформації, її контролю та захисту;
- проведення політики ідентифікації та автентифікації ресурсів;
- політика криптографічного захисту інформації;
- 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.

Основою для формування політики інформаційної безпеки банківської установи можна визначити:

- характеристику об'єкта застосування;
- аналіз поточного стану захисту інформаційної інфраструктури банку;
- облік можливих негативних факторів впливу та ймовірність їх реалізації;
- створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки.

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.

Політика інформаційної безпеки повинна містити положення стосовно:

- визначення інформаційної безпеки, її загальних цілей і сфери застосування, а також важливості безпеки як механізму можливості розповсюдження інформації;
- положення щодо намірів і підтримки керівництвом мети та принципів інформаційної безпеки згідно з бізнес-стратегією та цілями;
- основ встановлення цілей заходів безпеки і заходів безпеки, включаючи структуру оцінки ризику та управління ризиком;
- короткого пояснення особливо важливих для організації політики безпеки, принципів, стандартів безпеки і вимог щодо відповідності, включаючи:

1) відповідність законодавчим, нормативним та контрактним вимогами;

2) вимоги до освіти, навчання та поінформованості персоналу щодо безпеки;

3) управління безперервністю бізнесу;

4) наслідки порушення політики інформаційної безпеки;

- визначення загальних та спеціальних обов'язків з управління інформаційною безпекою, включаючи звітування щодо інцидентів інформаційної безпеки;
- посилань на документацію, яка може підтримувати політику, наприклад, більш детальні політики та процедури для певних інформаційних систем або правила безпеки, які користувачі повинні виконувати.

Розглянемо ієрархічний підхід до **впровадження інформаційної політики банківської установи** (рис. 1).

Політика інформаційної безпеки банківських установ повинна розроблятися відповідно до вимог чинних законодавства, нормативно-правових актів,

міжнародних стандартів у сфері інформаційної безпеки та внутрішніх нормативних документів банку.

Керівництво банку повинно розуміти, що інформаційна безпека є основою для нормального функціонування банку, та всебічно сприяти виконанню політики інформаційної безпеки.

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 (рис. 2), 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.

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.

Рис. 1 Ієрархічний підхід до впровадження інформаційної політики банківської установи

Рис. 2 Основні правила забезпечення політики безпеки в інформаційній системі

2. Перегляд політики інформаційної безпеки банків

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 банку має доповнюватися і змінюватися згідно з критеріями змін і цінності інформації, що підлягає захисту, у зв'язку із впровадженням нових інформаційних технологій та змін у нормативно-правових актах України, також у внутрішніх нормативних документах та іншими чинниками.

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.

3. 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 (для можливості адекватного реагування обслуговуючого персоналу на виникнення збоїв у системі);
- 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.

4. Приклад Політики інформаційної безпеки

Назва банку

ЗАТВЕРДЖЕНО
Рішення Правління банку
"___" _____ 201_ р.

Політика інформаційної безпеки

Вступ

Політика інформаційної безпеки описує та регламентує функціонування системи управління інформаційною безпекою (СУІБ) 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, відповідає вимогам законодавства України та нормативно-правовим актам Національного банку України, а також вимогам міжнародних та внутрідержавних платіжних систем та систем переказу коштів.

Ціль політики

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати захист інформації та ресурсів банку від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників банку, забезпечувати безперервну роботу банку, сприяти мінімізації ризиків операційної діяльності банку та створювати позитивну репутацію банку при роботі з клієнтами.

Сфера застосування

Політика поширюється на банк у цілому і повинна використовуватися для всіх критичних бізнес-процесів/банківських продуктів банку.

Предмет політики

Основними принципами Політики інформаційної безпеки є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності, доступності. Це, в першу чергу, стосується інформації з обмеженим доступом, яка відноситься до “банківської таємниці”, “комерційної таємниці” та іншої конфіденційної інформації.

Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтовного підходу описані в політики управління інформаційною безпекою.

Весь персонал банку обізнаний та виконує вимоги інформаційної безпеки в роботі. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

Публічні сервіси банку та внутрішні мережі банку відповідають вимогам стандартів з інформаційної безпеки.

Банк забезпечує виконання усіх вимог з інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.

Ролі та відповідальності

Керівництво банку чітко розуміє, що інформаційна безпека банку є основою життєдіяльності банку. У банку створений та постійно працює керівний орган з питань інформаційної безпеки, рішення якого є обов'язковими для виконання усім персоналом банку.

Документи Політики інформаційної безпеки розробляються підрозділом інформаційної безпеки та іншими підрозділами за відповідними напрямками діяльності. Постійний контроль впровадження, виконання, вдосконалення та підтримання Політики в актуальному стані покладений на підрозділ інформаційної безпеки.

Керівництво банку сприяє створенню, впровадженню, контролю та підтримці Політики інформаційної безпеки.

Стратегія розвитку інформаційних технологій банку, всі проекти, які пов'язані з інформаційними технологіями, узгоджуються з Політикою інформаційної безпеки.

Кожен працівник банку забезпечує підтримку відповідного рівня інформаційної безпеки банку. В межах своїх службових обов’язків та повноважень працівники повинні виконувати та відповідати за виконання вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм і несуть відповідальність за їх порушення згідно із законодавством України та внутрішньобанківськими нормативними документами.

Документи Політики доступні працівникам банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво банку створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

У банку складаються, діють, тестуються та оновляються плани забезпечення безперебійного функціонування на випадок непередбачених критичних ситуацій.

Лекція 5 Системи управління кібербезпекою в банківських установах

(2 год.)

Зміст

1. Особливості управління інформаційною безпекою в банківських установах
2. Система управління інформаційною безпекою банківської установи
3. Підготовка до впровадження СУІБ в банківських установах

1. Особливості управління інформаційною безпекою в банківських установах

У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки держави у банківському секторі.

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, аутентифікації тощо.

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

2. Система управління інформаційною безпекою банківської установи

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.

Передумовами впровадження СУІБ у банку є:

1) упровадження процесного підходу до діяльності банку;

2) упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку.

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.

У розділі ІІ викладено **вимоги щодо впровадження СУІБ у банку**:

- сформувати колективний керівний орган з питань впровадження та функціонування СУІБ (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;
- 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;
- покласти на керівний орган СУІБ обов'язок виконання таких завдань:

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

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

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

4) визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;

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

6) забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій;

- розробити та впровадити політику інформаційної безпеки, яка має містити:

1) цілі інформаційної безпеки;

2) сферу застосування політики інформаційної безпеки;

3) принципи, правила та вимоги інформаційної безпеки в банку;

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

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.

3. Підготовка до 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.

Формування такого керівного органу тільки з фахівців з питань інформаційної безпеки є недоцільним, оскільки в такому випадку питання інформаційної безпеки будуть за межами уваги керівників, відповідальних за критичні бізнес-процеси, або питання інформаційної безпеки будуть вирішуватися окремо для кожного бізнес-процесу, що створить додаткові умови для несанкціонованого доступу до інформації та порушення конфіденційності, а також призведуть до додаткових фінансових витрат. У разі необхідності до роботи з окремих питань в цьому керівному органі можуть долучатися зовнішні спеціалісти з питань інформаційної безпеки за умови підписання угоди про конфіденційність.

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 бізнес-процесів, 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 ІТ 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:

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

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

в) 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.

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.

Не існує стандартного набору бізнес-процесів/банківських продуктів для будь-якого банку. Тому банк має самостійно визначити відповідні бізнес-процеси/банківські продукти, які використовуються всередині банку.

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 (у тому числі додаткової вхідної інформації з інших бізнес-процесів);
- вимоги щодо забезпечення безперервності бізнес-процесу/ банківського продукту (максимально допустимий час простою);
- 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 (зокрема, файловий обмін або режим реального часу, в тому числі й для обміну інформацією з іншими програмно-технічними комплексами в разі наявності);
- 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 (за наявності окремих принципів для цього програмно-технічного комплексу).

Зазначимо деякі аспекти формування цієї інформації.

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.

Перелік процедур бізнес-процесу та блок-схема послідовності їх виконання з визначенням взаємозв’язків (у тому числі додаткової вхідної інформації з інших бізнес-процесів) буде дуже корисним під час аналізу та визначення вразливостей, притаманних цьому бізнес-процесу/банківському продукту. Цей перелік та блок-схема мають бути у достатньому ступені узагальненими. Дуже детальний перелік може призвести до ускладнення під час визначення вразливостей. Однак, якщо цей перелік та блок-схема будуть занадто узагальненими, то це може призвести до пропуску небезпечних вразливостей, які можуть створювати великі ризики.

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 (але не підрозділ, який відповідає за інформаційні технології) 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 (обласних дирекціях, філіях тощо) 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.

Концепцію захисту банку наведено на рис. 1

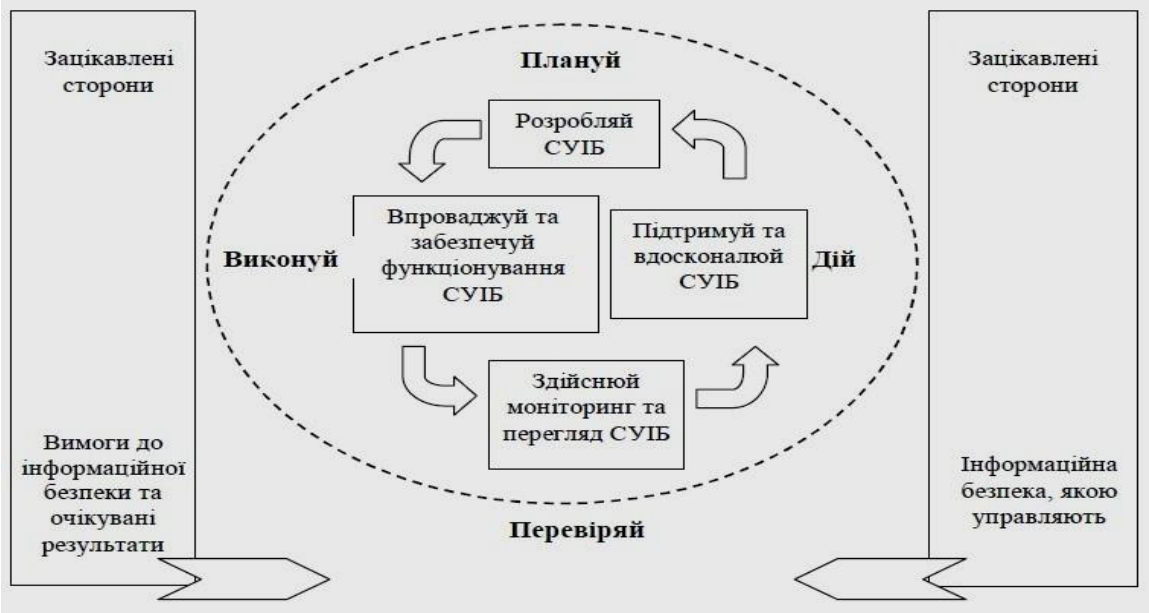

Рис. 1. Концепція захисту банківської установи

Опис взаємодії елементів захисту банківської установи навдено у табл. 1.

Таблиця 1

Взаємодія елементів захисту банківської установи

Плануй (розробляй СУІБ)	Розробити політику СУІБ, цілі, процеси та процедури, суттєві для управління ризиком та вдосконалення інформаційної безпеки для отримання результатів, які відповідають загальним політикам та цілям організації.
Виконуй (впроваджуй, забезпечуй функціонування СУІБ)	Впровадити та забезпечити функціонування політики інформаційної безпеки, заходів безпеки, процесів та процедур СУІБ.
Перевіряй (здійснюй моніторинг та перегляд СУІБ)	Оцінювати і, за можливості, вимірювати продуктивність процесів згідно з політикою, цілями СУІБ і практичним досвідом та звітувати про результати керівництву для перегляду.
Дій (підтримуй та вдосконалюй СУІБ)	Вживати коригувальні та запобіжні дії на підставі результатів внутрішнього аудиту і перегляду СУІБ з боку керівництва або іншої важливої інформації для досягнення постійного вдосконалення СУІБ.

Лекція 6 Кібербезпека в автоматизованих системах банківських установ (2 год.)

План лекції

1. Захист інформації в інформаційних системах банківських установ

2. Криптографічний захист інформації в автоматизованих банківських системах

1. Захист інформації в інформаційних системах банківських установ

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, банківські (комерційні) операції та операції банку, коштовності, фінансові документи);
- персонал банку (керівництво і вищий менеджмент банку, особи, які мають доступ до його таємниць, інші працівники банку);
- матеріальні засоби (будівлі, сховища, обладнання, транспорт, засоби і системи інформатизації);
- інформаційні ресурси банку з обмеженим доступом (відомості, що є банківською і комерційною таємницею банку і його конфіденційною інформацією).

Важливе значення у захисті інформації має політика безпеки банку. Ми вже знаємо, що політика безпеки – це прийнята в банку сукупність норм, правил, рекомендацій згідно з якими будується система його безпеки та управління нею. Вона реалізується за допомогою організаційних заходів і програмно-технічних засобів, які визначають архітектуру системи захисту та за допомогою засобів управління механізмами захисту. Для кожного конкретного банку політика безпеки є індивідуальною і залежить від особливостей технологій банківського виробництва, змісту інформаційної діяльності та умов роботи 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.

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

- визначення вразливості інформації банку (виявлення в інформаційній системі банку місць, використання яких зловмисниками може завдати шкоди інформаційним ресурсам і в цілому 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 (матеріальне, фінансове, наукове та ін.);
- 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.

Банки, як правило, не передбачають захисту відкритої інформації. Але ж відкритість інформації не позбавляє її цінності, а цінна інформація, безумовно, має захищатися, насамперед від втрати її. 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.

Водночас 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. Тобто це можуть бути відповідні документи, матеріали (у тому числі магнітні, магнітооптичні, оптичні та інші засоби), вироби (засоби відображення, оброблення, відновлення, передання інформації), мережі зв'язку та передання даних, а також працівники банку. Захист цих об'єктів має здійснюватися регулюванням доступу до них, установленням відповідного порядку їх використання (діяльності) та формуванням умов зберігання. Якраз ці заходи і складають структуру системи захисту інформації.

Зазначені заходи в системі захисту інформації проводяться за допомогою технічних, програмних і правових засобів (ми їх розглянули вище). До технічних засобів регулювання доступу можна віднести кодовані замки на вході в приміщення, міститься відповідна інформація, установлення засобів і систем пропуску на територію банку, спеціальні прилади та пристрої, що регулюють доступ до інформації, яка зберігається в комп'ютерах. За допомогою програмних засобів розмежовується доступ до інформації в інформаційних комп'ютерних системах і мережах банку. Правові засоби є загальними, вони встановлюють як порядок роботи з інформаційними ресурсами банку, так і

умови та правила використання технічних і програмних засобів захисту інформації.

На сьогодні вітчизняними банками напрацьовано певний досвід формування нормативно-правової бази з питань захисту інформації.

Насамперед відповідні положення про захист комерційної таємниці включаються до Статуту банку. Зокрема, у них вказується право банку на:

- комерційну таємницю;
- самостійне визначення складу й обсягу відомостей, що становлять комерційну таємницю і конфіденційну інформацію банку;
- захист комерційної таємниці.

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 (доцільний є використання програм-сирен);

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.

1.1. Кіберзахист в автоматизованих банківських системах.

Згідно із Законом України "Про основні засади забезпечення кібербезпеки України" Національний банк України повинен визначити порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки для суб'єктів переказу коштів, а також здійснювати контроль за їх виконанням.

Національний банк України має намір уперше врегулювати питання щодо забезпечення належного рівня кіберзахисту та інформаційної безпеки у сфері переказу коштів.

Вже розроблено відповідний проект постанови Правління Національного банку України "Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків".

Зокрема Проектом постанови передбачено визначити:

- вимоги до суб'єктів платіжного ринку щодо побудови системи захисту інформації та кібербезпеки;
- порядок дій при виявленні кібератак, що знижують надійність функціонування платіжних систем та систем розрахунків;
- вимоги до організаційних та технічних заходів з метою забезпечення захисту інформації та кібербезпеки суб'єктами платіжного ринку тощо.

В основу цього документу покладено вимоги і рекомендації національних та міжнародних стандартів з питань інформаційної безпеки, а також загальноприйняті у міжнародній практиці сучасні підходи до забезпечення інформаційної безпеки та кіберзахисту.

Прийняття проекту постанови дасть можливість:

- мінімізувати кількість інцидентів інформаційної безпеки та кіберінциндентів у сфері переказу коштів;
- урегулювати питання використання засобів захисту інформації;
- підвищити надійність функціонування та ефективність платіжних систем і систем розрахунків;
- пришвидшити процес модернізації існуючих платіжних систем з урахуванням сучасних технологій захисту інформації.

2. Криптографічний захист інформації в автоматизованих банківських системах

Більш детально розглянемо криптографічний захист інформації, яка зберігається та обробляється.

Криптографічний захист інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових)

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 інформації – спосіб маскування конфіденційної інформації; процес перетворення доступних даних на зашифровані (з обмеженим доступом). Процес маскування інформації здійснюється за допомогою спеціального шифру – набору цифр та символів за визначеним алгоритмом, розшифрування якого можливе лише після підбору до нього ключа. 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 (вбудований у систему або додатковий механізм, що може бути відключений);
- за способом реалізації (апаратний, програмний, програмно-апаратний);
- за криптографічними алгоритмами, які використовуються (загальні, спеціальні);
- за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачів);
- за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих 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 – найбільш надійний спосіб, але й найдорожчий. 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”.

Програмна реалізація криптографічного захисту є значно дешевшою та гнучкішою в реалізації. Але виникають питання щодо захисту криптографіч-

них ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від "вірусних" атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм "збирання сміття".

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.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

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

Криптографічні алгоритми застосовують із метою:

- шифрування інформації;
- захисту даних і повідомлень (інформації) від модифікації або підробки.

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 великі 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.

Сьогодні існує достатня кількість криптографічних алгоритмів. Коротко розглянемо деякі з них.

Найбільш поширеними з них є стандарт шифрування даних **DES (Data Encryption Standart) та алгоритм RSA,** названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Ще одним алгоритмом, що широко застосовується, зокрема, в банківській системі, є алгоритм Діффі-Геллмана.

Алгоритм Діффі-Геллмана (Diffie–Hellman key exchange (D–H)) – це метод обміну криптографічними ключами. Один з перших практичних прикладів обміну ключами, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку. Цей ключ можна використати для шифрування наступних сеансів зв'язку, що використовують шифр з симетричним ключем.

Схему вперше оприлюднили Вітфілд Діффі і Мартін Геллман у 1976 році.

Хоча протокол Діффі-Геллмана є анонімним (без автентифікації) протоколом встановлення ключа, він забезпечує базу для різноманітних протоколів з автентифікацією, і використовується для забезпечення цілковитої прямої секретності в недовговічних режимах Transport Layer Security (відомих як EDH або DHE залежно від комплектації шифру).

Алгоритм DSA (Digital Signature Algorithm) – криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису, але не для шифрування (на відміну від RSA і схеми Ель-Гамаля). Підпис створюється таємно, але може бути публічно перевірений. Це означає, що тільки один суб'єкт може створити підпис повідомлення, але будь-хто може перевірити її коректність.

Алгоритм Advanced Encryption Standard (AES) – симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий як американський стандарт шифрування урядом США.

Усі криптографічні алгоритми можна використовувати з різною метою, зокрема:

- для шифрування інформації, тобто приховування змісту повідомлень і даних;
- для забезпечення захисту даних і повідомлень від модифікації.
- Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується.

- Алгоритм RSA дає змогу виконувати шифрування в різних режимах:
- за допомогою секретного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;
- за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;
- за допомогою секретного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Але не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Іншою 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** (сукупність даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, яка його підписала.). Формуючи електронний цифровий підпис, виконують такі операції:

- за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;
- отримане значення хеш-функції шифрується:

а) таємним або відкритим;

б) таємним і відкритим ключами відправника і отримувача повідомлення – для алгоритму RSA;

- використовуючи значення хеш-функції і секретного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису.

Для того, щоб перевірити цифровий підпис, потрібно:

- виходячи із значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;
- обчислити хеш-функцію з тексту повідомлення;
- порівняти ці значення. Якщо вони збігаються, то повідомлення не було модифікованим і відправлене саме цим відправником.

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 між учасниками системи.

1. **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 (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). 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.

2. **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.

Загалом, для забезпечення належного рівня захищеності інформації потрібна **криптографічна система** – сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (зокрема й такої, що визначає заходи безпеки).

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 такі **принципи криптографічного захисту інформаційних систем Національного банку України**:

1) 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;

2) 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;

3) 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, SHA-512, “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.

2.1. Криптографічний захист інформації та заходи захисту інформаційної безпеки в платіжних системах банку

Використання криптографічного захисту інформації під час розроблення політики платіжної системи як складової політики інформаційної безпеки значно посилює безпеку роботи системи.

За принципами використання криптографічний захист може бути вбудованим у платіжну систему або бути додатковим механізмом, який може відключатися. Використовуються дві групи криптографічних алгоритмів:

1) загальні:
- симетричні;
- асиметричні;

2) спеціальні.

Особливу увагу потрібно приділити методам розподілу криптографічних ключів між учасниками платіжної системи, а саме методом:
- базово-сеансових ключів;
- відкритих ключів.

Апаратно-програмні засоби криптографічного захисту інформації в системі банківських платежів забезпечують автентифікацію відправника та отримувача електронних банківських документів і службових повідомлень системи банківських платежів, гарантують їх достовірність та цілісність, неможливість підроблення або викривлення документів у шифрованому вигляді та за наявності електронного цифрового підпису.

Криптографічний захист інформації охоплює всі етапи оброблення електронних банківських документів з часу їх створення до зберігання в архівах банку. Використання різних криптографічних алгоритмів на різних етапах оброблення електронних банківських документів дає змогу забезпечити безперервний захист інформації в системі банківських платежів. Криптографічний захист інформації гарантує цілісність та конфіденційність електронної банківської інформації, а також сувору автентифікацію учасників системи банківських платежів і їх фахівців, які здійснюють підготовку та оброблення електронних банківських документів.

Для здійснення суворої автентифікації банків (філій), які є учасниками системи банківських платежів, застосовують систему ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту. Учасник системи електронних платежів (СЕП) для забезпечення захисту інформації має трибайтові ідентифікатор, перший знак якого є літерою відповідної території, на якій він розташований; другий та третій знаки є унікальними ідентифікаторами учасника СЕП у межах цієї території. Ідентифікатори мають бути узгодженими з адресами СЕП і бути унікальними у межах банківської системи України.

Трибайтові ідентифікатори є складовою частиною ідентифікаторів ключів криптографічного захисту для робочих місць системи автоматизації банку, де формуються та обробляються електронні банківські документи. Ідентифікатор ключів криптографічного захисту для робочих місць складається з шести символів, з яких три перші є ідентифікаторами учасника системи електронних платежів, четвертий – визначає тип робочого місця (операціоніст, бухгалтер тощо), п’ятий і шостий – ідентифікатор конкретного робочого місця (тобто службовця, який відповідає за оброблення електронних банківських документів на цьому робочому місці). Трибайтовий ідентифікатор учасника СЕП убудований у програму генерації ключів і не може бути змінено учасником СЕП, що забезпечує захист від підроблення ключів від імені інших учасників СЕП. Ідентифікатори ключів записуються в апаратуру криптографічного захисту інформації (АКЗІ), яка надається учасникам СЕП і забезпечує апаратне формування (перевірку) електронного цифрового підпису та апаратне шифрування (розшифрування) на АРМ-НБУ.

Фізичний захист систем електронних платежів потребує виконання вимог щодо безпечного та надійного функціонування ключових обчислювальних машин платіжної системи.

Особливої охорони і захисту потребують центри генерації та сертифікації ключів платіжної системи. Вони повинні бути обладнані відповідною обчислювальною технікою, яка пройшла дослідження на побічні електромагнітні ви-

промінювання для захисту від перехоплення і витоку ключової інформації технічними каналами. Обчислювальна техніка для генерації і сертифікації ключів не повинна входити до локальних мереж центрального банку або повинна бути обладнана відповідною системою захисту від втручання з інших робочих місць локальної мережі. Доступ до приміщень центру генерації і сертифікації ключів повинен бути суворо обмеженим.

Лекція 7 Основні положення кібербезпеки в мережі передачі даних SWIFT (4 год)

План лекції

1. Основні поняття про мережу передачі даних SWIFT.
2. Програма забезпечення безпеки клієнтів в платіжній системі SWIFT.
3. Система S.W.I.F.T. та інформаційна безпека

1. Основні поняття про мережу передачі даних SWIFT.

Створена товариством SWIFT мережа передачі даних одна з найвідоміших мереж, створена з ініціативи фінансових організацій. Мережа 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.

У 1968 р. була почата робота над проектом створення міжбанківської системи SWIFT (Society for World-Wide Interbank Financial Telecommunication).

Метою її створення було забезпечення всіх банків, що беруть участь у проекті, (і інших фінансових організацій) захищеної від несанкціонованого доступу, надійною, високошвидкісною і цілодобово працюючою системою для передачі банківської інформації.

На початку 70-х рр. система почала функціонувати. Зараз швидкими темпами відбувається впровадження нової модернізованої системи SWIFT-2.

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.1).

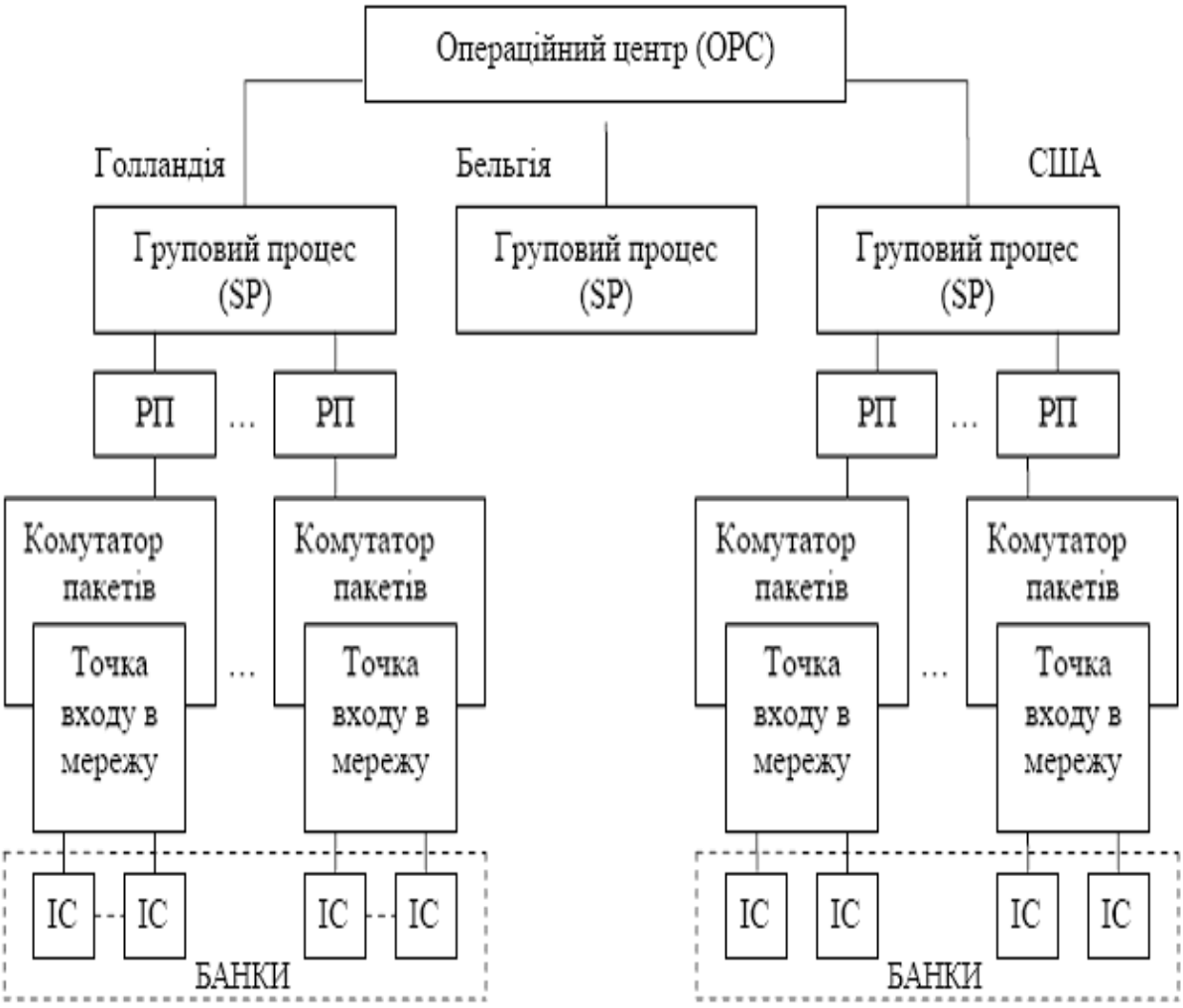

Рис. 1. Архітектура SWIFT

На верхньому (першому) рівні вона містить два Операційні Центри (ОЦ), один з яких розташований в США, а інший в Голландії. Другий рівень утворюють Регіональні Процесор (РП), які розміщені у більшості країн, банки яких

приєднані до системи. Україна підключена до Австрійського РП. ОЦ становлять ядро мережі, вони з'єднані каналами зв'язку між собою і відповідними Регіональними Процесорами. Користувачі з'єднуються з РП виділених каналах зв'язку. Кожен РП відіграє роль концентратора повідомлень, через який дані передають в ОЦ.

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 (табл. 1), які мають різну продуктивність і можуть бути реалізовані на основі різних комп'ютерних платформ. Основні характеристики стандартних інтерфейсів приведені в табл. 1.

Таблиця 1.

Стандартні інтерфейси SWIFT

Типи інтерфейсу	**Комп'ютерна платформа**	**Призначення й особливості**
ST200		Стандартний інтерфейс. Термінали розраховані на невеликий трафік (число повідомлень – до 10 у день). Обробка повідомлень виконується «вручну» (переносом текстових файлів у БС)
ST400	IBM RS/600 і AS400, DEC VAX і micro VAX HP U, Sun Sparkstation	Інтегрований інтерфейс підвищеної продуктивності. Орієнтований на автоматизовану обробку повідомлень. БС повинна мати ПО взаємодіє із системою SWIFT
ST500		Інтерфейс реального часу. Реалізується автоматизована, цілодобова обробка повідомлень SWIFT паралельно з роботою БС

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

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 інте-

гральної 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.

Таблиця 2.

Модифікації пакета TurboSWIFT

Назва	Продуктивність, повідом./день	Особливості застосування
TurboSWIFT 100	100	Підтримка ОС UNIX (модель «клієнт-сервер») і графічний стандарт інтерфейсу користувача X-Windows
TurboSWIFT T250	250	Обробка повідомлень і генерація звітів на основі SQL-СУБД
TurboSWIFT 750	750	Зв'язок із БС на основі мережних протоколів TCP/IP, SNA, ВЗС і ін.
TurboSWIFT 3000	3000	Максимальна продуктивність у режимі OLTP досягає 10 000 повідомлень у годину
TurboSWIFT 3000+	>3000	Використовується надійна багаторівнева система захисту

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. Генеральна Інспекція підпорядкована безпосередньо лише Раді Директорів, яка керує діяльністю SWIFT.

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 неса-

нкціонованого 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 слайсн 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 аутентифікації, 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 пере-

даних 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.

Економічна доцільність використання SWIFT у системі міжбанківських відносин полягає в наданні швидкого і зручного обміну інформацією між: фінансовими інститутами, розташованими будь-де на Землі, ефективне використання коштів за рахунок прискорення проведення і одержання підтверджень, збільшення продуктивності системи, підвищення рівня банківської автоматизації, зменшення ймовірності помило.

2. Програма забезпечення безпеки клієнтів в платіжній системі SWIFT?

Програма забезпечення безпеки членів (ПБЧ) в платіжній системі SWIFT охоплює три основні області, це захист і забезпечення безпеки інформаційної інфраструктури, запобігання і виявлення зловмисних дій в платіжних операціях, а також захист від потенційних загроз інформаційній безпеці Не дивлячись на те, що члени спільноти SWIFT (користувачі) як і раніше несуть основну відповідальність за захист своєї інформаційної інфраструктури, мета SWIFT - підтримати своїх користувачів в боротьбі проти кіберзагроз.

Чому це важливо?

У зв'язку з низкою кібератак, що трапилися в 2016 році, фахівці SWIFT визначили 16 обов'язкових і 11 рекомендованих заходів щодо зниження ризиків інформаційної безпеки для своїх користувачів. В зв'язку з цим, всі користувачі повинні будуть провести атестацію своєї інформаційної інфраструктури (що забезпечує функціонування SWIFT), результати якої необхідно буде повідомити контрагентам і регулюючим органам.

Принципи інформаційної безпеки

Цілі зниження ризиків

Програма забезпечення безпеки клієнтів в платіжній системі SWIFT

Далі описаний комплекс обов'язкових і рекомендованих заходів щодо зниження ризиків інформаційної безпеки. Обов'язкові заходи засновані на існуючих рекомендаціях і встановлюють принципи забезпечення інформаційної безпеки. Рекомендовані заходи являють собою кращу практику, яку спільнота SWIFT радить впровадити кожному користувачеві в його інформаційній інфраструктурі (табл. 3).

Таблиця 3.

Комплекс обов'язкових і рекомендованих заходів щодо зниження ризиків інформаційної безпеки

Принципи	**Засоби і процедури зі зниженню ризиків інформаційної безпеки**
Обмеження доступу до мережі Інтернет і захист інформаційних систем	Обов’язкові Захист інфраструктури SWIFT. **Необхідно створити захищений від несанкціонованого доступу, а також атак, сегмент мережі, в якому функціонує SWIFT.** Контроль за привілейованими обліковими записами. **Доступ привілегірованих облікових записів повинен контролюватися і відслідковуватися. Їх використання повинно бути дозволеним тільки для обмежених видів діяльності, наприклад для розгортання і налаштування інформаційних систем, технічного обслуговування користувачів, а також в умовах надзвичайних обставин. У всіх інших випадках дозволено використання облікових записів з мінімальним правами доступу.**
Зниження ймовірності виникнення загроз	**Обов’язкові** ***Безпека внутрішніх інформаційних потоків.*** *Повинні бути впроваджені механізми забезпечення конфіденційності, цілісності і авторизації даних для захисту потоків даних «додаток SWIFT-додаток» і «оператор-додаток».* ***Оновлення.*** *Все апаратне і програмне забезпечення всередині захищеної зони SWIFT і на персональних комп'ютерах операторів повинно регулярно оновлюватися.* ***Підвищення надійності системи****. Повинні застосовуватися механізми відмовостійкості інформаційних систем.* **Рекомендовані** ***Безпека інформаційних потоків бек-офісу****. Повинні бути впроваджені механізми забезпечення конфіденційності, цілісності і авторизації даних для захисту потоків даних між додатками бек-офісу (або про-*

	міжним ПО) і компонентами підключення до інфраструктури SWIFT. ***Захист каналів передачі даних**. Конфіденційні дані, що відносяться до SWIFT і ті, що покидають захищений периметр повинні шифруватися.* ***Цілісність і конфіденційність інтерактивних сесій оператора.** Повинні використовуватися механізми забезпечення конфіденціальності і цілісності інтерактивних сесій оператора, здійснюють з'єднання з захищеним сегментом SWIFT.* ***Пошук уразливостей** . Захищений сегмент SWIFT, системи, а також ПК операторів повинні скануватися на уразливості за допомогою сучасних інструментів пошуку вразливостей.* ***Аутсорсинг.** Діяльність, передана в аутсорсинг, повинна захищатися, як мінімум, по тим же стандартом безпеки, який застосовувався б в разі їх здійснення в ініціації організації.*
Забезпечення фізичного захисту	**Обов'язкові** ***Забезпечення фізичного захисту**. Повинні застосовуватися засоби контролю і управління фізичним доступом до найбільш критичного обладнання (сервера, комутаційне обладнання, системи зберігання даних).*

Огляд заходів щодо зниження ризиків інформаційної безпеки користувачів SWIFT (табл. 4).

3. Система S.W.I.F.T. та інформаційна безпека

З технічної точки зору мережа S.W.I.F.T. 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 S.W.I.F.T. В системі S.W.I.F.T. використовуються як міжнародні стандарти, розроблені ISO, так і стандарти Міжнародної торгової палати (ICC). В результаті розвитку мережі S.W.I.F.T. утворилася нова мережа - S.W.I.F.T. II, яка базується на 4-х рівневої мережевій архітектурі і на

системі управління процесорами, що знаходяться в операційних центрах S.W.I.F.T.

Таблиця 4.

Принципи Засоби і процедури щодо зниження ризиків інформаційної безпеки

Принципи	**Засоби і процедури зі зниження ризиків інформаційної безпеки**
Попередження несанкціонованого доступу	**Обов'язкові** **Парольна політика. Парольні налагодження повинні враховувати такі параметри як довжина, складність, термін дії та історія паролів.** **Багатофакторна аутентифікація. Повинна використовуватися багатофакторна аутентифікація для доступу користувачів до додатків, пов'язаних з системою SWIFT.**
Управління ідентифікаційної інформацією	**Обов'язкові** *Контроль логічного доступу. Доступ до інформаційних систем надається відповідно до принципу «мінімальних привілеїв» і тільки в разі наявності службової необхідності.* **Рекомендовані** *Зберігання паролів. Паролі для привілейованих облікових записів повинні зберігатися на захищеному фізичному або логічному носії, а доступ до них повинен бути обмежений.*
Виявлення аномальних активностей в системах і даних про операції	**Обов'язкові** **Антивірусний захист.** *Програмне забезпечення для захисту від шкідливого ПЗ повинно бути встановлено, підтримуватися і регулярно оновлюватися на всіх інформаційних системах і персональних комп'ютерах.* **Цілісність ПО.** *Повинна здійснюватися пе-*

	ревірка цілісності програмного забезпечення на інтерфейсах передачі повідомлень і передачі даних, а також інших додатках, пов'язаних з системою SWIFT. **Цілісність бази даних.** *Повинна здійснюватися перевірка цілісності баз даних в яких ведеться запис операцій SWIFT.* **Моніторинг подій.** *Повинні бути впроваджені засоби, здатні виявити і зареєструвати аномальну активність в системах і даних про операції, а також повинен здійснюватися аналіз таких активностей.* **Рекомендовані** **Виявлення вторгнень.** *Для виявлення вторгнень і незвичайної мережевої активності повинні використовуватися спеціалізовані засоби виявлення і запобігання вторгненням.*
Реагування на інциденти і підвищення обізнаності в області інформаційної безпеки	**Обов'язкові** **Порядок реагування на кіберзагрози.** *Повинні бути визначені і протестовані порядки реагування на кіберзагрози.* **Навчання питань забезпечення інформаційної безпеки.** *Для всіх співробітників повинні проводитися щорічні заходи по навчанню питань в області інформаційної безпеки. Програма навчальних заходів, повинна бути розроблена з врахуванням конкретних функцій співробітників в рамках їх взаємодії в системі SWIFT.* **Рекомендовані** **Тестування на проникнення.** *Тестування на проникнення в додатки, базові комп'ютери і мережі повинно проводиться в межах захищеної зони SWIFTi на ПК операторів.* **Оцінка ризиків інформаційної безпеки.** *Оцінка ризиків інформаційної безпеки повинна проводиться на регулярній основі з метою підвищення готовності до реагування на інциденти і*

	підвищення рівня зрілості ІБ інфраструктури.

Логічна архітектура системи S.W.I.F.T. II підпорядковується основним принципам встановленим ISO (Міжнародна організація стандартизації) для взаємодії відкритих систем. Кожен активний компонент архітектури S.W.I.F.T. II 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 S.W.I.F.T. II 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 S.W.I.F.T. II 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 S.W.I.F.T. II і, по суті, є вхідною і вихідною точкою системи. Програмне забезпечення RP, взаємодіючи з програмами користувача, здійснює точне і безпечне логічне підключення до S.W.I.F.T. II. 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 S.W.I.F.T. II, індивідуальні користувачі повинні мати комп'ютерний термінал (CBT), який підключається до системи S.W.I.F.T. II через ряд місцевих вузлів підключення, відомих як точки доступу до системи S.W.I.F.T. II (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 S.W.I.F.T. II (STN)
- порти надаються користувачам

Доступ до послуг S.W.I.F.T. II 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 S.W.I.F.T.

II 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 S.W.I.F.T. II 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 S.W.I.F.T. II 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.

Рішення завдання комплексного забезпечення безпеки інформації в інформаційно - телекомунікаційних мережах необхідно забезпечити виконання наступних загальних принципів:

- захист інформації (з метою забезпечення її конфіденційності, цілісності та достовірності) при її зберіганні, обробки і передачі по мережах;
- підтвердження достовірності об'єктів даних і користувачів (аутентифікація сторін, що встановлюють зв'язок);
- виявлення і попередження порушення цілісності об'єктів даних;
- живучість мережі зв'язку при компрометації частини ключової системи;
- захист технічних засобів і приміщень. в яких ведеться обробка конфіденційної інформації. від витоку інформації по побічним каналам і від можливо впроваджених в технічні засоби електронних пристроїв знімання інформації;
- захист програмних продуктів від впровадження програмних закладок і "вірусів";
- захист від несанкціонованого доступу до інформаційних і ресурсів і технічних засобів мережі, в тому числі і до засобів її управління, з метою запобігання зниженню рівня захищеності інформації та самої мережі в цілому;
- реалізація організаційно-технічних заходів, спрямованих на забезпечення схоронності конфіденційних даних.

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.

У світлі нинішніх тенденцій зростання відкритості технологій кредитно-фінансової сфери (використання Internet та інших відкритих мереж в якості транспортної мережі передачі даних) особливого значення набуває питання забезпечення конфіденційності, цілісності та достовірності передавався інформації. Досягти цього можна лише, використовуючи криптографічно стійкі і ефективно реалізовані кріптосхеми, і організовуючи надійні і зручні системи розподілу ключової інформації. Хоча в багатьох системах передачі економічно значимої інформації будуть панувати специфічні вимоги (в залежності від топології – навмисної зміни одержувачем повідомлення з метою дискредитації відправника або комунікаційної компанії;

- видачі одного користувача системою за іншого, щоб зняти з себе відповідальність або ж використовувати його повноваження з метою формування помилкового повідомлення, зміна законного, санкціонування хибних обмінів повідомленнями або ж їх підтвердження;
- відмови від факту формування та передачі повідомлення;
- твердження про те, що повідомлення отримано від деякого користувача, хоча насправді воно сформоване самим зловмисником;
- твердження про те, що одержувачу в заданий момент часу було послано повідомлення, яке насправді не надсилалося (або надсилалося в інший момент часу);
- відмови від факту отримання повідомлення, яке насправді було отримано, або видача неправдивих відомостей про час його отримання;
- несанкціонованого зміни повноважень інших користувачів на відправку та отримання повідомлень (помилкова запис інших осіб, обмеження або розширення встановлених повноважень і т.п.);
- набору статистики обміну повідомленнями (вивчення того, хто, коли і до яких повідомленнями отримує доступ);
- заяви про сумнівність протоколу забезпечення безпеки доставки повідомлень через розкриття деякої конфіденційної інформації;
- введення зловмисником помилкових повідомлень доручень і службової інформації;
- постановки перешкод в каналах зв'язку з тією метою виключення можливості доведення повідомлення до одержувача.

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.
- Всі питання, пов'язані з безпекою в системі S.W.I.F.T. II, умовно можна розділити на наступні розділи:
- Фізична безпека
- Безпека логічного доступу до системи S.W.I.F.T. II
- Забезпечення безпеки повідомлень, переданих і збережених в системі
- Безпека обміну повідомленнями користувач-користувач
- Засоби безпеки, що забезпечуються системою S.W.I.F.T. II складаються з:
- процедури входу в систему
- процедури вибору додатка
- нумерації повідомлень
- перевірки помилок передачі
- криптозахисту повідомлення знаходиться в мережі S.W.I.F.T. II
- контролю доступу до повідомлень в SAP-ах, регіональних процесорах, комутаційних процесорах, центрах управління системою

Відділ Головного інспектора системи S.W.I.F.T. II (CIO) управляє всіма питаннями, пов'язаними із забезпеченням безпеки роботи мережі S.W.I.F.T. II Користувачам рекомендується забезпечувати належну безпеку процедур, що здійснюються в їх власних організаціях, наприклад, контроль доступу до терміналів S.W.I.F.T. II, управління їх підключенням і використанням.

Фізична безпека

Здійснюється на основі розмежування і контролю доступу до всіх операційних і адміністративним вузлів S.W.I.F.T. шляхом використання електронних засобів і засобів виявлення несанкціонованого доступу. Застосовується також дистанційне керування для вузлів S.W.I.F.T. II, які управляються автоматично. Якщо користувач запитує центр про доступ до SAP, то в обов'язковому порядку повинен бути зроблений запит до CIO і без його санкції нікому не буде дано дозвіл на доступ до SAP.

Безпека логічного доступу до системи S.W.I.F.T. II

Як вже говорилося вище, користувачі можуть отримати фізичний доступ до системи S.W.I.F.T. II тільки через CBT, що працює з одним або більше LT. Кожному LT призначаються унікальні таблиці безпеки для процедур LOGIN і SELECT (вибір фінансового додатки - FIN), які представляють собою послідовності ключів в табличному вигляді. Кожен ключ в таблиці може використовуватися тільки один раз і пов'язаний з послідовними номерами процедур, які використовують ці ключі. Ці таблиці формуються і відсилаються користувачеві до їх підключення до системи S.W.I.F.T. II на основі запиту на їх використання,

причому нові таблиці безпеки створюються відразу після висилки чергових таблиць і пересилаються користувачеві тільки в міру необхідності. Користувачі, які використовують таблиці безпеки, можуть запросити в відділі Головного інспектора таблиці з 2400 ключами, замість звичайних таблиць (1200 ключів).

Доступ LT до системи S.W.I.F.T. II проводиться за допомогою команди LOGIN. До того, як буде надіслано запит LOGIN, користувачеві необхідно ввести ключ запиту і ключ відповіді з таблиці безпеки LOGIN. Мета запиту LOGIN:

Визначити логічний шлях для зв'язку LT з системою

Обмежити доступ в систему несанкціонованих користувачів

Дозволити користувачам перевірити, що вони підключилися до справжньої системі S.W.I.F.T. II

Вказувати державний розмір вікна, яке повинно бути відкрито для сеансу GPA

При запиті процедури LOGIN система S.W.I.F.T. II виробляє наступну послідовність дій:

Перевіряє заголовок і текст повідомлення, яке надсилатиметься процедурою LOGIN

Перевіряє справжність кінцевика MAC, сформованого з використанням ключа з таблиці безпеки, але не містить інформацію про сам ключ

Якщо підтвердження автентичності користувача пройшло успішно, то порядковий номер запиту LOGIN (LSN) порівнюється з очікуваним системою LSN. Якщо LSN знаходиться в допустимих межах, то система перевіряє, що запит LOGIN, виданий після дня зазначеного в останній команді LOGOUT (вказує тимчасові рамки для LT, протягом яких від даного LT не братимуться запити). Якщо ж LSN не збігається з очікуваним, то в поле підтвердження автентичності системи вказується наступний очікуваний LSN

Підтверджує запит LOGIN, повертаючи або позитивне підтвердження LOGIN (LAK), або негативне підтвердження LOGIN (LNK). Підтвердження міститиме кінцевик MAC, заснований на ключі відповіді, але не містить інформацію про нього і дозволяє користувачеві перевірити справжність системи

Записує спробу LOGIN разом з відповіддю системи в передісторію LT

Примітка: Спроба провести запит LOGIN на лінії зв'язку, по якій LT вже увійшов в систему розглядається, як серйозна помилка і ігнорується системою.

Доступ до програми FIN (з якого відправляються повідомлення користувач-користувач і ряд системних повідомлень) проводиться за допомогою команди SELECT, яка проходить процедуру підтвердження для гарантії того, що:

Тільки перевірені користувачі можуть отримати доступ до системи S.W.I.F.T. II

Користувач зв'язався зі справжньою системою S.W.I.F.T. II

Алгоритм підтвердження справжності повідомлення, використовуючи довільний ключ захисту і ключ відповіді, пов'язані послідовним номером із запитами LOGIN або SELECT, і інші елементи даних, (день / час позначки) формує кінцевик MAC.

Примітка: Цей процес відрізняється від процесу підтвердження автентичності повідомлення користувач-користувач. Він не вимагає обміну «ключами достовірності», але замість цього використовуються унікальні таблиці безпеки, створені для кожного користувача.

За винятком довільного ключа захисту і ключа відповіді, відомі тільки системі S.W.I.F.T. II і кінцевому користувачеві, елементи даних, що використовуються для формування MAC, надсилаються в складі MAC, як частина повідомлень LOGIN і SELECT. У відповідь система S.W.I.F.T. II формує новий кінцевик MAC, з тим же ключем захисту, але з іншими елементами даних і включає його в SAK або LNK, тим самим дозволяючи користувачеві підтвердити достовірність системи S.W.I.F.T. II Далі відбувається припинення підключення користувача до системи і формується запит з новим кінцевиком, використовуючи новий ключ доступу, для гарантії того, що сеанс буде відновлено санкціонованим LT з одночасною перевіркою автентичності системи S.W.I.F.T. II.

В даний час в системі S.W.I.F.T. II була розроблена і рекомендована Радою директорів для повсюдного використання поліпшена архітектура системи забезпечення безпеки, яка відповідає в широкому сенсі сучасному рівню розвитку телекомунікаційних технологій та криптографічних методів. Основою нового підходу стало використання інтелектуальних карт (ICC), зміна алгоритму перевірки достовірності і збільшення довжини двосторонніх ключів, якими обмінюються користувачі.

Для забезпечення безпеки логічного доступу до системи S.W.I.F.T. II в рамках нового підходу була розроблена служба безпечного входу в систему і вибору режиму (SLS), яка дозволяє користувачам отримати доступ до послуг системи S.W.I.F.T. II за допомогою ICC замість використання паперових таблиць Login і Select. Застосування ICC вимагає використання зчитувачів карт. Необхідно зауважити, що на даному етапі пропонується два різних типи зчитувачів карт. Перший - спрощений зчитувач карт (BCR), який підтримує тільки службу SLS. Другий - зчитувач карт з модулем захисту (SCR), в якому крім функцій кардридера реалізована також функція модуля апаратного захисту, що виконує генерування ключів і шифрування секретної інформації (застосовується як для підтримки SLS, так і інших служб, створених в рамках нового підходу). Так як в SCR повинні зберігатися секретні дані, він зроблений захищеним від розтину - будь-яка спроба дістатися до внутрішніх частин пристрою приводить до автоматичної знищення секретної інформації, що зберігається в SCR.

Крім того, при обслуговуванні SCR або BCR передбачено кілька різних варіантів режимів роботи (відключений від CBT або підключений до CBT), широкий перелік варіантів конфігурації цих пристроїв спеціально виділяються людьми (офіцери безпеки), а також широкий перелік послуг з навчання персоналу організації.

Служба SLS і операції

Як вже говорилося, основне призначення SLS - заміна паперових таблиць Login / Select новим механізмом, здатним генерувати сеансові ключі доступу до системи, які при використанні паперових таблиць доводилося прочитувати операторам CBT вручну. Необхідно відзначити, що ICC не містить самих ключів

доступу, але містить алгоритм, який може згенерувати необхідний сеансовий ключ для будь-якого запиту Login / Select. Так як даний алгоритм відрізняється від підведеного в системі S.W.I.F.T. II в даний час для генерації паперових таблиць, ключі доступу, одержувані з ICC, відрізняються від своїх еквівалентів в паперових таблиць.

Для забезпечення логічного доступу до послуг системи S.W.I.F.T. II необхідно вставити відповідним чином сконфігурованої ICC. У зчитувач карт і ввести PIN-код на клавіатурі пристрою для читання. При виборі функції Login (Select) на CBT необхідні коди автоматично генеруються ICC і передаються в CBT, до якого підключений зчитувач. Потім CBT продовжує обробляти запит Login (Select) звичайним чином. Для більшості користувачів зчитувач карт буде залишатися підключеним до CBT з метою отримання максимальної вигоди від використання служби SLS. Але є можливість використання і непідключеного зчитувача карт (наприклад, для віддалених терміналів або в разі аварії), коли необхідні коди доступу хоча і генеруються в ICC, але відображаються на дисплеї зчитувача карт, а потім вручну вводяться в CBT.

Забезпечення безпеки повідомлень, переданих і збережених в системі

Безпека обміну повідомленнями в системі S.W.I.F.T. II складається з наступних основних пунктів:

- забезпечення безпеки передачі
- перевірка повідомлень
- забезпечення безпеки доставки
- Зокрема, з огляду на, що мережа захищена від несанкціонованого доступу, потік повідомлень при передачі і зберіганні повинен мати захист від:
- втрати, підтвердження, помилковою доставки або затримки повідомлень
- помилок при передачі і зберіганні
- втрати конфіденційності
- внесення в повідомлення неправдивих змін

Забезпечення безпеки передачі

У всі повідомлення додатків GPA і FIN системи S.W.I.F.T. II додається обов'язковий кінцевик CHK, який містить контрольну суму даного повідомлення, перераховується в вузлах введення / виведення мережі. Якщо відбулося спотворення повідомлення протягом передачі (це встановлюються шляхом перевірки контрольної суми, прийнятого повідомлення, що є унікальною для кожного повідомлення, з обчисленої контрольної сумою) і це не було зафіксовано в протоколі перевірок низького рівня, то у відповідь на це повідомлення буде передано негативне підтвердження і воно буде надсилатися повторно.

Перевірка повідомлень

Всі вхідні повідомлення перевіряються відповідним RP до того, як передати їх SP. Тільки повідомлення, що відповідають стандартам S.W.I.F.T. II і синтаксису, приймаються до доставки. Результати безперервних перевірок постійно зберігаються і через дуже суворих стандартів, встановлених S.W.I.F.T. II, будь-яка серйозна помилка протоколу призводить до закриття сеансів FIN або GPA.

Безпека доставки

Після суворих перевірок, проведених для всіх вхідних потоків повідомлень і високоякісних методів забезпечення безпеки, використаних для передачі повідомлень, всі повідомлення, позитивно підтверджені системою S.W.I.F.T. II, розглядаються правильними і отже доставленим системі.

Обов'язковий кінцевик CHK використовується отримують LT для перевірки того, що жодної помилки не з'явилося при передачі між вхідним RP і реципієнтом. Обов'язкове використання підтверджень прийому користувачем повідомлення (UAK / UNK) дає можливість системі S.W.I.F.T. II підтвердити чи прийняв LT надіслане до нього повідомлення чи ні.

Система S.W.I.F.T. II не розглядатиме повідомлення, доставленим до тих пір, поки позитивне підтвердження прийому користувачем повідомлення (UAK) не отримано від LT-реципієнта. Система S.W.I.F.T. II буде намагатися надіслати Ваше повідомлення 11 разів, після чого доставка повідомлення припиняється і відправник повідомляється, що повідомлення не може бути доставлено. Кожна наступна спроба доставки після першої буде містити відповідну кількість кінцевиків PDM. Перевірка повідомлень S.W.I.F.T. II гарантує, що повідомлення для підготовки (які мають кінцевик TNG) не можуть бути адресовані чинним місць призначення, і навпаки діючий потік повідомлень не може бути адресований до метам призначення з підготовки.

Безпека обміну повідомленнями користувач-користувач

При обміні повідомленнями між користувачами для забезпечення конфіденційності і автентичності, а також для контролю за цілісністю повідомлень система S.W.I.F.T. II рекомендує використовувати алгоритм перевірки достовірності. Перевірка достовірності - важлива частина системи забезпечення безпеки S.W.I.F.T. II, вона ґрунтується на обміні між користувачами ключами і перевірці того, що результат перевірки достовірності був представлений в певних типах повідомлень.

Приймаючий термінал перевіряє текст отриманого повідомлення за допомогою стандартного алгоритму SA / 2 і узгодженого ключа достовірності. І якщо в ході перевірки отримано негативний результат, то це може швидше за все статися через:

- помилок передачі
- неправильного ключа достовірності

Ключ достовірності складається з 32 шістнадцяткових символів, розділених на дві частини по 16 знаків і може бути як для передачі, так і для прийому або використовуватися в обох напрямках. Для формування ключа необхідно дотримуватися наступних правил:

- перша і друга половина повинні бути різні
- в кожній половині будь дозволений символ може з'явитися тільки один раз

Крім цього необхідно відзначити, що ключі достовірності передаються між кореспондентами поштою, і для забезпечення безпеки ключової інформації всім користувачам системи S.W.I.F.T. II рекомендується підтримувати кореспо-

ндентські відносини тільки з відомими користувачами і в організації - ініціатора обміну вибирати тип ключа достовірності відповідно до проведеної політикою безпеки цієї організації.

Як вже говорилося в зв'язку з переходом на нові технології забезпечення безпеки в системі S.W.I.F.T. II, що використовують ICC, був вдосконалений і процес обміну ключами достовірності між користувачами, результатом чого стала поява служби обміну двосторонніми ключами (BKE). Призначення BKE - замінити тяжку систему ручного обміну двосторонніми ключами підтвердження автентичності між кореспондентами по відкритій пошті на систему, яка використовує нові повідомлення S.W.I.F.T. II і зчитувач карт з модулем захисту, спеціально розроблені для цієї мети. Нова система дозволить повністю автоматизувати процес обміну ключами. За новою технологією кожен двосторонній ключ підтвердження автентичності створюється всередині SCR і зашифрована перед передачею в CBT, до якого SCR підключений. Ключі підтвердження автентичності, якими обмінюються кореспонденти, можуть бути або двонаправленими (коли один і той же ключ використовується для перевірки автентичності переданих і прийнятих повідомлень окремого кореспондента), або односпрямованим (коли використовуються окремі ключі на прийом і на передачу повідомлень). Служба BKE заснована на стандарті ISO з обміну ключами (ISO 11166 – Banking - Key Management by Means of Asymmetric Algorithms). У цьому стандарті визначено використання асиметричних алгоритмів для шифрування і цифрового підпису двосторонніх ключів, якими обмінюються кореспонденти. Спеціально для забезпечення розподілу відкритих ключів в системі S.W.I.F.T. II був створений Центр управління безпекою (SMC) в складі якого працює Центр сертифікації ключів, який видає сертифікати відкритих ключів користувачів системи S.W.I.F.T. II.

Наступний за процедурами переходу і початкової установки реальний обмін двосторонніми ключами підтвердження автентичності через мережу S.W.I.F.T. II включає в себе обмін чотирма спеціальними повідомленнями S.W.I.F.T. II між кореспондентами, один з яких виступає як ініціатор обміну, а інший - як одержувач. Перші два повідомлення використовуються виключно для цілей встановлення сеансу обміну двосторонніми ключами. У третьому повідомленні ініціатор обміну посилає ключ, створений і зашифрований всередині SCR, використовуючи відкритий ключ одержувача. Так само SCR створює цифровий підпис ініціатора обміну ключами. Після отримання третього повідомлення учасник обміну перевіряє цифровий підпис і якщо вона дійсно належить відправнику, то йому надсилається підтвердження, ключ визнається вірним і заноситься в файл двосторонніх ключів.

Безпосередньо після обміну новий ключ стає «майбутнім» ключем для цих кореспондентів і буде використовуватися для перевірки фінансових повідомлень, починаючи з взаємно узгоджених дати і часу. При використання ключів прийому / передачі кожен кореспондент є ініціатором обміну для свого ключа передачі.

Але на закінчення хотілося б відзначити, що досвід забезпечення інформаційної безпеки в системі S.W.I.F.T. II II, хоча і є по суті своїй цінним, але йо-

го застосовність до окремо взятої ситуації не є однозначним при планування і побудова системи інформаційної безпеки, де основними факторами у виборі моделі і принципів будуть наступні:

- політика безпеки явно суперечить політиці відкритості
- витрати на побудову системи інформаційної безпеки не повинні перевищувати величину можливої шкоди

Лекція 8 Основні положення кібербезпеки даних в мережі банкоматів (3 год)

План лекції
1. Система банкоматів
2. Забезпечення безпеки банкоматів
3. Локальна відеоохоронна система

1. Система банкоматів

Банкомат (від банківський автомат, іноді АТМ від англ. Automated teller machine) — програмно-технічний комплекс, призначений для автоматизованих видачі й/або приймання наявних коштів як з використанням платіжних карт, так і без, а також виконання інших операцій, у тому числі оплати товарів і послуг, складання документів, що підтверджують відповідні операції.

Історія

Прототип першого банкомата був винайдений американським ученим арм'янського походження Лютером Джорджем Симджяном (англ. Luther George Simjian) ще в 1939 році. Пристрій видавав готівку, але при цьому не міг списати їх з рахунку: апарат не був пов'язаний з банком. Симджян запропонував випробувати винахід City Bank of New York, але через півроку банкіри повернули машину, повідомивши, що не бачать у ній необхідності. Винахід Симджяна було майже на 30 років забутий й дороблений тільки наприкінці 1960-х років.

Перший банкомат по видачі готівки, Automated Teller Machine (ATM), був установлено 27 червня 1967 року у районі Енфілд на півночі Лондона (Великобританія) у відділенні британського банку Barclays. Винахідником його був шотландець Джон Шепард-Баррон, що працював на замовлення компанії De La Rue– британського виробника паперу для грошових знаків більш ніж 150 країн світу. На ідею створення банкомата Шепард-Баррон наштовхнула побачена їм робота автомата із продажу шоколаду. Через неможливість перевірити наявність грошей на рахунку клієнта сума готівки, що знімалася, була обмежено фунтами. АТМ був «безкарточним» банкоматом і видавав готівку в обмін на спеціальний ваучер (чек), які треба було заздалегідь одержувати в банку. Для захисту від підробки на чеках була слаборадіоактивна, а тому безпечна для клієнтів, мітка (изотопС14).

В 1966 році шотландський інженер Джеймс Гудфеллоу одержав патент на секретний захисний код з 4 цифр, Персональний ідентифікаційний номер (Pin-PIN-код). Згідно з легендою, спочатку винахідник планував Пін-код довжиною в 6 цифр, але пізніше скоротив довжину коду до чотирьох цифр, нібито саме стільки цифр могла запам'ятати його дружина. Згодом Пін-коди стали широко використовуватися для захисту від несанкціонованого доступу до банківських рахунків.

Впровадження банкоматів відбувалося поступово. В 1971 році перші типи банкоматів використовувалися приблизно в 35 американських банках. Першим

банком, який в 1972 році почав повсюдно встановлювати банкомати, став американський Citibank. У тому ж році банк Lloyds увів у Великобританії перші онлайн-онлайн-банкомати за назвою Cash-Point, розроблені компанією IBM. Замість ваучера вони використовували пластикові карти з магнітною смугою, що було набагато зручніше для клієнта. Розвиток телекомунікацій дозволив будувати мережі банкоматів, які могли використовуватися відразу декількома банками. Уперше це відбулося в 1972—1975 роках у США. Кілька сотень банкоматів 18 банків у штаті Вашингтон були об'єднані в мережу за назвою Exchange. Пізніше були винайдені банкомати, здатні не тільки видавати готівку, але й приймати її.

У СРСР перші банкомати з'явилися в 1991 році, два в московському Центрі міжнародної торгівлі (ЦМТ) і один в офісі американської компанії American Express на вулиці Садово-Кудринский. Видавали вони не готівку, а дорожні чеки AmEx.

ДО 1975 році у світі працювало ледве більш 5 тис. банкоматів, з них близько 3140 — в 534 американських банках. Згідно даним дослідницької компанії RBR, наприкінці 2011 року в усьому світі налічувалося 2,4 млн банкоматів, а до 2017 році, за прогнозами RBR, кількість АТМ виросте до 3,4 млн. В 2000 -х роках виробники банкоматів почали впроваджувати технологію Cash Recycling, що полягає в тому, що наявні гроші, внесені одним клієнтом у банкомат, можуть бути отримані на руки іншим клієнтом. Великий вплив на індустрію АТМ в останні десять років виявляють розвиток Інтернету і мобільних технологій. На початку 2010--х років компанія KAL оголосила про розробку безготівкового банкомата, Retail Teller Machine (RTM). Замість готівки такий банкомат видає клієнтові рахунок, який той пред'являє касирові магазину для оплати придбаного товару. В 2012 році в японському банку The Ogaki Kyoritsu Bank (Огаки, префектура Гифу) з'явилися банкомати, що здійснюють ідентифікацію клієнтів не по банківській карті й паролю, а по введеній даті народження й прикладеної до сенсорного пристрою долоні.

Принцип дії

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.

Банкоматне шахрайство

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

Способи

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 (у тому числі випадки, коли Пін-код зберігається поруч із картою або записується на ній).
- «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.

Організаційну структуру цього підприємства і специфічні деталі функціонування мережі визначають банки-учасники.

Практика створення телекомунікаційного середовища із застосуванням банкоматів свідчить, що вигіднішою для банків є побудова загальних мереж банкоматів і об'єднання вже побудованих мереж. Результатом цього стає стандартизація кредитних карток, від якої виграють і банк і його клієнти.

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.

Уже 1990 року 30% усіх операцій із БА проводились через автомати, що належали іншим банкам. Однак зростання колективних мереж породило і безліч проблем, що пов'язані з розробленням загальних стандартів безпеки, сумісністю обладнання, правилами врегулювання платежів тощо. Окрім того, обслуговування через спільні мережі банківських автоматів є дорожчим, оскільки три чверті всіх банків беруть плату з клієнтів за користування чужими банкоматами (від 0,75 до 2% за операцію і 3 долари США за операцію через банкомат в іншій країні). Ці кошти використовують для часткового покриття витрат на утримання колективних мереж.

Порівняльна статистика з банківських автоматів, які є в розпорядженні різних країн, дозволяє, зокрема, відзначити велику щільність автоматів у США і Японії та, навпаки, малу їх пильність в Італії, Німеччині та Нідерландах. Окрім того, у США, як і в Японії, парк автоматів дуже подрібнений між "приватними" мережами та мережами незалежних установ.

Щодо експлуатації національних мереж банківських автоматів у різних країнах можна навести такі дані. У США функціонують мережі: Plus і Cirrus, що об'єднують банкомати більшості штатів із кількістю клієнтів понад 60 млн. З 1991 року в мережі банкоматів Cirrus приймаються картки Eurocard!'MasterCard згідно з укладеною угодою між EuroCard International і Cirrus International. У Великобританії конкурують між собою мережі: Visa {Barclays bank) і ACCES (National Westminster Bank і Midlands Bank). Розподіл банкома-

тів за мережами виглядає так: мережа Barclays (49%) із банками Lloyds, Bank of Scotland і Royal Bank; мережа Natwest (33%) із банком Midland; мережі Building societies (будівельних об'єднань) Link та Matrix.

У Бельгії співіснують дві мережі: Mistercash і Bancontact У Франції всі карткові операції банкоматів обслуговує одна мережа, яка має назву "Банківські картки".

Банкомати Німеччини обслуговує загальнонаціональна мережа Eurocheque та спеціалізовані банківські мережі.

В Італії 70% автоматів належать до мережі Bancomat, решта 30% - до інших спеціалізованих банківських мереж.

У Нідерландах використовують міжбанківські мережі автоматичних банківських кас, де застосовується гарантійна чекова картка, та міжбанківські мережі ощадних кас.

В Японії співіснують дев'ять міжбанківських національних мереж та 51 спеціалізована банківська мережа. Одна з найбільших мереж NCS (Nippor cash service) нараховує 53 банки учасники.

Окрім національних угод за картками, укладено міжнародні угоди. Так, 1980 року близько 1 700 АТМ, що належали емітентам карток Visa у Великобританії, були підключені до міжнародної мережі, в якій працювало близько 21 700 АТМ у 22-х країнах світу. А вже через чверть століття грошовий обіг за картками системи Visa International перевищив суму в 2 трильйони доларів, а кількість точок, де обслуговують Visa, досягла кількості 28 мільйонів. Регіональні підрозділи охоплюють: Центральну і Східну Європу, Близький Схід, Африку, Латинську Америку, Азію і країни Тихого океану, США, Канаду.

Так, банки багатьох західноєвропейських країн створюють мережі банківських автоматів, дозволяючи резидентам інших країн, що мають картку Eurocheque, користуватися послугами автоматів на території будь-якої країни. З 1989 року 45 млн власників зазначених карток могли здійснювати операції через банківські автомати у Великобританії, Німеччині, Австрії, Італії, Данії та в інших країнах. Більшість банків Англії випускають міжнародні чекові картки Eurocheque, які можуть застосовуватись для отримання готівкових грошей через АТМ єдиної мережі у понад 20 країнах, що випускають єврочекові чекові картки.

У Великобританії тільки АТМ Midland-банку дозволяє здійснювати отримання готівки за допомогою єврочекових карток. Це можливо для карток, що випущені в Бельгії, Німеччині, Ірландії, Люксембурзі" Нідерландах, Португалії і самим Midland-банком. У 1987 році було укладено взаємну угоду між системами Link і Plus (Північна Америка), що дало власникам карток Link. на той час доступ до 11 000 АТМ на території Північної Америки і 67 млн власників карток Plus - доступ до АТМ Links.

EuroCard та MasterCard, діючи спільно, значно збільшили свої обороти після підписання угоди з компаніями Cirrus та Maestro, результатом якої стало придбання великої мережі банкоматів та електронних платіжних терміналів. У вересні 1992 року було утворено EuroPay International - як результат злиття EuroCard International, Eurocheque International, Eurocheque International

Holdings. MasterCard International належать 100% капіталу Cirrus System (мережа банківських автоматів), 50% акціонерного капіталу Maestro International (всесвітня система електронних платіжних терміналів), 12,25% капіталу EuroPay International та 15% капіталу European Payment Systems Services - EPSS (Європейська система платіжних послуг). У свою чергу, EuroPay International володіє 86% капіталу EPSS і 50% капіталу Maestro International

Щодо рентабельності банківських автоматів слід зазначити, що за терміну окупності сім років автомати з видачі готівкових грошей можуть бути рентабельними в разі виконання не менше ніж 40 тис. операцій на рік; для банкоматів, розміщених усередині банку, межа становить 75 тис. операцій, поза банком - 126 тисяч. Як свідчить практика експлуатації банкоматів, автомати з видачі готівкових грошей уже всі рентабельні, а універсальні банкомати поки що ні. При цьому спостерігається зниження собівартості автоматів за налагодження їх масового випуску. Окрім того, якщо в деяких країнах видача грошей автоматом свого банку проводиться безкоштовно і лише за отримання грошей в автоматі іншого банку стягується певний комісійний збір за міжбанківський обмін, то в інших країнах, наприклад, у США, за кожне отримання грошей потрібно платити, що значно знижує межу рентабельності, а відповідно, і термін окупності.

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. Для найпопулярніших мереж банкоматів у Великобританії, США цей показник становить 2-4 тисячі карток на 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 банкоматів. 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.

Наприклад, клівлендський банк Key Bancorp розробив унікальний метод управління мережею своїх банкоматів без установлення плати за користування ними. Проект банку Agent Bank (агентський банк) - це програма, що передбачає здавання в оренду частини своїх банкоматів невеликим фінансовим установам, які хочуть розширити свою присутність та підвищити конкурентоздатність, водночас надаючи банкові більш суттєву вигоду від своїх каналів.

Споживачі - учасники програми Agent Bank, окрім банкоматів "свого" банку, можуть користуватися будь-яким банкоматом банку Key Bancorp. При цьому комісії не стягується ні після самої операції, ні наприкінці місяця. Ця програма підтверджує, що банки змінюють своє ставлення до комісійних збо-

рів, мереж своїх банкоматів та каналів доставки і можуть отримувати набагато суттєвішу вигоду від своїх каналів. При цьому, як свідчать дані консультаційної компанії Dove Consulting, кількість фінансових компаній-орен-дарів швидко зростає (приблизно удвічі за рік).

Партнери (банки -агенти) Key Bancorp орендують банкомати і платять одноразову авансову комісію. Окрім цього, банк-агент платить банкові-орендодавцю за кожну трансакцію своїх клієнтів, здійснену банкоматом орендодавця - близько 20-25 центів за кожну операцію. Ця плата призначена для покриття витрат на підтримку мережі.

Сьогодні мережа SUM від нью-йоркської фондової біржі покриває північно-східний регіон США. Фінансова установа, що випускає картки під логотипом біржі, надає частину своїх банкоматів у загальну мережу. Клієнти фінансової установи отримують можливість безоплатного користування будь-яким банкоматом мережі SUM, яка сьогодні нараховує близько 3 000 автоматів, представлених 500 банками.

2. Забезпечення 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).

3. Локальна відеоохоронна система

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 синх-

ронізує 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 (можливість пошуку за датою / часом, ID банкомату, номеру картки клієнта, сумі транзакції, тривожного події);
- 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

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

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.

Лекція 9. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України

(4 год)

План лекції

1. Вимоги до інформаційної безпеки в банківській системі України
2. Вимоги до банків
3. Вимоги щодо впровадження СУІБ
4. Криптографічний захист інформації в інформаційних системах Національного банку

1. 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 (далі – Національний банк), з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах Національного банку.

3. У цьому Положенні терміни та поняття вживаються в таких значеннях:

1) багатофакторна автентифікація – автентифікація, яка здійснюється за

допомогою захищених механізмів двох або більше типів [наприклад,

застосування для автентифікації пароля разом із апаратним засобом захисту інформації (токеном) або біометричної автентифікації разом із паролем];

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 (комп'ютерне обладнання, інші компоненти інформаційних систем банку) усередині периметра банку;

5) мінімальний рівень повноважень – повноваження та права доступу,

мінімально 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.

2. 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. 1 Принципи забезпечення інформаційної безпеки:

1) підхід до забезпечення інформаційної безпеки має бути системним (комплексним);

2) процес удосконалення та розвитку інформаційної безпеки має бути безперервним і здійснюватися шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;

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

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

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

3. Принципи криптографічного захисту інформаційних систем Національного банку:

1) 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;

2) 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;

3) 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);

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

5) 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;

6) 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.

2.2 Передумовами впровадження СУІБ у банку є:

1) упровадження процесного підходу до діяльності банку;

2) 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.

3. Вимоги щодо впровадження СУІБ

14. 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.

15. 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.

16. Банк зобов'язаний покласти на керівний орган СУІБ обов'язок виконання таких завдань:

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

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

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

4) визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;

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

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

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

1) цілі інформаційної безпеки;

2) сферу застосування політики інформаційної безпеки;

3) принципи, правила та вимоги інформаційної безпеки в банку;

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

18. 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.

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

20. 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.

21. 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.

22. 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.

4. Криптографічний захист інформації в інформаційних системах Національного банку

23. 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.

24. 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.

25. Банк зобов'язаний призначити відповідальну особу за інформаційну безпеку банку (Chief information security officer, CISO), яка має повноваження, достатні для прийняття управлінських рішень (посада не нижче заступника голови правління банку), та забезпечує:

1) стратегічне керівництво з питань інформаційної безпеки банку;

2) визначення напрямів розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку банку;

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

4) контроль за впровадженням заходів безпеки інформації в банку.

26. 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.

27. Підрозділ з інформаційної безпеки банку має здійснювати:

1) розроблення вимог щодо налаштувань безпеки інформаційних систем банку;

2) розроблення або участь у розробленні документів банку щодо інформаційної безпеки;

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

4) розслідування інцидентів безпеки інформації;

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

28. 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.

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

30. 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.

31. 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.

32. 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.

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

34. 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:

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

2) категорії інформації, яка може оброблятися на змінних носіях інформації;

3) ідентифікації змінних носіїв інформації, які використовуються в банку;

4) обмежень використання змінних носіїв інформації (у тому числі поза межами банку);

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

6) обов'язковості перевірки змінних носіїв інформації на наявність зловмисного коду перед використанням у банку.

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

36. 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:

1) вимоги до ідентифікації, автентифікації, авторизації користувачів;

2) послідовність дій під час управління доступом, у тому числі в разі віддаленого доступу (реєстрація, надання повноважень, перегляд та скасування доступу);

3) перелік типових функцій та прав доступу до інформаційних систем банку;

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

5) періодичність контролю наданих прав доступу;

6) вимоги до протоколювання дій під час управління доступом.

37. Банк зобов’язаний забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (уключаючи доступ привілейованих користувачів).

38. 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.

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

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

2) заборону одноосібного ініціювання заявки, підтвердження та надання доступу;

3) перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень;

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

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

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

1) п’яти невдалих спроб автентифікації поспіль (автоматичне блокування);

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

3) звільнення користувача.

42. 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 зберігання не менше ніж протягом трьох років.

43. 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.

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

1) цілі безпеки, для яких використовуються криптографічні заходи безпеки (конфіденційність, цілісність, доступність);

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

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

1) процедури генерації ключів для різних криптографічних систем;

2) розподілу ключів серед відповідальних осіб;

3) зберігання ключів;

4) заміни або оновлення ключів;

5) поводження із скомпрометованими ключами;

6) відкликання ключів;

7) відновлення ключів, які зруйновано;

8) процедури резервного копіювання або архівування ключів;

9) знищення ключів;

10) реєстрації та аудиту діяльності, пов'язаної з управлінням ключами.

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

1) асиметричні алгоритми:

- алгоритм Діффі – Геллмана (далі – алгоритм DH) для узгодження сеансових ключів шифрування;
- алгоритм цифрового підпису (далі – алгоритм DSA) для цифрових підписів;
- алгоритм Діффі – Геллмана на еліптичних кривих (далі – алгоритм ECDH) для узгодження сеансових ключів шифрування;
- алгоритм цифрового підпису на еліптичних кривих (далі – алгоритм ECDSA) для цифрових підписів;
- алгоритм Ривест – Шаміра – Адлемана (далі – 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 еліп-

тичних кривих. Формування та перевіряння", затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002)] для цифрових підписів;

2) алгоритми безпеки гешування SHA-224, SHA-256, SHA-384, SHA-512, "Купина" (ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431) 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", прийнятий наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495);
- алгоритм "Калина" (ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484).

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

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

49. 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).

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

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

52. 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.

53. 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.

54. 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.

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

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

57. 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) (якщо банк не використовує криптографічний протокол захисту на транспортному рівні).

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

59. Банк зобов'язаний забезпечити наявність та актуальність такої документації до СКС:

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

2) схеми підключення обладнання СКС;

3) таблиці маркування кабелів СКС та кабельних з'єднань (кабельний журнал).

60. Банк зобов'язаний забезпечити персоналізований та контрольований доступ до комутаційних вузлів СКС.

61. 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:

1) вимог до безперервного забезпечення захисту від зловмисного коду;

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

3) 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;

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

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

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

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

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

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

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

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

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

2) усього вхідного Інтернет-трафіку;

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

65. 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.

66. 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.

67. 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.

68. Банк зобов'язаний зберігати електронні журнали роботи засобів захисту від зловмисного коду не менше ніж три місяці.

69. Банк зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість:

1) ідентифікації та автентифікації всіх користувачів операційної системи;

2) розмежування доступу користувачів операційної системи;

3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.

70. Банк зобов'язаний використовувати офіційні стабільні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.

71. Банк зобов'язаний визначити стандартне еталонне джерело часу та забезпечити синхронізацію з ним операційних систем.

72. 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 (якщо немає технічної можливості на рівні фунціоналу операційної системи) перейменувати такі вбудовані облікові записи та змінювати їх пароль не рідше ніж один раз на 30 діб.

73. 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 (за винятком робочих станцій або серверів, на яких блокування неможливе або потребує більшого інтервалу часу відсутності активності за технологією використання).

74. Банк зобов'язаний забезпечити централізоване розповсюдження налаштувань параметрів безпеки та інших параметрів конфігурації операційних систем (наприклад, за допомогою використання групових політик контролера домену "Active Directory").

75. Банк зобов'язаний створити та підтримувати в актуальному стані перелік програмного забезпечення, що використовується в банку (в електронному або паперовому вигляді).

76. Банк зобов'язаний забезпечити блокування можливості здійснення працівниками банку, яким не надано адміністративних прав у операційних системах, таких дій (налаштувань):

1) самостійного встановлення програмного забезпечення, яке не внесено до переліку програмного забезпечення, що використовується в банку;

2) автоматичного запуску програм із зовнішніх пристроїв та носіїв інформації;

3) самостійного видалення встановленого програмного забезпечення, оновлень безпеки.

77. Банк зобов'язаний розробити та затвердити внутрішні документи, які містять опис процесу управління оновленнями (описи дій щодо отримання, тестування, розповсюдження та застосування оновлень операційних систем, прикладного програмного забезпечення та драйверів). Процес управління оновленнями має містити такі стадії:

1) підготовка тестового середовища (тестових клієнтів);

2) підготовка переліку оновлень;

3) застосування оновлень в тестовому середовищі;

4) застосування оновлень на пілотній групі користувачів;

5) застосування протестованих оновлень.

78. 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).

79. 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.

80. Банк зобов'язаний забезпечити видалення/блокування неперсоналізованих і гостьових облікових записів користувачів СУБД та персоналізацію технологічних облікових записів СУБД.

81. Банк зобов'язаний забезпечити фізичне або віртуальне функціональне розділення серверів СУБД та серверів застосувань інформаційних систем банку.

82. Банк зобов'язаний розміщувати сервери баз даних в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

83. 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.

84. 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.

85. 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.

86. 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.

87. Банк зобов’язаний забезпечити використання виключно персоналізованих облікових записів для виконання адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів.

88. Банк зобов’язаний визначити та запровадити посилені вимоги щодо парольної політики для привілейованих облікових записів (довжина та складність паролів, частота зміни) або застосовувати багатофакторну автентифікацію для таких облікових записів.

89. Банк зобов’язаний забезпечити централізоване управління мережею банку (єдине місце управління). Банк має право здійснювати локальне управління мережею банку на різних вузлах за умови централізованого управління такими функціями:

1) вибір і монтаж кабельної системи мережі;

2) підбір комутаційного обладнання мережі;

3) підбір обладнання, що підключається до мережі банку, операційних систем, програмного забезпечення інформаційних систем банку, прикладного програмного забезпечення;

4) управління мережевими адресами та ідентифікаторами обладнання і користувачів;

5) розподіл мережі на сегменти.

90. Банк зобов’язаний забезпечити підтримання в актуальному стані документації мережі банку (в електронному та/або паперовому вигляді), 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:

1) фізичну схему мережі, уключаючи бездротові мережі, що відображає всі з'єднання в мережі;

2) логічну схему мережі, уключаючи бездротові мережі, що відображає всі мережеві пристрої, критично важливі сервери та сервіси;

3) конфігурацію мережевого обладнання, уключаючи бездротові мережі.

91. 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.

92. 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.

93. Банк зобов'язаний забезпечити ідентифікацію обладнання (наприклад, за ідентифікатором управління доступом до обладнання, MAC- адреса), що підключається до мережі банку, та вжиття заходів, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

94. Банк зобов'язаний забезпечити програмне відключення портів на активних мережевих пристроях мережі банку, які не використовуються.

95. Банку забороняється використовувати облікові записи та паролі за замовчуванням на активних мережевих пристроях, які підключені до мережі банку.

96. Банку забороняється використовувати протокол Інтернету версії 6 (IPv6) у мережі банку.

97. Банку забороняється використовувати версії 1 або 2 простого протоколу керування мережею (Simple network management protocol, SNMP) для управління пристроями в мережі.

98. Банк зобов'язаний забезпечити синхронізацію всіх активних мережевих пристроїв з еталонним джерелом часу банку.

99. Банк зобов'язаний розробити та впровадити заходи безпеки інформації у разі використання бездротових мереж передавання даних (далі –бездротові мережі).

100. Банк зобов'язаний розмістити бездротові мережі банку в окремій зоні безпеки мережі банку (сегмент або набір сегментів мережі зі спільним рівнем безпеки) та розмежувати доступ із зони безпеки бездротових мереж до мережі банку з використанням міжмережевих екранів.

101. 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 (окрім бездротової мережі, призначеної для гостьових підключень).

102. Банк зобов'язаний забезпечити використання в бездротових мережах банку режиму безпеки WPA2-Enterprise (корпоративний режим у наборі алгоритмів і протоколів Wireless protected access версії 2) та використання режиму безпеки WPA2-Personal (персональний режим у наборі алгоритмів і протоколів Wireless protected access версії 2) для реалізації гостьових підключень.

103. Банк зобов’язаний застосовувати такі заходи безпеки інформації для організації віддаленого доступу до інформаційних систем банку:

1) 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;

2) шифрування каналів зв’язку для доступу до сервера віддаленого доступу до інформаційних систем банку;

3) багатофакторна автентифікація користувачів.

104. Банк зобов’язаний забезпечити розмежування доступу між мережею банку і публічною мережею з використанням міжмережевих екранів та/або пристроїв уніфікованого управління загрозами.

105. 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.

106. Банк зобов’язаний забезпечити доступ з публічної мережі до мережі банку виключно із застосуванням захищених з’єднань.

107. 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.

108. Банк зобов’язаний виконувати перевірку ефективності заходів щодо захисту периметра мережі банку шляхом виконання періодичних тестів на проникнення.

109. 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).

110. У випадках отримання послуг електронного цифрового підпису від зареєстрованих центрів сертифікації ключів (далі – зареєстровані ЦСК) 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.

111. 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.

112. 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:

1) функцій та обов'язків персоналу банку стосовно підключення, технічного обслуговування та експлуатації систем та пристроїв зв'язку;

2) категорій інформації за критерієм конфіденційності, що може передаватися пристроями зв'язку;

3) обов'язковості очищення оперативної та постійної пам'яті факсимільних апаратів і багатофункціональних пристроїв перед передаванням їх третім сторонам або перед виведенням з експлуатації.

113. Банк зобов'язаний створити та підтримувати в актуальному стані перелік факсимільних апаратів і багатофункціональних пристроїв (в електронному або паперовому вигляді), який містить унікальні ідентифікатори обладнання та місце його розташування.

114. 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.

115. Банк зобов'язаний розміщувати обладнання телефонної мережі (сервери, комутаційне та абонентське обладнання) в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

116. Банк зобов'язаний запровадити такі заходи безпеки в разі використання телефонного зв'язку на основі протоколу Інтернет (IP-телефонії):

1) активувати вбудовані алгоритми шифрування трафіку між шлюзами, які забезпечують роботу телефонної системи банку, або між шлюзом та кінцевим абонентським обладнанням (телефоном);

2) здійснювати розподіл унікальних ідентифікаторів мережевого рівня (IP-адрес) у телефонній мережі банку відповідно до стандарту RFC 1918 "Розподіл адрес у приватних IP-мережах".

117. Банк зобов'язаний розробити та затвердити документ щодо використання електронної пошти, який має містити положення щодо:

1) обмежень під час пересилання інформації банку;

2) категорії інформації, яка може надсилатись засобами електронної пошти;

3) обмежень використання сторонніх сервісів електронної пошти, які не пов'язані з виконанням функціональних обов'язків персоналом банку.

118. Банк зобов'язаний розробити та впровадити заходи безпеки інформації для сервера електронної пошти, які включають:

1) додаткові заходи безпеки операційної системи, на якій встановлено сервер застосувань електронної пошти;

2) заходи безпеки сервера застосувань електронної пошти;

3) налаштування правил доступу до сервера електронної пошти.

119. Банк зобов'язаний забезпечити перевірку програмними або апаратними засобами захисту всіх повідомлень, що обробляються сервером застосувань електронної пошти, на наявність зловмисного коду.

120. Банк зобов’язаний впровадити періодичне тестування захищеності та перегляд налаштувань параметрів безпеки операційної системи сервера застосувань електронної пошти та безпосередньо сервера застосувань електронної пошти.

121. Банк зобов’язаний розміщувати сервер застосувань електронної пошти на окремому фізичному або віртуальному сервері.

122. У разі використання віддаленого доступу до сервера застосувань електронної пошти банк зобов’язаний запровадити такі заходи безпеки інформації:

1) 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;

2) доступ до сервера електронної пошти має надаватись лише шифрованими каналами зв’язку.

123. Банк зобов’язаний запровадити такі заходи безпеки інформації для сервера електронної пошти:

1) використовувати міжмережевий екран операційної системи сервера електронної пошти для обмеження доступу до сервера;

2) заблокувати отримання вхідних повідомлень від серверів мережі Інтернет, що розсилають спам;

3) 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.

124. Банк зобов’язаний визначити та задокументувати вимоги безпеки інформації для інформаційних систем банку під час їх розроблення, модернізації (у тому числі їх компонентів) або в разі придбання.

125. 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.

126. 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.

127. Банк зобов’язаний на стадії експлуатації інформаційних систем задокументувати положення щодо:

1) 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;

2) контролю вразливостей в обладнанні та програмному забезпеченні інформаційних систем банку;

3) контролю конфігурації програмного забезпечення інформаційних систем банку;

4) відновлення всіх реалізованих заходів щодо забезпечення безпеки інформації в інформаційних системах банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

128. 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.

129. 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.

130. Банк зобов'язаний упровадити процес управління інцидентами безпеки інформації та розробити і затвердити документи, які містять описи дій стосовно:

1) виявлення інцидентів;

2) інформування про інциденти, у тому числі відповідальної особи за інформаційну безпеку, підрозділу з безпеки інформації та працівників банку;

3) класифікації інцидентів та оцінки негативного впливу (збитку), нанесеного банку інцидентом;

4) реагування на інциденти;

5) аналізу причин, що призвели до інцидентів та оцінки результатів реагування на інциденти;

6) зберігання інформації щодо інцидентів, аналізу інцидентів та результатів реагування на інциденти.

131. 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.

132. Банк зобов'язаний забезпечити документування інформації щодо інцидентів безпеки інформації та її зберігання не менше ніж один рік.

Додаткові заходи безпеки інформації

133. Банку забороняється використовувати радіотелефони та/або радіоподовжувачі телефонної лінії без активованих у них алгоритмів шифрування сигналу, який передається радіоканалом.

134. Банк зобов'язаний створити та підтримувати в актуальному стані (в електронному або паперовому вигляді) перелік змінних носіїв інформації банку.

135. Банк зобов'язаний використовувати виключно ідентифіковані змінні носії інформації в інформаційних системах банку.

136. Банк зобов'язаний автоматизувати процес контролю за використанням змінних носіїв інформації в інформаційних системах банку. Банк має право самостійно визначати методи та засоби (технології) автоматизації такого процесу.

137. Банк зобов'язаний використовувати централізовані системи управління обліковими записами.

138. Банк зобов'язаний використовувати інструменти централізованого моніторингу та застосування оновлень безпеки для операційних систем.

139. Банк зобов'язаний автоматизувати процес управління інцидентами безпеки інформації. Банк має право самостійно визначати методи та засоби (технології) автоматизації такого процесу.

140. Банк зобов'язаний використовувати досконалу пряму секретність (Perfect forward secrecy, PFS) для з'єднань на основі протоколу захисту на транспортному рівні.

141. Банк зобов'язаний здійснювати маркування та документування елементів СКС відповідно до рекомендацій міжнародного стандарту ANSI/TIA/EIA-606.

142. Банк зобов'язаний застосовувати комбінацію програмних та програмно-апаратних засобів захисту від зловмисного коду (наприклад, використання програмних антивірусних засобів на робочих станціях і серверах та використання систем запобігання несанкціонованому доступу до мережі на зовнішньому периметрі мережі банку).

143. Банк зобов'язаний використовувати стандарти, документи та настанови відкритого проекту захисту веб-додатків "Open web application security project" (OWASP) для розроблення безпечних веб-додатків.

144. Банк зобов'язаний забезпечити шифрування каналів передавання даних між серверами СУБД і серверами застосувань або шифрування даних, що передаються між серверами СУБД і серверами застосувань банку.

145. Банк зобов'язаний здійснити функціональний розподіл серверів банку на мережевому рівні та забезпечити між ними мінімально необхідний зв'язок, що дозволить працювати серверам незалежно один від одного.

146. Банк зобов'язаний використовувати проміжний сервер для виконання функцій адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів. Підключення до такого сервера має здійснюватися з використанням непривілейованих облікових записів, а підключення з проміжного сервера до інформаційних систем банку, мережевого обладнання та серверів – із використанням привілейованих облікових записів.

Банк має право застосовувати альтернативні технології щодо управління та контролю доступом, які виключають прямий доступ привілейованих користувачів (адміністраторів) до інформаційних систем банку, мережевого обладнання та серверів.

147. Банк зобов'язаний використовувати механізми багатофакторної автентифікації під час надання доступу до САБ.

148. Банк зобов'язаний упровадити системи виявлення несанкціонованого доступу до мережі (Intrusion detection system, IDS) та системи запобігання несанкціонованому доступу до мережі (Intrusion prevention system, IPS) для захисту периметра мережі банку.

149. Банк зобов'язаний застосувати заходи безпеки для захисту від атак на відмову в обслуговуванні та/або розподілених атак на відмову в обслугову-

ванні (DoS/DDoS-атак) на зовнішньому периметрі мережі банку. Банк самостійно визначає методи та засоби (технології) захисту від такого типу атак.

150. Банк зобов’язаний використовувати сертифікати відкритих ключів, отримані в акредитованих/зареєстрованих ЦСК для ідентифікації та автентифікації, забезпечення конфіденційності інформації під час інформаційного обміну між інформаційними системами банку та Національного банку.

Лекція 10 Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи

(2 год.)

План лекції

1. Загальні положення
2. Вимоги до приміщень з обмеженим доступом
3. Вимоги до комутаційних кімнат
4. Вимоги до серверних приміщень і приміщень електронних архівів
5. Вимоги до екранованих приміщень
6. Вимоги до систем заземлення банків та систем захисту від пошкодження блискавкою
7. Вимоги до систем електроживлення банків
8. Рекомендації щодо побудови структурованих і локальних мереж

1. Загальні положення

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 (далі - приміщення електронних архівів).

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 (або зменшення такого впливу).

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 темпера-

туру повітря 18-24 град.С 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 (далі - екран), способи його з'єднання та кріплення до стін;
- конструкцію дверей;
- типи кабелів і комунікацій та способи їх уведення в екроване 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 (далі - двері).

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 (наприклад, з берилієвої бронзи) або сріблене чи луджене обплетення (з пружного матеріалу чи з гумовим джгутом усередині), які укладають на планку з корозостійкого матеріалу (наприклад, з нержавіючої сталі).

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 ripляться 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 (фільтри, систему вентиляції тощо).

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 (так звані хвилеподібні фільтри), 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 варюватися 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 (наприклад, STP, FTP, SFTP), 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 (крім інформаційних) увести 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 (трубопроводи, металеві конструкції будівлі тощо).

5.21. Провідник захисного заземлення в місці введення в екрановане приміщення зварюється по периметру з екраном. Провідник робочого заземлення, якщо воно ізольоване від захисного, потрібно вводити в екрановане 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 (установлення додаткових фільтрів, перерозведення провідників тощо).

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 (позисторів, розрядників);
- 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).

Лекція 11 Вимоги до захисту інформації при здійсненні переказів грошових коштів в Платіжній Системі Вестерн Юніон

(2 год.)

План лекції

1. Інформація, що підлягає захисту при здійсненні переказів грошових коштів
2. Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів
3. Способи виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів
4. Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації призначенні і розподілі ролей осіб, пов'язаних із здійсненням переказів грошових коштів
5. Склад 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
6. Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури
7. Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ
8. Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації з використанням технологічних заходів захисту інформації
9. Склад вимог до організації та функціонування служби інформаційної безпеки
10. Склад вимог до підвищення обізнаності в галузі забезпечення захисту інформації
11. Склад вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів
12. Склад вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів.

1. Інформація, що підлягає захисту при здійсненні переказів грошових коштів

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів застосовуються для забезпечення захисту такої інформації (далі – інформація, що захищається):

а) інформації про залишки коштів на банківських рахунках;

б) 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;

в) інформації, що міститься в оформлених в рамках застосовуваної форми безготівкових розрахунків розпорядженнях клієнтів Учасників (далі - клієнтів), розпорядженнях Учасників, розпорядженнях платіжного клірингового центру;

г) інформації про платіжні клірингових позиціях;

д) інформації, необхідної для посвідчення клієнтами права розпорядження грошовими коштами, в тому числі даних власників платіжних карт;

е) ключової інформації засобів криптографічного захисту інформації (далі - ЗКЗІ), використовуваних при здійсненні переказів грошових коштів (далі - криптографічні ключі);

ж) 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 (далі - об'єкти інформаційної інфраструктури), а також інформації про конфігурацію, яка визначає параметри роботи технічних засобів по захисту інформації;

з) 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.

2 Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів включають в себе:

а) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при призначенні і розподілі функціональних прав і обов'язків (далі – ролей) осіб, пов'язаних із здійсненням переказів грошових коштів;

б) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації (використання за призначенням, технічного обслуговування і ремонту), модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури;

в) 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;

г) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації від впливу про-

грамних кодів, що призводять до порушення штатного функціонування засобів обчислювальної техніки (далі - шкідливий код);

д) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при використанні інформаційно-телекомунікаційної мережі Інтернет (далі - мережа Інтернет) при здійсненні переказів грошових коштів;

е) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при використанні ЗКЗІ;

ж) 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 (далі - технологічні заходи захисту інформації);

з) вимоги до організації та функціонування підрозділу (працівників), відповідального (відповідальних) за організацію і контроль забезпечення захисту інформації (далі - служба інформаційної безпеки);

і) вимоги до підвищення обізнаності працівників Учасника, Агента (субагентів), який є юридичною особою, Оператора Послуг Платіжної Інфраструктури і клієнтів (далі - підвищення обізнаності) у сфері забезпечення захисту інформації;

к) вимоги до виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, і реагування на них;

л) вимоги до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів;

м) вимоги до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

н) 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;

о) вимоги до вдосконалення Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури захисту інформації при здійсненні переказів грошових коштів.

3. Способи виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів

Виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів забезпечується шляхом:

а) 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 організа-

ційних 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;

б) 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.

4. Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації призначенні і розподілі ролей осіб, пов'язаних із здійсненням переказів грошових коштів

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.

а) 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.

б) 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 (далі - електронні повідомлення).

в) 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.

г) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують контроль і реєстрацію дій осіб, яким призначено ролі, визначені в цьому пункті.

5. Склад 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

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.

а) 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.

б) 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.

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.

д) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують реалізацію заборони використання інформації, що захищається на стадії створення об'єктів інформаційної інфраструктури.

е) 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 Послуг Платіжної Інфраструктури;

- знищення інформації, що захищається, в тому числі міститься в архівах, способом, що забезпечує неможливість її відновлення.

6 Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури, включаються такі вимоги.

а) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують облік об'єктів інформаційної інфраструктури, які використовуються для обробки, зберігання та (або) передачі інформації, що захищається, в тому числі банкоматів і платіжних терміналів.

б) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують застосування некриптографічних засобів захисту інформації від несанкціонованого доступу, в тому числі пройшли в установленому порядку процедуру оцінки відповідності. Допускається застосування некриптографічних засобів захисту інформації від несанкціонованого доступу іноземного виробництва.

в) При здійсненні доступу до інформації, що захищається, що знаходиться на об'єктах інформаційної інфраструктури, зазначених вище, Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують:

- виконання процедур ідентифікації, аутентифікації, авторизації своїх працівників під час здійснення доступу до інформації, що захищається;
- ідентифікацію, аутентифікацію, авторизацію учасників платіжної системи при здійсненні переказів грошових коштів;
- визначення порядку використання інформації, необхідної для виконання аутентифікації;
- реєстрацію дій при здійсненні доступу своїх працівників до інформації, що захищається;
- реєстрацію дій, пов'язаних з призначенням та розподілом прав доступу до інформації, що захищається.

г) При здійсненні доступу до інформації, що захищається, яка знаходиться на об'єктах інформаційної інфраструктури, зазначених вище, Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують:

- виконання процедур ідентифікації, аутентифікації, авторизації осіб, які здійснюють доступ до програмного забезпечення банкоматів і платіжних терміналів;
- виконання процедур ідентифікації та контроль діяльності осіб, які здійснюють технічне обслуговування банкоматів та платіжних терміналів;

- реєстрацію дій клієнтів, які виконуються з використанням програмного забезпечення, що входить до складу об'єктів інформаційної інфраструктури та використовуваного для здійснення переказів грошових коштів (далі - програмне забезпечення), і автоматизованих систем, що входять до складу об'єктів інформаційної інфраструктури і використовуваних для здійснення переказів грошових коштів (далі - автоматизовані системи), при наявності технічної можливості;
- реєстрацію дій, пов'язаних з призначенням та розподілом прав клієнтів, наданих їм в автоматизованих системах і програмному забезпеченні, при наявності технічної можливості.

д) При здійсненні доступу до інформації, що захищається, яка знаходиться на об'єктах інформаційної інфраструктури, зазначених вище, Учасник забезпечує реєстрацію дій з інформацією про банківські рахунки, включаючи операції відкриття і закриття банківських рахунків.

е) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують:
- реалізацію заборони несанкціонованого розширення прав доступу до інформації, що захищається;
- призначення своїм працівникам мінімально необхідних для виконання їх функціональних обов'язків прав доступу до інформації, що захищається.

ж) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури приймають і фіксують у внутрішніх документах рішення про необхідність застосування організаційних заходів захисту інформації та (або) використання технічних засобів захисту інформації, призначених для:
- контролю фізичного доступу до об'єктів інформаційної інфраструктури (за винятком банкоматів і платіжних терміналів), збої і (або) відмови в роботі яких призводять до неможливості надання послуг з переказу грошових коштів або до несвоєчасності здійснення переказів грошових коштів, а також доступу до будівлі та приміщення, в яких вони розміщуються;
- запобігання фізичного впливу на засоби обчислювальної техніки, експлуатація яких забезпечуються Учасником, Агентом (субагентів), Оператором Послуг Платіжної Інфраструктури і які використовуються для здійснення переказів грошових коштів (далі - засоби обчислювальної техніки), і телекомунікаційне обладнання, експлуатація якого забезпечується Учасником, Агентом (субагентами), Оператором Послуг Платіжної Інфраструктури і яке використовується для здійснення переказів грошових коштів
- комунікаційне обладнання), збої і (або) відмови в роботі яких призводять до неможливості надання послуг з переказу грошових коштів або до несвоєчасності здійснення переказів грошових коштів, за винятком банкоматів і платіжних терміналів;
- реєстрації доступу до банкоматів, в тому числі з використанням систем відеоспостереження.

з) У разі прийняття Учасником, Агентом (субагентів), Оператором Послуг Платіжної Інфраструктури рішення про необхідність застосування організацій-

них заходів захисту інформації та (або) використання технічних засобів захисту інформації, зазначених вище, Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують застосування зазначених організаційних заходів захисту інформації та (або) використання технічних засобів захисту інформації, призначених для запобігання несанкціонованому доступу до інформації, що захищається шляхом використання вразливостей програмного забезпечення;

- зниження тяжкості наслідків від впливів на об'єкти інформаційної інфраструктури з метою створення умов для неможливості надання послуг з переказу грошових коштів або несвоєчасність здійснення переказів грошових коштів;
- фільтрацію мережевих пакетів при обміні інформацією між обчислювальними мережами, в яких розташовуються об'єкти інформаційної інфраструктури, і мережею Інтернет.

б) Учасник забезпечує формування для клієнтів рекомендацій щодо захисту інформації від несанкціонованого доступу шляхом використання неправдивих (фальсифікованих) ресурсів мережі Інтернет.

7. Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ

Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ здійснюється в наступному порядку.

а) 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.

б) 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.

в) 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.

г) Криптографічні ключі виготовляються клієнтом (самостійно), Оператором Послуг Платіжної Інфраструктури і (або) Учасником.

д) 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.

е) Оператор визначає необхідність використання СКЗІ, якщо інше не передбачено законами та іншими нормативними правовими актами України.

8 Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації з використанням технологічних заходів захисту інформації

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.

а) 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.

в) 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.

г) 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;
- аутентифікацію вхідних електронних повідомлень;
- взаємну (двосторонню) аутентифікацію 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.

9. Склад вимог до організації та функціонування служби інформаційної безпеки

До складу вимог до організації та функціонування служби інформаційної безпеки включаються такі вимоги.

а) Учасник, Агент (Субагент), який є юридичною особою, Оператор Послуг Платіжної Інфраструктури:

- забезпечують формування служби інформаційної безпеки, а також визначають у внутрішніх документах цілі і завдання діяльності цієї служби;
- надають повноваження і виділяють ресурси, необхідні для виконання службою інформаційної безпеки встановлених цілей і завдань.

б) Учасник, Оператор Послуг Платіжної Інфраструктури призначають куратора служби інформаційної безпеки зі складу свого органу управління і визначають його повноваження. При цьому служба інформаційної безпеки і служба інформатизації (автоматизації) не повинні мати загального куратора.

в) Учасник, який має філії:

- забезпечує формування служб інформаційної безпеки в зазначених філіях, визначає для них необхідні повноваження і виділяє необхідні ресурси;
- забезпечує взаємодію та координацію робіт служб інформаційної безпеки.
- г) Служба інформаційної безпеки здійснює планування і контроль забезпечення захисту інформації при здійсненні переказів грошових коштів, для чого наділяється такими повноваженнями:
- здійснювати контроль (моніторинг) виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;
- визначати вимоги до технічних засобів захисту інформації та організаційним заходам захисту інформації;
- контролювати виконання працівниками вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;
- брати участь в розглядах інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, і пропонувати застосування дисциплінарних стягнень, а також надсилати пропозиції щодо вдосконалення захисту інформації;
- брати участь в діях, пов'язаних з виконанням вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються при відновленні надання послуг платіжної системи після збоїв і відмов в роботі об'єктів інформаційної інфраструктури.

10. Склад вимог до підвищення обізнаності в галузі забезпечення захисту інформації

До складу вимог до підвищення обізнаності в галузі забезпечення захисту інформації включаються такі вимоги.

а) Учасник, Агент (Субагент), який є юридичною особою, Оператор Послуг Платіжної Інфраструктури забезпечують підвищення обізнаності працівників в сфері забезпечення захисту інформації:

- по порядку застосування організаційних заходів захисту інформації;
- по порядку використання технічних засобів захисту до забезпечення захисту інформації при здійсненні переказів грошових коштів.

б) Учасник і Оператор Послуг Платіжної Інфраструктури забезпечують виконання зазначених у цьому підпункті вимог.

в) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують:

застосування організаційних заходів захисту інформації та (або) використання технічних засобів захисту інформації, призначених для виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

- інформування служби інформаційної безпеки, в разі її наявності, про виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

- реагування на виявлені інциденти, пов'язані з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;
- аналіз причин виявлених інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, проведення оцінки результатів реагування на такі інциденти.

г) Оператор забезпечує облік і доступність для Учасників і Операторів Послуг Платіжної Інфраструктури, що залучаються для надання Послуг Платіжної Інфраструктури в Платіжної Системі Вестерн Юніон, інформації:

д) про виявлені в Платіжної Системі Вестерн Юніон інциденти, пов'язані з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

е) про методики аналізу і реагування на інциденти, пов'язані з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів.

11 Склад вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів

До складу вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів включаються такі вимоги.

а) Документи, що становлять порядок забезпечення захисту інформації при здійсненні переказів грошових коштів, визначають:

- склад і порядок застосування організаційних заходів захисту інформації;
- склад і порядок використання технічних засобів захисту інформації, включаючи інформацію про конфігурацію технічних засобів захисту інформації, що визначає параметри їх роботи;
- порядок реєстрації та зберігання інформації на паперових носіях і (або) в електронному вигляді, що містить підтвердження виконання порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації.

б) Оператор встановлює розподіл обов'язків щодо визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів шляхом:

- самостійного визначення Оператором порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;
- розподілу обов'язків щодо визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів між Оператором, Операторами Послуг Платіжної Інфраструктури і Учасниками;

в) Оператор, Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів в рамках розподілу обов'язків, встановлених оператором платіжної системи.

г) Для визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів Оператор, Учасник, Оператор Послуг Платіжної Інфраструктури в рамках обов'язків, встановлених Оператором, можуть використовувати:

- положення національних стандартів щодо захисту інформації, стандартів організацій, в тому числі стандартів НБУ, рекомендацій в галузі стандартизації, в тому числі рекомендацій НБУ, прийнятих відповідно до законодавства України про технічне регулювання;
- положення документів, визначених міжнародними платіжними системами;
- результати аналізу ризиків при забезпеченні захисту інформації при здійсненні переказів грошових коштів на основі моделей загроз і порушників безпеки інформації, визначених у національних стандартах щодо захисту інформації, стандартах організацій, в тому числі стандартах НБУ, прийнятих відповідно до законодавства України про технічне регулювання, або на основі моделей загроз і порушників безпеки інформації, визначених Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури.

д) Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів.

е) Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують призначення осіб, відповідальних за виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів.

ж) Служба інформаційної безпеки Учасника, Оператора Послуг Платіжної Інфраструктури здійснює контроль (моніторинг) виконання порядку забезпечення захисту інформації.

12 Склад вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів.

До складу вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів включаються такі вимоги.

а) Учасник, Оператор, Оператор Послуг Платіжної Інфраструктури забезпечують проведення оцінки виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів (далі - оцінка відповідності).

б) Оцінка відповідності здійснюється на основі:

інформації на паперовому носії та (або) в електронному вигляді, що містить підтвердження виконання порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації;

- аналізу відповідності порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації вимогам законодавства України;

- результатів контролю (моніторингу) виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів.

в) Оцінка відповідності здійснюється Учасником, Оператором, Оператором Послуг Платіжної Інфраструктури самостійно або із залученням сторонніх організацій.

г) Оператор, Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують проведення оцінки відповідності не рідше одного разу на два роки, а також на вимогу НБУ зі змінами, внесеними до законодавчих актів Російської Федерації, нормативні акти Банку Росії, що регулюють відносини в національну платіжну систему.

б) Учасник, Оператор Послуг Платіжної Інфраструктури регламентують порядок вжиття заходів, спрямованих на вдосконалення захисту інформації при здійсненні переказів грошових коштів, у випадках:

- зміни вимог до захисту інформації, визначених Правилами;
- змін, внесених до законодавчих актів України, нормативні акти НБУ, що регулюють відносини в національну платіжну систему;
- зміни порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;
- виявлення загроз, ризиків і вразливостей в забезпеченні захисту інформації при здійсненні переказів грошових коштів;
- виявлення недоліків при здійсненні контролю (моніторингу) виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;
- виявлення недоліків при проведенні оцінки відповідності.

в) Прийняття рішень Учасник, Оператора Послуг Платіжної Інфраструктури щодо вдосконалення захисту інформації при здійсненні переказів грошових коштів узгоджується зі службою інформаційної безпеки.

Лекція 12 Нормативно-правові акти з питань інформаційної безпеки в банках

(2 год)

План лекції

1. Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України

1. Положення про захист 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 http://yurist-online.org/ 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 (далі - Національний банк).

Організації взаємодіють за всіма поточними питаннями роботи із ЗЗІ з Департаментом інформаційної безпеки Національного банку України (далі- Департамент інформаційної безпеки) та отримують ЗЗІ в територіальних управліннях Національного банку України (далі - територіальні управління) 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 (далі - Правила).

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 (далі - Положення про порядок перевірки).

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 (далі - 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,

http://yurist-online.org/

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:

1) 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;

2) 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 (крім ВК для робочих місць операціоністів, що використовуються лише в САБ).

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.

http://yurist-online.org/

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:

1 АКЗІ (для безпосереднього учасника СЕП) 1

2 СК (для безпосереднього учасника СЕП) 2

3 ПМГК 1

4 Копія ПМГК 1

5 ТКАРМ-СЕП (для безпосереднього учасника СЕП) 1 + копія

6 ТК АРМ-НБУ-інф 1 + копія

7 ТК АРМ бухгалтера САБ (для безпосереднього учасника СЕП). За кількістю відповідальних осіб, але не більше 5

8 ТК технолога (для безпосереднього учасника СЕП). За кількістю відповідальних осіб, але не більше 5

9 ТК операціоністів (для безпосереднього учасника СЕП). За кількістю відповідальних осіб

10 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:

http://yurist-online.org/

- 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, що 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:

1) переходу на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку банку на іншу;

2) зміни місцезнаходження філії з однієї області України на іншу;

3) 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:

1) виготовляє ЗЗІ для цієї організації;

2) 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).

http://yurist-online.org/

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:

1) ліквідації;

2) 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;

3) виходу з ладу ЗЗІ;

4) 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

http://yurist-online.org/

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:

1) 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;

2) 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);

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. IV. 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 http://yurist-online.org/ документів. Наприкінці бан-

ківського дня журнали програмного та апаратного шифрування і протокол роботи 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:

1) ідентифікатор банку - учасника СЕП, який надіслав (зашифрував) електронний банківський документ;

2) ідентифікатор банку - учасника СЕП, якому адресовано електронний банківський документ;

3) дату, годину та хвилину виконання шифрування електронного банківського документа;

4) дату, годину та хвилину розшифрування електронного банківського документа;

5) відповідність усіх електронних цифрових підписів, якими був захищений від модифікації електронний банківський документ.

Під час використання АКЗІ додатково визначаються:

1) номер АКЗІ, на якій виконувалося шифрування або розшифрування електронного банківського документа;

2) 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:

1) невиконання автентифікації або розшифрування електронного банківського документа;

2) відмови від факту одержання електронного банківського документа;

3) відмови від факту формування та надсилання електронного банківського документа;

4) ствердження, що одержувачу надійшов електронний банківський документ, а насправді він не надсилався;

5) ствердження, що електронний банківський документ був сформований та надісланий, а він не формувався або було надіслане інше повідомлення;

6) виникнення спору щодо змісту одного й того самого електронного банківського документа, сформованого та надісланого відправником і одержаного та правильно автентифікованого одержувачем;

7) роботи з архівом роботи АРМ-СЕП під час проведення ревізій тощо.

http://yurist-online.org/

Департамент інформаційної безпеки надає учасникам СЕП письмові відповіді щодо порушених питань. V. 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:

1) виконання (спроби виконання) фіктивного платіжного документа;

2) компрометація ЗЗІ;

3) пошкодження ЗЗІ;

4) несанкціоноване проникнення в приміщення з АРМ-СЕП/АРМ-НБУ-інф (пошкодження вхідних дверей, ґрат на вікнах, спрацювання сигналізації за нез'ясованих обставин тощо);

5) проведення правоохоронними органами та іншими органами державної влади перевірки діяльності організації, унаслідок якої створюються умови для компрометації ЗЗІ;

6) 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 (особа, яка виконує його обов'язки);

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 і рекомендованих джерел.

1. Закони України

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
2. Закон України «Про Національний банк України» / Відомості Верховної Ради України (ВВР). – 1999. – № 29. – ст. 238.
3. Закон України "Про основи національної безпеки".
4. Закон України «Про доступ до публічної інформації».
5. Закон України «Про захист персональних даних».
6. Закон України «Про захист інформації в автоматизованих системах».
7. Закон України "Про електронні документи та електронний документообіг".
9. Закон України “Про електронний цифровий підпис” від 22.05.2003 р. № 852-IV. — ВВР. — 2003 . — № 36.
10. Закон України «Про банки і банківську діяльність» від 7 грудня 2000 року № 2121-III (із змінами та доповненнями).
11. Закон України «Про державну таємницю» // Відомості Верховної Ради (ВВР), 1994, № 16, ст.93 (із змінами та доповненнями).
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради (ВВР), 1994, № 31, ст.286 (із змінами та доповненнями).
13. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради (ВВР), 1994, № 31, ст.286 (із змінами та доповненнями).
14. Закон України «Про основні засади забезпечення кібербезпеки України», 2017 р.

2. Постанови Кабінету Міністрів України

1. Концепція ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.
2. ISO/IEC 27002. "Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью."
3. ISO/IEC 27005. "Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности.
4. ISOIEC 15408-1:2000 - Information technology - Security techniques - Evaluation criteria for IT sector - Introduction and general model.
5. ISOIEC 15408-1:2001 - Information technology - Security techniques - Evaluation criteria for IT sector - Security functional requirements.

6. ISOIEC 15408-1:2002 - Information technology - Security techniques - Evaluation criteria for IT sector - Security assurance requirements.
7. CEM-9717. Common Evaluation Methodology for Information Technology Security - Part 1: International general model.
8. ISOIEC 7498-2: 1999. - Information processing systems - Open Systems Interconnection - Basic Report - Part 2: Security Architecture.
9. Конвенція про кіберзлочинність // Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 (Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, № 5-6, ст.71).

3. Постанови НБУ

1. ПРАВЛІННЯ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ. ПОСТАНОВА. від 26 листопада 2015 року N 829 Про затвердження нормативно-правових актів з питань інформаційної безпеки
2. Правила оформлення Регламенту роботи центрів сертифікації ключів банків України (z1036-10), зареєстровані в Міністерстві юстиції України 04.11.2010 за N 1036/18331
3. - Правила реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України (z1035-10), зареєстровані в Міністерстві юстиції України 04.11.2010 за N 1035/18330.
4. . Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0095500-17.
5. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем // Постанова Національного банку України від 25.09.2007 р. № 348 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
6. Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 N 265 (z0857-04).
7. Положення про застосування Національним банком України заходів впливу за порушення банківського законодавства // Постанова Національного банку України від 28.08.2001 р. № 369 зі змінами та доповненняші 7 [Етектрон. ресурс]. — Режим доступу: www.rada.kiev.ua.
8. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0095500-17.
9. Положення про порядок формування, зберігання та знищення електронних архівів у Національному банку України і банках України, затверджене постановою Правління Національного банку України від 12.09.2006 N

357 (z1089-06), зареєстроване в Міністерстві юстиції України 03.10.2006 за N 1089/12963.
10. Постанова Правління Національного банку України "Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України" від 17.06.2010 N 284 (z1034-10), зареєстрована в Міністерстві юстиції України 04.11.2010 за N 1034/18329.
11. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджені постановою Правління Національного банку України від 02.04.2007 N 112 (z0419-07), зареєстровані в Міністерстві юстиції України 24.04.2007 за N 419/13686.
12. Правління Національного банку України. Постанова 04 грудня 2017 року м. Київ № 124. Про затвердження Змін до Правил зберігання, захисту, використання та розкрит-тя банківської таємниці.
13. Правління Національного банку України. Постанова 26.11.2015 № 829. Про затвердження нормативно-правових актів з питань інформаційної безпеки.
14. ПРАВЛІННЯ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ. П О С Т А Н О В А. 04.07.2007 N 243. Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи
15. Правління Національного банку України. П О С Т А Н О В А. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України
16. Правління Національного банку України. Постанова 10 лютого 2016 року м. Київ № 63. Про затвердження Правил з організації захисту приміщень банків в Україні
17. Рекомендації Національного банку України держателям платіжних карток [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua/doccatalog/document?id=70904.
18. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Стандарт організації України. Настанова методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). Київ. національний банк України.2010
19. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Стандарт організації України. Настанова методи захисту в банківській діяльності. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD). банк України. . 2010

4. Укази президента України

1. Указ Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про

Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/962016-19836.

Базова

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с.
2. *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.
3. *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.
4. *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.
5. *Конахович Г.Ф. и др.* Защита информации в телекоммуникационных системах.-К. «МК-Пресс», 2005. - 288 с.

Допоміжна

6. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
7. Бондаренко М. Ф. Визначення та обґрун¬тування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін.// Радиотехника. – 2003. – № 134. – С. 9-25.
8. Бузов О.О. Защита информации от утечки по техническим каналам. Учебное пособие. М.: Гостехкомисия Росии, 2005. - 435 с.
9. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною без¬пекою / В. В. Домарєв, Д. В. Домарєв, С. Б Горді¬єнко. // Вісник Державного університету інформа¬ційно-комунікаційних технологій. – 2012. – Т. 10, № 2. – С. 102-104.
10. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
11. Зубок М. І. Безпека банківської діяльності: навч. посібник / Зубок . І. — К. : КНЕУ, 2002. — 190 с.
12. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник.-К. ДУІКТ, 2010. - 316 с.
13. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. – К: Арий, 2008, т. 1, 2 - 806 с.
14. Литвиненко В.К. Охрана, сопровождение грузов, денежных средств и ценных бумаг. М.: Арсин, 2001. – 76с.

15. Лужецький В.А. Захист персональних даних. Навчальний посібник./ Лужецький В.А., Войтович О.П., Дудатьєв А.В – Вінниця: ВНТУ, 2009. – 487 с.
16. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-СУМ-Вінниця, 2009. – 240 с.
17. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник – СПб.: Питер, 2002.
18. Минаев Г. А. Безопасность организации : учебник / Минаев Г. А. — :КНТ,2009. — 440
19. Настанови з кібербезпеки від експертів [Електронний ресурс]. – Режим доступу: http://www.isaca.org.ua/ index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity
20. Основні функції структурних підрозділів центрального апарату НБУ [Електронний ресурс]. – Режим доступу : https://bank.gov.ua/doccatalog/document?id=24604231.
21. Петренко С.А. Политики информационной безопасности / С.А. Петренко, В. А. Курбатов. – М.: Компания АйТи. 2006. – 400 с.
22. 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.
23. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002.
24. Хорев А.А. Техническая защита информации: учеб. Пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ "Аналитика", 2008. – 436 с.
25. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
26. 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.
27. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. — К. : НАУ, 2011. — 640 с.
28. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ “НВП”ІНТЕРСЕРВІС”, 2009. – 716 с.
29. Потій О.В., Горбенко Ю.І. Визначення та обґрунтування суті політики інформаційної безпеки // http://www.security.ukrnet.net/ modules/sections/ index.php?op=viewarticle&artid=95
30. Банківський менеджмент: Підручник/ За ред. О.А. Кириченка, В.І. Міщенка. — К.: Знання, 2005. — 831 с.