РЕФЕРАТ

Атестаційна робота складається зі вступу, чотирьох розділів, загального висновку, переліку посилань і має 60 сторінки основного тексту, 8 рисунків. Список посилань містить 20 найменувань і займає 2 сторінки. **Загальний обсяг роботи 64 сторінок**.

Об'єктом дослідження є рівні захисту інформації банківських системах

Мета дослідження: Побудова багаторівневої системи захисту інформації яка відповідає сучасним вимогам і стандартам.

Під час виконання роботи я прийшов до висновку, що побудова систем захисту інформації потребує покращення існуючих методів шляхом оновленням. Слід розуміти, що без знання та кваліфікованого застосування сучасних технологій, стандартів, протоколів і засобів захисту інформації неможливо досягти необхідного рівня інформаційної безпеки комп'ютерних систем.

Предметом дослідження є розробка рекомендацій для оптимізації роботи систем захисту інформації в банківських системах та на об’єктах інформаційної діяльності.

Галузь застосування. Організації та підприємства.

Ключові слова: Безпека, інформація, банківські системи.

ЗМІСТ

Стор.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

БС — банківські системи

ОДІ — об’єкт інформаційної діяльності

АС — автоматизована система

ЗЛ — зловмисник

ТЗІ — технічний захист інформації

СЕП — система електронних платежів

АРМ — автоматизовані робочі місця

ІзОД — інформація з обмеженим доступом

ТЕО — техніко-економічні обґрунтування

ПЗАТЛ — пристрій захисту аналогових телефонних ліній

ПЕМВН — побічні електромагнітні випромінювання і наводи

ЛЗАР — лазерні засоби акустичної розвідки

ВСТУП

Захист інформації має величезне значення у повсякденному житті, тим більше в банківських системах (БС) та на об’єктах інформаційної діяльності (ОІД). Сучасні інформаційні системи мають складну структуру. Вони містять додатки, що працюють у взаємодії з різними операційними системами, встановленими на комп'ютерах, об'єднаних в локальну мережу, часто пов'язану тим чи іншим чином з сегментом глобальної мережі. Забезпечення безпеки такої системи вимагає проведення цілого комплексу заходів відповідно до розробленої на підприємстві політикою інформаційної безпеки. В БС фінансові дані являють собою найбільш бажану ціль для кіберзлочинців. Дані які використовують фінансові установи для отримання грошового прибутку мають особливе значення тому банківські установи завжди знаходяться під загрозою кібернетичних атак.

Для захисту важливих об’єктів є необхідним створення комплексу інженерно-технічних засобів охорони. Особливо важливим є аналіз вразливості ОІД, предмет захисту, загрози безпеки та оцінювання можливої шкоди. Необхідний комплексний науковий підхід до створення систем захисту та мати різні варіанти побудови комплексу інженерно-технічних засобів охорони з оцінкою її вартості. Такий підхід допоможе уникнути більшість помилок та зменшити витрати.

Для забезпечення ефективного захисту необхідно використовувати комплекс програмних та апаратних засобів. Необхідні роботи с персоналом такі як контроль відвідуваних сайтів і якими додатками користуються співробітники організації. Також необхідні курси для безпечної роботи в інтернеті, інформування про можливі загрози.

Таким чином, створення ефективного комплексу захисту інформації в БС та на ОІД потребую проведення аналізу вразливостей на стадії проектування і повинна базуватися на науковому підході. Захист інформації та інформаційна безпека повинні бути на високому для запобіганню атак. Без знання та

кваліфікованого застосування сучасних технологій, стандартів, протоколів і засобів захисту інформації неможливо досягти необхідного рівня інформаційної безпеки комп'ютерних систем і мереж.

Метою роботи було на практиці аналізувати загрози, причини їх виникнення та створення комплексної програми захисту для ТВБВ №10003/0467 АТ «Ощадбанк».

РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА БАНКІВСЬКИХ СИСТЕМАХ

1.1 Система технічного захисту інформації

В наш сучасний інформаційний час викрадення інформації, яка становить чи державну, конфіденційну чи будь-яку іншу, передбачену законом, таємницю. становить реальну загрозу безпеці України.

Які саме загрози можуть спричинити шкоду? В банківських системах (БС) серед таких можна виділити несанкціонований доступ до інформації, а також технічні інформаційні канали з яких може бути витік інформації.

В Україні існує система технічного захисту інформації, яка дозволяє протидіяти загрозам викрадення інформації в БС.

"Система являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Функції органу державного управління у сфері технічного захисту інформації виконує Департамент спеціальних систем та захисту інформації Служби безпеки України, який реалізує державну політику, здійснює управління захистом інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, а також державний контроль за функціонуванням системи технічного захисту інформації.

На відомчому рівні в центральних органах виконавчої влади, інших державних органах, підпорядкованих ним підприємствах, установах та організаціях створюються або визначаються підрозділи, на які покладаються завдання із забезпечення технічного захисту інформації." [1]

Системи технічного захисту інформації виконує свою роботу разом з необхідними гарантіями які відповідають рівням захищеності інформації в нормативних документах. Якісну роботу з побудови технічного захисту інформації досягається залученням спеціалістів з відповідною фаховою підготовкою та з досвідом роботи разом з спеціальним технічним оснащенням.

"З урахуванням зазначеного та відповідно до “Положення про технічний захист інформації в Україні”, затвердженого Указом Президента України від 27 вересня 1999 року №1229, для здійснення розроблення, впровадження, атестації та експлуатації комплексів (систем) технічного захисту інформації необхідно отримати відповідні дозволи або ліцензії.

Суб’єкти господарської діяльності отримують ліцензію відповідно до Закону України “Про ліцензування певних видів господарської діяльності” та затверджених Ліцензійних умов." [1]

ТЗІ має державний контроль який здійснюється за допомогою організації контрольно-інспекторської роботи та її проведення, які визначають питання до технічного захисту інформації.

"Контрольно-інспекторська робота з питань ТЗІ включає планування, проведення інспекційних перевірок стану технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, аналіз їх результатів та надання рекомендацій щодо вдосконалення стану технічного захисту інформації у зазначених органах." [2]

Степанов Володимир Дмитрович начальник Головного управління технічного захисту інформації ДСТСЗІ СБ України надає у своїй роботі як підвищити ефективність технічного захисту інформації.

"Серед напрямків підвищення ефективності технічного захисту інформації в державних органах Департаментом вбачається:

- створення дієво здатних підрозділів технічного захисту інформації та укомплектування їх фахівцями з відповідною підготовкою;

- розробка та впровадження відомчих нормативно-правових актів з питань технічного захисту інформації;

- визначення доцільності отримання дозволу на право провадження робіт з технічного захисту інформації для власних потреб залежно від обсягів робіт з захисту інформації та економічної доцільності;

- розробка органами, які мають дозвіл на право провадження робіт з технічного захисту інформації для власних потреб, та погодження з Департаментом документів, які дозволяють оптимізувати проведення робіт з захисту інформації в інформаційно-телекомунікаційних системах, в тому числі роботи з оцінки захищеності інформації." [1]

1.2 Порядок створення комплексів технічного захисту інформації в банківських системах та на об’єктах інформаційної діяльності

Технічний захист інформації є системою забезпечення національної безпеки України яка стосується інформаційної сфери та виконує свої функції за допомоги інженерно-технічних заходів. Вони виконують роботу для забезпечення цілісності, доступності, конфіденційності в автоматизованих системах які знаходитсья на об'єктах інформаційної діяльності.

"На конкретних об’єктах інформаційної діяльності (ОІД) створюються комплекси ТЗІ - комплекси захисту інформації з обмеженим доступом (ІзОД) від витоку по технічних каналах.

При створенні комплексів ТЗІ досліджуються й аналізуються елементи ОІД, що можуть впливати на показники ефективності ТЗІ.

Суб’єктами створення комплексу захисту можуть бути:

– установа, яка є замовником створення комплексу захисту (далі - замовник або установа-замовник);

– структурний підрозділ установи, що обґрунтовує необхідність і заявляє створення комплексу захисту (далі – заявник);

– фахівець (фахівці), підрозділ, якому доручено організацію і супроводження робіт з ТЗІ в установі;

суб'єкти господарської діяльності, що мають відповідні ліцензії на провадження діяльності у галузі ТЗІ." [1]

Для створення комплексу захисту інформації необхідно виконати деякі умови.

"Основою для створення комплексу захисту є рішення керівника установи-замовника щодо:

– надання споруді, де планується це створення, статусу ОІД, та призначення відповідальної особи для організації, супроводження та координації робіт на всіх етапах цього створення;

– обов'язкового оформлення результатів створення комплексу згідно з встановленим порядком;

– затвердження програми для проведення обстеження ОІД (відповідно до п.4.2 ДСТУ 3396.1) та термінів виконання інших робіт з ТЗІ.

При цьому враховуються:

– пропозиції від заявників щодо організації створення комплексів захисту;

– відомості про діючі ОІД та створені в установі комплекси захисту;

– перспективу подальших робіт з ТЗІ в установі;

технічні та економічні можливості установи щодо впровадження інженерно-технічних заходів з ТЗІ." [1]

Створення комплексів технічного захисту інформації являє собою сукупність дій які пов’язані між собою логічною цілю забезпечення оптимальних рішень для забезпечення захисту інформації.

"Створення комплексів ТЗІ це:

1. Процес, пов'язаний з вивченням, дослідженням, конструктивними змінами і т.п. об'єкта, його елементів, оточення, що можуть бути можливим

середовищем поширення носіїв ІзОД (складові частини технічних каналів витоку інформації).

2. Збір вихідних даних та оформлення (узгодження й затвердження) необхідних документів:

– протоколів, актів досліджень, вимірів технічних засобів, розпоряджень на експлуатацію технічних засобів, призначених для оброблення ІзОД;

– переліку загроз для безпеки ІзОД (модель загроз);

– результатів категорування на ОІД;

– технічних завдань на розробку і впровадження заходів для ТЗІ і т.п.

3. Прийняття рішень з ТЗІ, їх реалізація й оформлення (узгодження чи затвердження) необхідної документації, а саме:

– техніко-економічних обґрунтувань (ТЕО), проектно-кошторисної,

– робочої, конструкторської, іншої документації;

– програми і методики приймальних і атестаційних випробувань;

– протоколів випробувань;

– актів приймання й атестації комплексу.

4. Оформлення документації для введення в експлуатацію ОІД з урахуванням вимог з ТЗІ:

– технічного паспорта на комплекс ТЗІ і паспорта на кожне приміщення ОІД;

– наказів, розпоряджень (на підставі позитивних результатів атестації), що дозволяють обробляти чи озвучувати, працювати з ІзОД (для АС готують окремі дозвільні документи);" [1]

Комплекс ТЗІ створюється при ремонті, розширенні, будівництва нової інженерно-технічної споруди де діяльність пов’язана з інформацією з обмеженим доступом під час створення автоматизованих систем.

"При будівництві ОІД повинні бути впроваджені відповідні організаційні та інженерно-технічні заходи для таких видів ІзОД:

– мовної ІзОД, яка озвучується в приміщеннях ОІД, де можливе проведення нарад, показів із звуковим супроводженням кіно- і відеофільмів тощо, а також у приміщеннях, де встановлені кінцеві пристрої систем спеціального зв’язку, засоби обчислювальної техніки тощо;

– ІзОД, яка обробляється на ОІД технічними засобами (формування, збирання, введення, записування, накопичення, підсилення, перетворення, відтворення, зчитування, зберігання, копіювання, множення, знищення, реєстрація, приймання, отримання, передавання, відображення тощо);

– виробничої ІзОД, що має місце при виробництві й експлуатації продукції спеціального призначення.

Організаційні та інженерно-технічні заходи, що застосовуються при створенні комплексу захисту на ОІД, повинні відповідати вимогам нормативних документів з питань ТЗІ та містять:

– архітектурно-будівельні заходи захисту;

– інженерно-технічні заходи пасивного захисту інформації (оптичне, акустичне, електромагнітне, радіаційне екранування, технічні засоби із захистом, спеціальні засоби захисту інформації в телефонних та інших проводових лініях тощо);

– технічні заходи активного захисту інформації (генератори віброакустичного, просторового акустичного та електромагнітного зашумлення, лінійного електромагнітного зашумлення);" [1]

1.3 Охорона об’єктів та її принципи. Охороні системи

Для якісної охорони об’єкта ми повинні визначити принципи щодо охорони цих самих об’єктів.

"Принципи, що визначають загальні вимоги до засобів охорони об’єктів (способів та засобів захисту інформації):

1. безперервність охорони об’єктів (захисту інформації) характеризує постійну готовність системи і засобів охорони об’єктів до відбиття загрози несанкціонованого доступу на об’єкти (до інформації);

2. активність перодбачає прогнозування дій зловмисника, розробку і реалізацію випереджаючих заходів охорони (захисту);

3. скритність виключає ознайомлення сторонніх осіб з засобами і техннологією охорони об’єктів (захисту інформації);

4. цілеспрямованість передбачає зосередження зусиль по запобіганню загрозам найбільш важливим об’єктам (найбілш цінній інформації);

комплексність використання засобів охорони об’єктів, що дозволяє компенсувати недоліки одних засобів достоїнствами іншими." [3]

Процес створення проекту системи забезпечення безпеки ОІД складається з обстеження об’єкта, проектування і впровадження. Необхідні роботи з монтажем устаткування, навчання персоналу, прокладка кабельних мереж, організаційне забезпечення роботи системи включаються до проекту.

"Як правило, системи безпеки комплектуються з устаткування різних підприємств і фірм, проектування і монтаж можуть проводитися також різними організаціями, тобто відповідальність за працездатність та надійність усієї системи розподіляється між проектувальниками, виробниками та монтажниками. Тому дуже важливо для користувача правильно орієнтуватися на сучасному ринку пропонованих послуг із забезпечення безпеки фізичних об’єктів. Об’єкт, що охороняється, може являти собою:

- комплекс будинків, будівель, споруд, відкритих майданчиків з матеріальними цінностями, розташований на одній загальній охоронюваній території;
- окремі будинки, будівлі, споруди, відкриті майданчики з матеріальними цінностями;
- одне чи кілька приміщень, розташованих у будинку, будівлі, споруді з матеріальними цінностями." [4]

Сукупність організаційних заходів з інженерно-технічним оснащенням являє собою систему охорони. Існує два аспекти:

- активний (стосується людини);
- пасивний (стосується технічних засобів);

Ці аспекти необхідні щоб впіймати порушника на місці злочину, а саме для виявлення небезпечних дій злочинця та для передавання важливої інформації службі, яка затримає злодія.

Використання електронних технічних засобів у системах охоронної сигналізації є необхідністю. Оскільки отримати сигнал про порушення краще ніж недотримувати нічого. Але бідь-яка система залежніть від людей. Про це не слід забувати. Тому при впровадженні системи охорони об’єктів мі розглянемо принципи побудови охорони за допомогою технічних засобів.

"Охорона об’єктів здійснюється по периметру території (зовнішня периметрова) та всередині (внутріоб’єктна). Крім того, система охорони об’єктів повинна передбачати використання індивідуальних засобів захисту, що забезпечують безпеку фізичних осіб, які зайняті в сфері охорони об’єкта і можуть піддаватися нападу ЗЛ.

Першою перешкодою на шляху ЗЛ, що зменшує фактор ризику, є інженерні засоби охорони. Крім функцій фізичної перешкоди, інженерні засоби охорони виконують функції психологічної перешкоди, попереджаючи можливість здійснення порушення. Крім того, фізичні бар’єри збільшують час, необхідний ЗЛ для їх подолання, що робить більш імовірною можливість його затримки." [4]

"Інженерні засоби призначаються для: Утруднення дій ЗЛ при проникненні на об'єкт чи з об'єкта;

- Полегшення працівникам охорони виявлення слідів і затримки ЗЛ; індуктивні датчики;
- Створення працівника охорони необхідних умов для виконання завдань щодо охорони об’єкта;

Позначення меж постів і заборонених зон об’єктів;" [5]

"Усередині об'єктів технічними засобами охорони блокуються:

- різні конструктивні елементи будинків (вікна, двері, ворота, підлоги, стіни, світлові ліхтарі, перегородки, люки, виходи на дахи і т. д.);
- обсяг чи частина обсягу приміщення, підходів і проходів, коридори і сходові клітки;
- різні трубопроводи, сходи, елементи конструкцій козлових кранів, люки та ін., що дозволяють проникнути в охоронюване приміщення;
- сейфи, стенди, стелажі, технологічне устаткування, окремі предмети;
- місця стоянки чи збереження виробів." [4]

З інформації яка подана вище ми розуміємо, що маємо декілька рубежів, а саме перший який являє собою систему датчиків, які розташовані у дверях, вікнах и т.п. цей рубіж можемо назвати охоронний. Він необхідний блокування доступу на ОІД порушників. Другий це система сигналізації, яка використовується, як для блокування ОІД так і для блокування сейфів, предметів, окремих ділянок приміщення.

"При розробленні чи удосконалюванні системи охорони треба пам'ятати, що правильний вибір технічних засобів, правильно спроектована система визначають ступінь надійності охорони об'єкта." [4] При цьому необхідно враховувати ряд факторів, таких як:

- режимність підприємства;
- конструктивні особливості будинків, споруд;
- час реагування працівників охорони;
- рельєф і кліматичні умови;
- рівень шумів, радіо- і електроперешкод;
- створення працівникам охорони необхідних умов для виконання завдань щодо охорони об'єкта;
- позначення меж постів і заборонних зон об'єктів.

До периметрових інженерних засобів охорони належать:

- основне огородження;
- огородження заборонної зони;
- контрольно-слідова смуга;
- дорога охорони і стежка нарядів;
- дротові загородження;
- спостережні вишки, постові грибки, постові будки; вказівні, попереджувальні і розмежувальні знаки; окопи й укриття;
- устаткування постів вартових собак.

До електронних технічних засобів охорони належать:

- засоби виявлення ЗЛ;
- засоби виявлення пожежі;
- засоби оперативного зв'язку та оповіщення;
- засоби спостереження та телеконтролю;
- засоби забезпечення пропускного режиму;
- електроживленні установки;
- охоронне освітлення;
- лінії зв'язку (сполучні і живильні);

Технічні засоби охорони повинні забезпечувати:

- своєчасну подачу сигналу тривоги у вартове приміщення;
- при спробі порушників проникнути на охороняєму територію, в будинок чи приміщення із вказівкою місця, часу порушення (пожежі), а також напрямку руху порушника, включення сирени, дзвінків, гучномовного зв"язку з метою змусити порушника відмовитися від своїх намірів;
- отримання достовірної інформації про стан охороняємого об'єкту без виходу на місце особового складу охорони;
- двосторонній зв'язок аварти з постами для керування нарядами охорони;

- автоматизацію і механізацію контрольно-пропускного режиму;
- подачі сигналу про виникнення пожежі;
- ведення охорони об”єкта мінімальною кількістю людей;
- забезпечення особистої безпеки і поліпшення умов праці особовому складу варти.

В залежності від цілей існують різні види підготовки технічних засобів охорони, вони можуть буті одно рубіжні чи багато рубіжні системи охорони, тобто охоронно-пожежні сигналізації. “Охоронно-пожежні сигналізації“ мають на увазі передачу, отримання та обробку інформації про об’єкт (проникнення та пожежу) завдяки технічним засобам. Кожен випадок створення системи є унікальним і потребую визначення необхідних типів технічних засобів в залежності від категорії об’єкта .

"Підприємства, що працюють з відомостями, що становлять державну таємницю, іншою інформацією з обмеженим доступом, широко використовують при організації та забезпеченні охорони території та об'єктів різні засоби фізичного захисту.

Під фізичним захистом розуміється сукупність організаційних заходів, інженерно-технічних засобів і дій підрозділів охорони з метою запобігання диверсій чи розкрадань носіїв конфіденційної інформації та інших матеріальних засобів на об'єктах, що охороняються. Застосування засобів фізичного захисту значно підвищує ефективність функціонування системи охорони підприємства в цілому, а з урахуванням специфіки розташування деяких об'єктів підприємства та виконуваних ними завдань, практично гарантує досягнення головних цілей і вирішення основних завдань охорони підприємства. При розгляді основних підходів до фізичного захисту об'єктів підприємства та принципів її організації, а також при застосуванні засобів фізичного захисту використовуються такі терміни та поняття:

– допуск — дозвіл на проведення певної роботи або на отримання певних документів і відомостей;

- доступ — прохід (проїзд) в охоронювані зони об'єкта підприємства;
- захищена зона — територія об'єкта підприємства, яка оточена фізичними бар'єрами, постійно перебувають під охороною і наглядом, і доступ до якої обмежується і контролюється;
- порушник — особа, яка вчинила або намагається вчинити несанкціоновану дію, а також особа, яка надає йому сприяння в цьому;
- несанкціонована дія — розкрадання або спроба розкрадання носіїв конфіденційної інформації та матеріальних засобів підприємства, здійснення або спроба здійснення несанкціонованого доступу, пронесення (провезення) заборонених предметів, вчинення диверсії, виведення з ладу засобів фізичного захисту;
- несанкціонований доступ — проникнення осіб, які не мають права доступу в охоронювані зони, на об'єкти, в службові приміщення підприємства;
- виявлення — встановлення факту несанкціонованої дії;
- периметр — межа зони, що охороняється, обладнана фізичними бар'єрами та контрольно-пропускними пунктами;
- підрозділ охорони — озброєний підрозділ, що виконує завдання по охороні і обороні об'єктів підприємства;
- система охоронної сигналізації — сукупність засобів виявлення, тривожно-викличної сигналізації, системи збору, відображення та обробки інформації;
- технічний засіб виявлення — пристрій, призначений для автоматичної подачі сигналу тривоги у випадку несанкціоновані дії;
- фізичний бар'єр — фізична перешкода, що утрудняє проникнення порушника в охоронювані зони." [4]

З цього ми робимо висновок, що завданням фізичного захисту є:

- Попередження несанкціонованого доступу;
- Уповільнення проникнення порушника;

- Затримка порушників які проникло на об’єкт;

Планування організаційних заходів та контроль за їх виконанням здійснює служба безпеки разом із керівництвом. Вони створюють необхідні нормативні, методичні та плануючі документи та слідкують за їх виконанням. Це складає основу систем фізичного захисту.

1.4 Підзахисні зони безпеки їх розбиття в банківських системах та на об’єктах інформаційної діяльності

При розбитті на зони та присвоєння категорію доступу до них ми впроваджуємо необхідні умови захисту.

"Типовими зонами є:

- територія, яку займає організація і що обмежується огорожею або умовним зовнішнім кордоном;
- будівля на території;
- кордон або його частина;
- приміщення (службове, кабінет, і т.і.);
- шафа, сейф, сховище.

Кожна зона характеризується рівнем безпеки інформації, що знаходиться в ній. Безпека інформації в зоні залежить від:

1) відстані від джерела інформації (сигналу) до порушника або його засобу добування інформації;

2) кількості і рівня захисту рубежів на шляху руху порушника або поширення іншого носія інформації (наприклад, поля);

3) ефективності способів і засобів управління допуском людей і автотранспорту в зону;

заходів захисту інформації всередині зони." [5]

Варіант класифікації зон по ступеню захищеності наведений в таблиці 1.1

Таблиця 1.1

Категорія зон	Найменування зон	Функціональне призначення зон	Умови доступу співробітників	Умови доступу відвідувачів
0	Вільна	Місця вільного відвідування	Вільний	Вільний
I	Зона, що спостерігається	Кімнати прийому відвідув.	Вільний	Вільний
II	Реєстраційна	Кабінети співробітників	Вільний	З реєстрацією за посвідченням особи
III	Режимна	Секретаріат, комп'ютерні зали, архіви	За ідентифікаційні. картами	За разовими перепустками
IV	Посиленого захисту	Касові операційні зали, матеріальні склади	За спец документами	За спец. перепустками
V	Вищого захисту	Кабінети керівників, спеціальні сховища	За спец. документами	За спец. перепустками

"Безпека інформації в і-й зоні оцінюється імовірністю $Q_i(\tau)$ забезпечення заданого рівня безпеки інформації протягом певного часу. Для незалежних зон значення цих імовірностей незалежні, для вкладених - $Q_1(\tau)<Q_2(\tau)<Q_3(\tau)<...<Q_5(\tau)$ ($Q_1 \ldots Q_5$ – імовірності забезпечення заданого рівня безпеки інформації відповідно для території, будівлі, поверху, приміщення і сейфа). Якщо безпека інформації в кожній зоні забезпечується тільки рубежем на її кордоні, то для доступу ЗЛ, наприклад, до документа, що зберігається в сейфі, йому необхідно подолати 5 рубежів: кордон території, увійти в будівлю, в коридор потрібного поверху, в приміщення і відкрити сейф. В цьому випадку безпека інформації в к-ій зоні $Q_к$ оцінюється величиною:

$$Q_k(\tau_k) = 1 - \prod_{i=1}^{k} P_i(\tau_i), \text{ а } \tau_k = \sum_{i=1}^{k} \tau_i , \qquad (1.1)$$

де $P_i(\tau_i)$ – імовірність подолання порушником і-го рубежа за час τ_i .

Наприклад, якщо для всій і-ва імовірність $P_i = 0{,}2$ за час $\tau_i = 5$ хвилин, то $Q_5 = 0{,}99968$ забезпечується протягом 25 хвилин. За більший час значення імовірності Q_5 зменшується, бо збільшиться імовірність подолання рубежів захисту." [5]

РОЗДІЛ 2. МОДЕЛІ ЗАГРОЗ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. ФІЗИЧНА ОХОРОНА БАНКІВСЬКИХ СИСТЕМ ТА ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1 Описи технічних каналів витоку інформації

Для початку складемо класифікацію загроз, які впливають на інформацію. В загальних положеннях щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1 – 002 – 99) виділяють основні властивості інформації, яка захищається, а саме доступність, цілісність, конфіденційність та спостережність. Також після аналізу нормативних документів:

- НД ТЗІ 1.1 – 002 – 99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;
- НД ТЗІ 2.5 – 004 – 99 Критерії оцінки захищеності інформації в комп'ютерних системах від НСД;
- НД ТЗІ 1.4 – 001 – 2000 Типове положення про службу захисту інформації в автоматизованих системах;

Ми можемо виділити класи загроз в АС, такі як:

1. "Порушення доступності чи відмовлення в обслуговуванні (ПД);

– порушення при керуванні послугами і ресурсами користувача (ПДК);

– порушення стійкості до відмовлень (ПДС);

– порушення при гарячій заміні (ПДГ);

2. Порушення цілісності (логічної – ПЛЦ чи фізичної – ПФЦ);

– загрози при керуванні потоками інформації (ПЛЦП, ПФЦП);

– неможливість відкату – повернення захищеного об'єкта у вихідний стан (ПЛЦВ, ПФЦВ);

– порушення цілісності при обміні - загрози при експорті/імпорті інформації через незахищене середовище (ПЛЦО, ПФЦО);

3. Порушення конфіденційності (ПК);

– загрози при керуванні потоками інформації (ПКП);

– загрози існування безконтрольних потоків інформації (наявність схованих каналів) (ПКБ);

– порушення конфіденційності при обміні – загрози при експорті/імпорті інформації через незахищене середовище (ПКО);

4. Порушення спостережності;

– порушення при реєстрації небезпечних дій (ПСР);

– порушення при ідентифікації та автентифікації (ПСІ);

5. Несанкціоноване використання інформаційних ресурсів (НВ). " [6]

Загрози мають об’єктивну та суб’єктивну природу. До об’єктивних відноситься зміна умов середовища, відмовлення елементів системи. До суб’єктивних помилки персоналу чи дії зловмисника, тобто вони можуть бути випадковими чи навмисними.

З цього випливає, що на об’єкт впливають різні чинники (події, обставини), які можуть перешкоджати захисту інформації. Ці чинники можна описати, а саме:

1) "вони об’єктивно існують і можуть реалізовуватися в будь-який момент часу на будь-якому об’єкті АС, де обробляється інформація, що підлягає захисту;

2) вони не зводяться до загроз; один і той же процес чи подія в одному випадку призводить до загроз, а в іншому – не являє собою жодної небезпеки для інформації;

3) їх можна явно описати і класифікувати;

4) для кожного такого фактору існує можливість явно встановити, з якими видами загроз він пов’язаний;

5) для кожного такого фактору існує можливість визначити канали витоку інформації;

6) виникає можливість здійснювати конкретні дії з метою протидії загрозам.

Таким чином, виявляється, що загрози виникають внаслідок реалізації цих факторів, тобто є їх результатом. " [6] Ці фактори називаються дестабілізуючими (ДФ).

Причинами загроз можуть бути дії ЗЛ, випадкові дії персоналу, конкуренція збоку інших організацій. Необхідно виділити технічні канали витоку, такі як акустичні, радіотехнічні, оптичні и тп., канали спеціального впливу (порушення цілісності, знищення систем захисту зо допомогою полів та сигналів) та несанкціонований доступ до якого відноситься під’єднання до апаратури, використання маскування акаунтів користувачів для подолання захисту.

"Акустичний канал витоку інформації з обмеженим доступом. Акустичний канал витоку інформації може бути створений шляхом безпосереднього прослуховування розмов, що ведуться у кабінетах керівника товариства.

Створення акустичного каналу витоку інформації шляхом безпосереднього прослуховування мовної ІзОД малоймовірне, оскільки в приміщення закрито доступ стороннім особам, і всі відвідувачі контролюються системою відеоспостереження.

Ці засоби технічної розвідки можуть використовувати спеціальні вмонтовані та виносні мікрофони.

Враховуючи міські умови і особливості розташування ОІД, а також наявність місць неконтрольованого перебування фізичних осіб та автотранспортних засобів поблизу будинку, застосування технічних засобів

акустичної розвідки цілком імовірне. Найбільш вірогідне застосування засобів акустичної розвідки з північного сходу. Гранична відстань, з якої може використовуватися технічні засоби акустичної розвідки в умовах міста — 70 м." [7]

Далі розглянемо віброакустичний канал."Віброакустичний канал витоку інформації з обмеженим доступом. Даний канал витоку відбувається завдяки вібраційним коливанням, спричиненим акустичним полем мови, що розповсюджуються будівельними конструкціями та жорсткими інженерними комунікаціями, елементи яких виходять за межі контрольованої зони, та за рахунок недостатньої віброізоляції повітряних каналів системи вентиляції, шибок віконних отворів у кімнатах, недостатніх віброізоляційних властивостей труб систем, водопостачання, водяного опалення та каналізації." [7]

Оскільки на об’єкті інформаційної діяльності існують контрольовані зони які мають контроль за допомоги відеоспостереження та фіксації і перевірки при наближенні до перемету об’єкта створення вільроакустичного каналу є майже нульові шанси.

Наступний канал витоку інформації являє собою лазерний акустичний канал витоку інформації. "Лазерний акустичний канал витоку ІзОД утворюється за рахунок дистанційного перехоплення вібраційних коливань жорстких поверхонь, що виникають під впливом акустичного поля мови, лазерними засобами акустичної розвідки (ЛЗАР). які встановлюються в зоні прямої видимості з вікон кімнат.

До факторів, що знижують ефективність застосування ЛЗАР слід віднести: високу інтенсивність руху автотранспорту та високий рівень шуму по вулиці, також ускладнення пошуку зони прямої видимості за рахунок зелених насаджень.

Гранична відстань для використання ЛЗАР в міських умовах складає не більше 200 м." [7]

Акустоелектричний канал витоку інформації. "Акустоелектричний канал утворюється під впливом акустичного поля мови на технічні засоби, що встановлені у приміщеннях чи кімнатах за рахунок акустоелектричного перетворення в електронних схемах цих засобів та має самочинний характер.

Акустоелектричний канал може бути створений за рахунок: поширення інформативних сигналів дротовими лініями технічних засобів (ОТЗ та ДТЗС), які мають "мікрофонний ефект", наприклад, лініями відкритого телефонного зв'язку та їх приймання засобами технічної розвідки, які підключаються до провідних ліній, що виходять за межі КЗ, і працюють в діапазоні від одиниць Гц до 500 МГц;

Можливість витоку ІзОД дротовими лініями зв’язку блокуватиметься використанням пристрою захисту аналогових телефонних ліній (ПЗАТЛ) та протизавадних мережевих фільтрів «Імпульс».

Перехоплення засобами технічної розвідки інформативних сигналів ведеться із застосуванням радіоприймальних пристроїв систем і комплексів радіоелектронної розвідки. В залежності від потужності сигналу ефективна відстань зйому інформації становить від десятків до сотень метрів. " [7]

Допоміжні технічні засоби, провідники які знаходяться на ОІД якщо вони знаходяться в одній зоні та мають спільні лінії, якими можуть поширюватися небезпечні сигнали. Вони можуть створювати антени які призведуть до витоку інформації. "Канали витоку інформації з обмеженим доступом за рахунок побічних електромагнітних випромінювань і наводів. Канали витоку ІзОД за рахунок побічних електромагнітних випромінювань і наводів (ПЕМВН) розрізняються, як за видом середовища розповсюдження, так й за причиною або фізичним явищем, завдяки яким небезпечний сигнал потрапляє в це середовище. Цілком ймовірним є утворення таких каналів:

–каналу витоку, обумовленого електричними і магнітними полями розсіяння ОТЗ;

–каналу витоку, що виникає за рахунок взаємного впливу між ланцюгами, якими передається секретна інформація (ланцюг, що впливає) і ланцюгами, які мають вихід за межі КЗ (ланцюги, на які вплив розповсюджується);

– каналу витоку, що виникає за рахунок стікання (витоку) струмів інформативного сигналу в ланцюги заземлення;

– каналу витоку, що виникає під час нестійкої роботи підсилювачів («паразитна» генерація);

– каналу витоку, обумовленого «паразитною» модуляцією високочастотних генераторів і підсилювачів;

– каналів витоку, що виникають під час впливу електричних, магнітних або акустичних полів небезпечного сигналу на ДТЗС.

Перехоплення ПЕМВН здійснюється шляхом приймання та аналізу електромагнітних випромінювань, які виникають під час роботи ОТЗ і ДТЗС, а також наводів інформативних сигналів в телекомунікаціях ОТЗ і ДТЗС, які виходять за межі контрольованої зони.

Витік інформації з обмеженим доступом за рахунок побічних електромагнітних випромінювань і наводів стане унеможливлена за рахунок використання комплексів засобів обчислювальної техніки в захищеному виконанні – «Плазма 3В Робоча станція» на яких здійснюється обробка ІзОД, що усуває можливість витоку інформації каналами ПЕМВН. " [7]

"Канали витоку інформації з обмеженим доступом шляхом високочастотного нав'язування. Реалізація методів дистанційного перехоплення ІзОД можлива також шляхом ВЧ-нав'язування провідними лініями, які виходять за межі КЗ. Найбільш ймовірним є організація ВЧ-нав'язування лініями відкритого міського телефонного зв'язку та лініями мережі електроживлення, що унеможливлюється використанням протизавадних мережевих фільтрів «Імпульс» та ПЗАТЛ. " [7]

Візуально-оптичний канал витоку інформації. Створюється за допомогою спеціальних технічних засобів, які знаходяться в прямій видимості у вікнах

об’єкта інформаційної діяльності, мається на увазі документі у паперовому вигляді та розуміння обстановки та структури об’єкта інформаційної діяльності.

В залежності від умов спостереження інформацію можна отримати різними шляхами, а саме зйомки на відстані чи спостереження через візуально оптичні технічні засоби.

Цей канал витоку інформації легко блокує ефективне використання технічних засобів при наявності жалюзів на об’єкті інформаційної діяльності.

Останній канал витоку матеріально речовий. "Матеріально – речовий канал витоку інформації з обмеженим доступом. Матеріально-речовий канал витоку може бути реалізований через несанкціоноване отримання доступу до матеріальних носіїв інформації – документів, цифрових носіїв. Проте всі носії зберігаються у сейфі, доступ до якого мають лише начальник відділу та керівник установи. Використання систем контролю доступу, систем охоронної сигналізації та відеоспостереження унеможливлює доступ до інформації сторонніх осіб та працівників без допуску. " [7]

2.2 Модель порушника

"Порушник - це особа, яка може отримати доступ до роботи з включеними до складу АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки. " [8]

Існують різні моделі порушників, оскільки кожен випадок залежить від конкретної ситуації в ІС. Виходячи с того яка використовується технологія обробки інформації можливо розробити моделі порушників.

"При розробці моделі порушника визначаються:

- припущення про категорії осіб, до яких може належати порушник;
- припущення про мотиви (цілях) порушника;
- припущення про кваліфікації порушника і його технічної оснащеності;
- обмеження і припущення про характер можливих дій порушників." [8]

Існують порушники внутрішні та зовнішні. Також допускається, що порушник являє собою фахівця високої кваліфікації у якого є інформація про систему.

"Внутрішнім порушником можуть бути:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки і супроводи ПО (прикладні і системні програмісти);
- технічний персонал, що обслуговує будинки (прибиральники, електрики, сантехники й інші співробітники, що мають доступ у будинки і приміщення, де розташовані компоненти ІС);
- співробітники служби безпеки ІС;
- керівники різних рівнів посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

- клієнти;
- відвідувачі;
- представники організацій, взаємодіючих з питань забезпечення життєдіяльності організації (энерго-, водо-, теплопостачання і т.п.);
- представники конкуруючих організацій (іноземних спецслужб) або особи, що діють по їхньому завданню;
- особи, випадково або навмисне порушили пропускний режим (без мети порушити безпеку ІС);
- будь-які особи за межами контрольованої території. " [8]

Основними мотивами порушень:

1. корисливий інтерес;
2. безвідповідальність;
3. самоствердження;

Корисливий інтерес це напад на систему заради доступу інформації. Безвідповідальний це некомпетентні чи недбалі дії які призводять до витіку інформації. Самоствердженний мотив це коли користувач отримавши доступ до системи вважає, що може використовувати її для власних цілей заради самоствердження перед власною персоною чи самоствердженням перед колегами.

"Усіх порушників можна класифікувати в такий спосіб:

За рівнем знань про ІС:

– знає функціональні особливості ІС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

– має високий рівень знань і досвідом роботи з технічними засобами системи і їхнього обслуговування;

– має високий рівень знань в області програмування й обчислюваної техніки, проектування й експлуатації автоматизованих інформаційних систем;

– знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (використовуваним методам і засобам):

– застосовуючи тільки агентурні методи одержання зведень;

– застосовуючи пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

– застосовуючи тільки штатні засоби і недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, що можуть бути потай пронесені через посади охорони;

– застосовуючи методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, упровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

За часом дії:

– у процесі функціонування ІС (під час роботи компонентів системи);

– у період пасивності компонентів системи (неробочий час, планові перерви в роботі, перерви для обслуговування і ремонту і т.п.);

– як у процесі функціонування ІС, так і в період пасивності компонентів системи.

По місцю дії:

– без доступу на контрольовану територію організації;

– с контрольованої території без доступу в приміщення;

– усередині приміщень, але без доступу до технічних засобів ІС;

– з робочих місць кінцевих користувачів (операторів) ІС;

– з доступом у зону даних (баз даних, архівів і т.п.);

– з доступом у зону керування засобами забезпечення безпеки ІС.

Необхідно враховувати наступні обмеження і припущення про характер дій можливих порушників:

– робота з підбору кадрів і спеціальні заходи утрудняють можливість створення коаліцій порушників, тобто об'єднання (змови) і цілеспрямованих дій по подоланню підсистеми захисту двох і більш порушників;

– порушник, плануючи спроби НСД, ховає свої несанкціоновані дії від інших співробітників.

НСД може бути наслідком помилок користувачів, адміністраторів, що експлуатує й обслуговує персоналу, а також недоліків прийнятої технології обробки інформації і т.д. " [8]

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ ІСНУЮЧОЇ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА ОХОРОНИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ (ТВБВ №10003/0467 АТ «Ощадбанк»)

3.1 Дослідження ТВБВ №10003/0467 філії - Дніпропетровського обласного управління публічного акціонерного товариства "Державний ощадний банк України" як об'єкту інформаційної діяльності та його захист

ТВБВ №10003/0467 АТ «Ощадбанк» створено з метою обслуговування клієнтів, ведення рахунків клієнтів (резидентів) та здійснення розрахунків за їх дорученням (у національній валюті України), залучення депозитів фізичних осіб, ведення валютних рахунків клієнтів, неторгівельні операції. Місцезнаходження філії: м. Нікополь проспект Трубників, 26. Вибір відділення ТВБВ №10003/0467 АТ «Ощадбанк» як об'єкта інформаційної діяльності обумовлений наступними факторами:

1. "Відомості про банківські рахунки клієнтів
2. Операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;
3. Фінансово-економічний стан клієнтів;
4. Системи охорони банку та клієнтів;
5. Інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;
6. Відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
7. Інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;
8. Коди, що використовуються банками для захисту інформації;

9. Інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності" [9]

10. у відділенні розміщуються різні радіо – електронні прилади, які можуть бути джерелами побічних електромагнітних випромінювань і наводок;

11. у відділенні є елементи інтер'єру та меблі, в яких можна легко заховати заставні пристрої;

Структура ТВБВ №10003/0467 АТ «Ощадбанк» складається з: начальника відділення, заступник відділення, менеджер по роботі з клієнтами, касир, старший касир, менеджери мікро-, малого та середнього бізнесу, інженер систем відеоспостереження, охоронник.

До основних завдань ТВБВ №10003/0467 АТ «Ощадбанк»:

1. Своєчасне обслуговування клієнтів.

2. Ведення рахунків клієнтів (резидентів) та здійснення розрахунків за їх дорученням (у національній валюті України).

3. Залучення депозитів фізичних осіб.

4. Ведення валютних рахунків клієнтів.

5. Неторгівельні операції.

6. Підтримка та оновлення програмного забезпечення у робото-спроможному стані.

7. Здійснення заходів із забезпечення постійного функціонування системи антивірусного захисту інформаційних ресурсів.

8. Здійснення організаційно-технічних заходів щодо захисту програмних комплексів, телекомунікацій, каналів зв'язку і мереж від несанкціонованого доступу.

Відділення ТВБВ №10003/0467 АТ «Ощадбанк» знаходиться на першому поверху у п'ятиповерховому будинку и безпосередньо не межує з іншими приміщеннями. У приймальні залі можлива тривала присутність сторонніх осіб (співробітників і відвідувачів), які очікують прийому, проводять різноманітні види операцій з грошима та документацією. Будівля, в якій знаходиться

відділення оточена іншими жилими і адміністративними будинками з яких можливе перехоплення радіосигналів закладних пристроїв і побічних електромагнітних випромінювань і наведень.

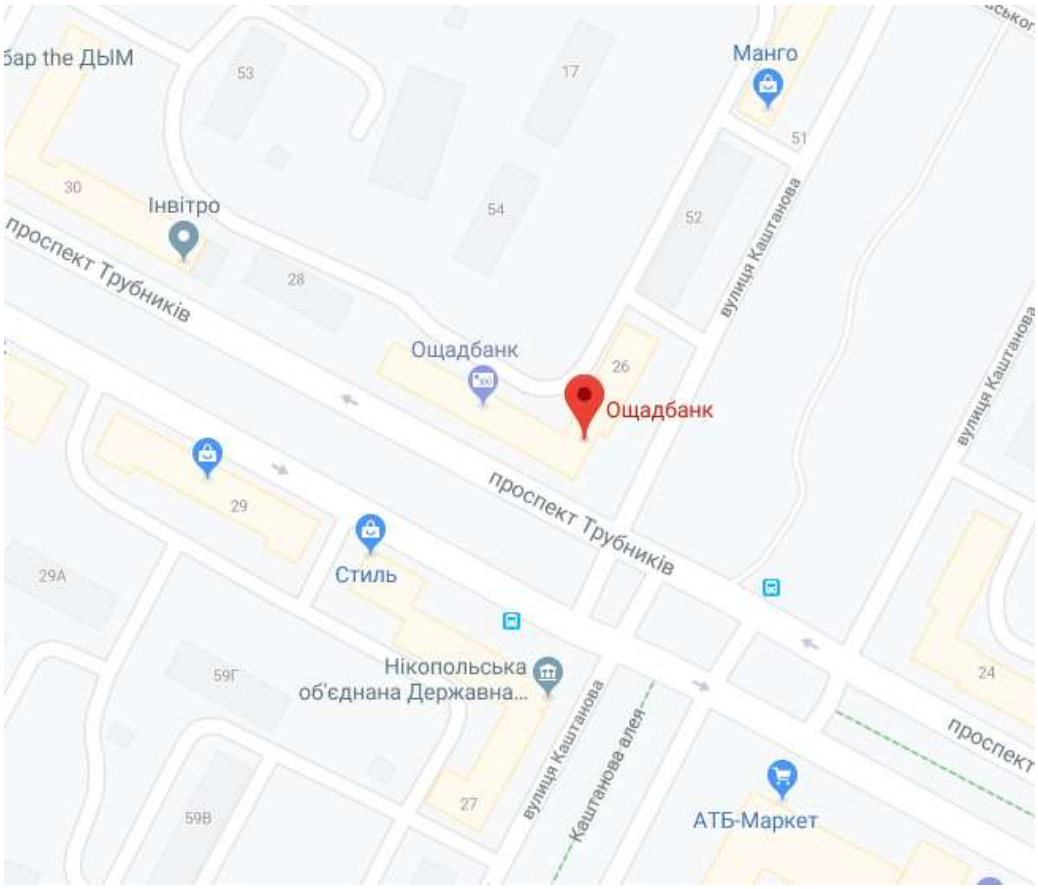

Рис. 3.1 Місцезнаходження ТВБВ №10003/0467 АТ «Ощадбанк» (супутниковий знімок)

Вікна відділення виходять на одну сторону вулиці, де знаходиться парк, житловий будинок. Поруч знаходяться магазин одежі «Лабіринт», аптека без назви та асфальтоване місце для автомобілів. Ширина вулиці 15 м. На протилежному боці від дверей вулиці розташований парк з дитячим майданчиком. З боку відділення знаходиться проспект із зеленним насадженням де висота дерев не менш 8м. Позаду знаходяться житлові будинки. Відділення не має власну територію поза виділеним приміщенням тому не має парканів.

Вхід відбувається через головні двері, які знаходяться зі сторони місця для парковки автомобілів. Вікна укріпленні масивним металопластиковим профілем та мають армування із замкненим контуром.

Система відеоспостереження підключена до централізованого пульту охорони, що знаходиться всередині будівлі в кімнаті охорони і контролюється оператором цілодобово.

Загальна площа приміщення складає 74.5 м^2: передпокій 3 м^2, приймальня клієнтів 12 м^2, кімната охорони 8 м^2, кабінет директора відділення 8.5 м^2, дві касі по 4 м^2, офіс 27 м^2, санітарний вузол 4 м^2, коридор між офісом та приймальною 2 м^2.

Рис. 3.2 схема відділення ТВБВ №10003/0467 АТ «Ощадбанк»

3.2 Моделювання ТВБВ №10003/0467 АТ «Ощадбанк»

Для моделювання чинників, які впливають на захищеність інформації, необхідно провести його обстеження. Модель приміщення містить 5 груп факторів:

- огородження;
- загальна характеристика приміщення;
- предмети меблів і інтер'єру;
- засоби комунікацій;
- радіоелектронні засоби та електричні прилади;

Результати обстеження приміщення знаходяться в таблиці 3.1

Всередині контрольованої зони знаходяться лінії електроживлення із заземленням основних технічних засобів. В таблиці 3.2 знаходяться допоміжні технічні засоби, які знаходяться у відділенні.

Результати обстеження приміщення таблиця 3.1

Таблиця 3.1

№	Фактори	Параметри
Загальна характеристика приміщення		
1.1	Поверх	Перший
1.2	Площа,м^2	74.5
1.3	Суміжні приміщення	При вході передпокій далі приймальня клієнтів де знаходяться каси з вікнами прийому для клієнтів, з лівої сторони знаходиться коридор між офісом та приймальною, в коридорі знаходиться вхід до приміщення охорони. Кабінет директора відокремлений від офісного приміщення.
Огородження		
2.1	Стіни	Зовнішні з червоної цегли товщиною у 3 цеглини; внутрішні в офісі, кабінетом директора, кімнатою охорони – товщиною 1 цеглу. Каси побудовані з монолітних

		(легкий бетон) стін.
2.2	Стеля	Підвісна стеля білого кольору, як елемент декору закриває собою залізобетонні плити, товщиною 50 см. Відстань між стелями 15 см.
2.3	Підлога	Керамічна плитка білого кольору.
2.4	Вікна	2 вікна у приймальній для клієнтів; Масивний металопластиковий профіль, армуванні із замкненим контуром; Товщина металу в каркасі –2,5 мм.; Склопакет відповідно до класифікації безпеки DIN EN 356
2.5	Двері	До входу у передпокій відділення двері металопластикові. В саме відділення металеві. Кімната охорони та каси мають укріпленні металеві двері. Кабінет директора має броньовані двері.
Предмети меблів та інтер'єру		
3.1	Стіл для роботи	Дерев'яний (1 шт.), пластмасовий (8 шт.)
3.2	Сейф	Для документації в кабінеті директора, для грошей у касі.
3.3	Крісло	Шкіряне (1 шт.), пластмасове (8 шт.)
3.4	Лавка	Пластмасова (2 шт.)
Радіоелектронні засоби та електричні прилади		
4.1	Банкомат	1 шт.
4.2	Термінал	1 шт.
4.3	Комп'ютер	ASUS: системний блок, монітор, клавіатура, миша (10 шт.)
4.4	Камера відеоспостереження	8 шт.
4.5	Сповіщувач пожежний	9 шт.
4.6	Датчик руху	5 шт.
4.7	Датчик розбиття скла	3 шт.
4.8	Телефон міський	В офісі та в кабінеті директора (2 шт.)
Засоби комунікацій		
5.1	Електропроводка	Схована у стінах
5.2	Розетка електроживлення	14 шт.

Технічні засоби які використовуються таблиця 3.2

Таблиця 3.2

№	Найменування ТЗ	Тип ТЗ	Місце розташування	***Кількість, шт.***
1.	Телефон міського зв’язку	Huawei ets 3053	У кабінеті директора відділення, в офісі.	3
2.	Принтер	HP LaserJet Pro M28a (W2G54A)	В офісі та в касі.	3
3.	Пасивний інфрачервоний сповіщувач	Optex MX-40QZ	На стінах в усіх приміщеннях	5
4.	**Камера відеоспостереження**	**Bosch VDN-244V03-1**	На вулиці при вході до відділення, у приміщенні де знаходяться банкомат та термінал, перед касами безпосередньо біля вікон обслуговування, в коридорі між приймальною та офісом, в офісі, перед кабінетом директора.	8
5.	Датчик диму	**Covi Security SM-01**	На стелі в усіх приміщеннях	9
6.	Датчик розбиття скла	DSC AC-101	На стелі навпроти вікон та на вході у відділення навпроти скляних дверей.	3

Слід зазначити, що користування допоміжними технічними засобами сторонніми особами суворо заборонено.

Система охорони та пожежної сигналізації знаходиться та прокладено в усіх приміщеннях відділення. Системи підключені до пульту охорони, який знаходиться в кімнаті службі охорони. Всі дроти елементів системи охоронної та пожежної сигналізації екрановані, що означає недоступність для сторонніх осіб. До системи охоронної та пожежної сигналізації входять:

– пасивні інфрачервоні сповіщувачі;

– датчики пожежної сигналізації.

– датчики розбиття скла;

В кімнаті службі охорони знаходиться пульт охорони до якого підключена система відеоспостереження.

РОЗДІЛ 4. РОЗРОБКА ПРОЕКТУ УДОСКОНАЛЕНОЇ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТВБВ №10003/0467 АТ «ОЩАДБАНК»

4.1 Вибір елементів та пристроїв для фізичної охорони приміщення

Під час проходження практики у відділені ТВБВ №10003/0467 АТ «Ощадбанк» мною був проведений аналіз відділення і засобів покращення захисту та моделювання основних загроз. Основуючись на цих даних створюю рекомендації щодо покращення стану захищеності відділення.

"Засоби запобігання проникнення порушника до джерел інформації повинні забезпечувати:

– затримку зловмисника чи іншого джерела загрози на час, більший часу нейтралізації загрози;

– виявлення зловмисника, або джерела іншої загрози;

– нейтралізацію загроз впливу на джерело інформації.

Якщо зловмисник збирається на проникнення, то швидкість його просування залежить від довжини шляху від місця вторгнення до місця знаходження джерела, кількості і міцності механічних перешкод. Один і той же час затримки забезпечується невеликою кількістю добре укріплених рубежів і великою кількістю слабших рубежів. Раціональний варіант знаходиться в результаті мінімізації вартості. Однак слід враховувати можливість допомоги завербованих співробітників, зовнішньому зловмисникові. Чим більше використовується заходів захисту, тим складніше співробітнику їх виявити і передати відомості про них зловмисникові.

Якщо джерело інформації зберігається в сейфі приміщення, то зловмисникові в типовому варіанті необхідно подолати огорожу, вхідні двері, сходи, двері у приймальню, двері у кабінет, сейф. Механічна міцність кожної з

цих перешкод оцінюється часом їх подолання при використанні різних інструментів." [7]

З метою створення перешкод для злочинці, а сама збільшення часу затримок необхідно дотримуватись наступних заходів:

6. Місяця чергової зміни мають знаходитись поруч з приміщенням які мають цінної інформацією;
7. Побудова додаткових рубежів захисту на найбільш ймовірних шляхах дій зловмисників до місця зберігання важливої інформації;
8. Укріплення механічної міцності стін, вікон, дверей, приміщень, сейфів;

З метою затримкою вогню, як загрози для інформації:

- Постійне спостереження та контроль усіх проводів та пристроям комутації, тобто розетки, запобіжники, автомати. Швидка заміна усіх неполадок, проводів з пошкодженою ізоляцією;
- У приміщеннях в яких знаходиться цінна інформація не повинно бути приладів які мають тепло-електронагрівальний пристрій і легкозаймистих речовин і матеріалів;
- Використання спеціальних пожежостійких сейфів;

З метою блокування приміщення необхідно застосовувати різноманітні сповіщувачі:

- Датчик руху;
- Пасивний ІЧ сповіщувач;
- Датчик розбиття скла;
- Камери відеоспостереження;

"Датчик руху – різновид датчика охоронної сигналізації, який виявляє і реагує на переміщення об’єктів в запрограмованій зоні дії. Принцип роботи датчиків руху полягає у відстеженні рівня інфрачервоного випромінювання в полі зору датчика: при появі людини (або об’єкту з температурою більше за фонову) збільшується напруга на виході датчика. Для визначення руху датчик використовує оптичну систему – лінзу Френеля або систему увігнутих

сегментних дзеркал: при цьому сегменти оптичної системи фокусують інфрачервоне випромінювання на піроелементі, що видає електричний імпульс. Датчики руху в системах охоронної сигналізації мають вихідне реле – спеціальний перемикач, електромеханічний пристрій для комутації електричних ланцюгів. При виявленні процесу руху датчик передає відповідний тривожний сигнал в спеціальний охоронний пристрій, який пересилає тривогу на пульт централізованого спостереження.” [10]

Встановимо у відділенні внутрішній датчик руху DSC LC-100 PI. Задача датчику відстеження рухів людей в приміщенні в якій знаходиться інформація та приміщень які охороняються.

Перевага даного засобу в тому, що виробник дає довічну гарантію на свої плати. З цього робимо висновок, що датчик руху DSC LC-100 PI володіє високою якістю та надійністю. Має доступну ціну.

Використовує спеціально розроблену лінзу з унікальним квадратичним PIR датчиком і нову схему на базі ASIC, оптимізовані для виключення помилкових тривог від малих тварин. DSC LC-100 PI забезпечує відмінний рівень захисту від видимого світла. Сповіщувач забезпечує надійне виявлення об'єктів для будь-яких випадків застосування. DSC LC-100 PI поставляється з ширококутного лінзою.

Рис. 4.1 DSC LC-100 PI

Функціональні характеристики:

- зчетверений піроелемент;
- цифрова обробка сигналу;
- ігнорує тварин вагою до 25 кг;
- автоматична термокомпенсація;
- регульований лічильник імпульсів;
- регулювання чутливості;
- світлодіодна індикація;
- світлодіод загоряється під час спрацювання;
- контакт несанкціонованого доступу розмикається при відкритті кришки;

"Пасивні інфрачервоний сповіщувач (ПІК) це один з найбільш поширених типів сповіщувачів, що застосовуються в системах охоронної сигналізації. В основі принципу роботи сповіщувача лежить реєстрація змін потоку теплового випромінювання, які виникають у разі перетину людиною спеціальних чутливих зон, і перетворенні інфрачервоного (ІЧ) випромінювання в звичайний електричний сигнал з подальшим аналізом його по амплітуді часу.

Прості ПІК використовують обробку сигналу аналоговими методами, більш складні і, відповідно, найдорожчі - цифрові методи (вбудованим процесором) При цьому, форма зони виявлення (може бути лінійної, об'ємної або поверхневої) формується відомої лінзою Френеля.

Інфрачервоні сповіщувачі можуть бути стельового і настінного типу, який і застосовуються найчастіше. У комплектацію датчиків можу входити кронштейни, що дозволяють орієнтувати сповіщувач в потрібному напрямку, однак, багато сучасних сповіщувачі припускають установку і без кронштейна в кутку приміщення. Існують особливі сповіщувачі, орієнтовані для установки в приміщеннях з тваринами (собаками або кішками), в яких для попередження помилкових спрацьовувань на вихованців використовуються спеціальні лінзи з захистом від домашніх тварин.

Як застереження варто сказати, що не рекомендується встановлювати ІК датчики поблизу від вентиляційних отворів, дверей, вікон та інших отворів, що створюють повітряні потоки, а також систем центрального та іншого опалення, приладів для обігріву і т.п., що створюють теплові перешкоди. В іншому випадку можлива висока помилкова оброблюваність сповіщувачів. Також на якість спрацьовування датчика може вплинути пряме попадання світлового випромінювання від сонця, ламп розжарювання і т.д. " [11]

На вулиці встановимо OPTEX BX-80N. Всепогодний охоронний сповіщувач Optex BX-80N належить серії BX - вуличних ПІК сповіщувачів для захисту фасадів будівель (наприклад вікон).

Модель Optex BX-80N охоплює дуже велику область детекції, так як спрямований в дві сторони. Для випадків коли зона детекції може охоплювати небажані об'єкти передбачена можливість обмеження відстані до 12, 8, 5 або 2 метрів в кожну сторону.

Сповіщувач BX-80N повністю виключає помилкові спрацьовування, викликаними діями дрібних тварин, так як здатний визначити розмір об'єкта детекції.

Крім цього сповіщувач відрізняється зручністю монтажу і простотою налаштування.

Особливості:

- Вуличний ІК сповіщувач для захисту фасадів будівель (24 м).
- Функція обмеження зони детекції
- Розпізнавання розміру об'єкта
- Звукове попередження

Рис. 4.2 Optex BX-80N

Характеристики:

• Метод детекції ПІК;

• Область детекції 12 м в кожну сторону (2 зони детекції в кожну сторону);

• Налаштування області детекції обмеження дальності 2/5/8/12 м;

• Висота установки від 0,8 до 1,2 м;

• Індикація стану індикація тривоги (вкл. / Викл.);

• Чутливість 1,6 ° С при швидкості 0,6 м/с, можлива швидкість переміщення об'єкта 0,3 - 1,5 м/с;

• Час тривоги тривалість тривожного сигналу 2 с;

• Час розігріву 45 с;

• Тривожний вихід 2 виходи - Н.З. і Н.О. .; 28 В пост. струму; 0,2 А (макс.);

• Вихід тампера розтин корпусу, Н.З .; 24 В пост. струму; 0,1 А (макс.);

• Умови експлуатації робоча температура від -35 до +50 ° С, ступінь захисту IP55;

• Захист від радіоперешкод;

• Вага 400 г;

"Датчик розбиття скла – це акустичний пристрій, призначений для виявлення і визначення звуку розбитого скла на території знаходиться під

охороною, з подальшою подачею сигналу на ППК. Практично датчики розбиття скла запобігають несанкціоноване проникнення в охоронювані приміщення через вікна, уловлюючи звук від пошкодження скла. Спрацьовування детектора може викликати будь-який звук, який лунає на частоті звуків склом в момент його розбиття. " [12]

У відділенні знаходиться два вікна з виходом на вулицю, скляні вікна обслуговування до кас та скляні двері до входу у приміщення обслуговування клієнтів. Встановимо бездротовий датчик розбиття скла Ajax GlassProtect. Може бути встановлений на відстані до 9 метрів від скла і фільтрує події, які можуть спричинити помилкове спрацьовування тривоги. Принципом роботи Ajax GlassProtect є визначати зо допомогою електронного мікрофона розбиття скла. Має двофакторний метод визначення розбиття.

Рис 4.3 Ajax GlassProtect

"Технічні характеристики:

- Класифікація: сповіщувач охоронний поверхневий звуковий радіоканальний. Тип датчика: бездротовий.
- Спосіб установки: всередині приміщень.
- Сумісність: працює з Hub, Hub Plus, ocBridge Plus, uartBridge.
- Чутливий елемент: електретний мікрофон.

- Дальність визначення розбиття: до 9 метрів.
- Час доставки сигналу тривоги: 0,15 с.
- Чутливість: настроюється, 3 рівня.
- Кут огляду: 180°.
- Температурний сенсор.
- Діапазон робочих температур: від -10°C до +40°C.
- Допустима вологість: до 75%.
- Антисаботаж: захист від підробки, оповіщення про глушіння, тампер на відкриття і відрив.
- Діаметр: 20 мм.
- Висота: 90 мм.
- Вага: 30 г. " [13]

На вході ззовні встановимо камеру спостереження IP-камера Hikvision DS-2CD2043G0-I (Рис. 4.5) та у відділенні камери HIKVISION DS-2CD2121G0-IS (Рис 4.6)

Рис. 4.5 IP-камера Hikvision DS-2CD2043G0-I

Технічні характеристики:

- Нахил: 0 ° - 90 °
- Інфрачервоне підсвічування: до 30 м
- Поворот: 0 ° - + 360 °
- Інтерфейси: 10 / 100BASE-TX Ethernet
- Розмір матриці: 1/3
- Виробник і тип матриці: Progressive Scan CMOS
- Формат відео: MJPEG H.264 H.265
- Фокусна відстань: 4 мм мм
- Кут огляду по горизонталі: 78 °
- Слот для карт пам'яті MicroSD

Рис. 4.6 Внутрішня купольна камера HIKVISION DS-2CD2121G0-IS

Технічні характеристики

- Матриця 1 / 2,8 "Progressive Scan CMOS - 2Мп (1920x1080);
- Фіксований об'єктив з фокусною відстанню 2,8 мм і кутами огляду 115°, 62°, 136°;

- Режим "день-ніч" і ІК-підсвічування до 20 м;
- Інтерфейси: аудіо 1 вх / 1 вих; тривога 1 вх / 1 вих;
- Зберігання даних: NAS (NFS, SMB / CIFS), ANR, Micro SD до 128 Гб;

З метою забезпечити захисту від пожежі в приміщеннях відділення використовуємо спеціальні пожежні сповіщувачі.

"Датчик диму – це пожежний датчик, призначений для виявлення загорянь у приміщеннях різних будівель і споруд, а також передачі сигналу «Пожежа» на пожежний приймально-контрольний прилад (ППКП). Димовий датчик важлива частина пожежної сигналізації, він розрахований на безперервну цілодобову роботу, як правило, має функцію індикації чергового режиму роботи (блимання червоного світлодіода). " [14]

Встановлюємо Covi Security SM-01 призначений для відстеження загорянь і присутності диму в приміщенні. Так як пристрій бездротовий, легко монтується і демонтується, немає необхідності тягнути дроти через це значна економія за рахунок відсутності монтажу. Один датчик розрахований на площу 20 м². Маємо можливість регулювати його потужність в залежності від розміру приміщення. При тривозі включається сирена з потужністю звуку 85 дБ., така сирена привертає увагу, але не робить психофізичного впливу на оточуючих. Пристрій можна підключати до охоронних централей. Також датчик може працювати автономно. У будь-якому випадку, буде забезпечено захист від пожежі. Передача бездротового радіосигналу на відстань до 100 м дає можливість охопити великі площі. При необхідності збільшити відстань є можливість встановити підсилювачі сигналу. Низький рівень споживання енергії, працює від однієї батареї до 24 місяців.

Рис. 4.7 Covi Security SM-01

Технічні характеристики

Тип датчика: бездротовий;

Тип сенсора: фотоелектричний;

Покривається площа: 20 м²;

Гучність вбудованої сирени: 85 дБ;

Дальність передачі: 100 м;

Частота передачі: 433 МГц;

Потужність радіопередавача: 10 мВт;

Харчування: батарея PP3 (Крона);

Термін роботи без заміни елементів живлення: до 24 міс.;

Робоча напруга: 9 В;

Струм в режимі бездіяльності / тривоги: 5/36 мА;

Діапазон робочих температур: -0 ° C - +40 ° C;

Робоча вологість: від 10 до 85%;

Розміри: 115x35 мм;

4.2 Поліпшення захищеної системи технічного захисту

Відділення ТВББ №10003/0467 АТ було не великим та виконувало малу кількість функцій, але при розширенні є необхідність удосконалення систем технічного захисту. ТВББ №10003/0467 АТ повинна мати реєстрацію працівників, що мають допуск та територію відділення чи в спеціальні приміщення з важливою інформацією, грошима. Також це допоможе контролювати співробітників відділення щодо вчасного приходу до роботи.

Для подолання цих проблем буде доцільним використання найсучасніших систем управлінням доступу, які будуть знаходитися в загальній АС обробки інформації у відділенні. Система управлінням доступу програмно-апаратний комплекс встановлюється у відділенні та інформація про всіх співробітників заноситься та впорядковується в базу даних і фізично розташовується в кімнаті охорони, яка захищена від стороннього доступу. База даних перебуває під керівництвом директора відділення. Доступ до бази мають тільки співробітники відділення. Для керування використовується програмний інструментарій. Також кожному співробітнику передають спеціальний ідентифікаційні документи, який має вигляд персоніфікованої пластикової картки, які працюють за допомоги безконтактної технології зчитування інформації. За допомоги цих документів ми розуміємо хто з співробітників зайшов чи вийшов з відділення.

Директор відділення має повноваження переглядати інформацію про затримку співробітників та момент входу до приміщень спеціального призначення.

Програмно-апаратний комплекс надає звуковий та візуальний сигнал якщо особа без ідентифікаційного посвідчення буде намагатися проникнути до приміщень спеціального призначення.

Оскільки у відділенні лише два вікна у приймальню для клієнтів, то захист від оптичного каналу витоку інформації виконують жалюзі тому, що вони

найкраще виконують свої функції, а саме захист від спостереження через вікно сусіднього будинку та захист від сонця. Варіант із затемненням спеціальною тонованою плівкою вікон не підходить. Це одразу показую ЗЛ про намір підвищити умови захисту інформацію також занадто сильно зменшують природне освітлення в приміщенні.

Двері до важливих приміщень мають спеціальні доводчики дверей, які закривають двері якщо ті з якоїсь причини не булі замкнуті.

Для виявлення встановлених сторонніх пристроїв та камер які були таємно встановленні у відділенні, періодично проводять заходи по їх виявленню.

4.3 Захист інформації в ТВБВ №10003/0467 за допомогою СЕП

Основною інформацією яка захищається у ТВБВ №10003/0467 є інформація про особу та персональні дані, конфіденційна, бухгалтерська і комерційна. Щоб захистити інформацію у відділенні ТВБВ №10003/0467 необхідно використовувати програмно-апаратний комплекс захисту інформації, тобто систему електронних платежів надалі СЕП.

"Система електронних платежів Національного банку України - це загальнодержавна платіжна система, яка забезпечує здійснення розрахунків в електронній формі між банківськими установами та їх філіями як за дорученнями клієнтів банків, так і за зобов'язаннями банків один перед одним на території України. Розрахунковий документ в електронному вигляді - документ визначеного формату, що містить установлені реквізити і несе інформацію про рух коштів, має форму електронних записів, обов'язково захищений криптографічними методами захисту інформації, передається засобами телекомунікаційного зв'язку та зберігається на зовнішніх засобах збереження інформації у вигляді файлу. " [15]

Система електронних платежів виконує функцію розрахунків в Україні між банками за запитом клієнтів, за зобов’язанням банків та в загалі між

іншими учасниками системи. Міжбанківські перекази виконуються у файловому режимі в реальний час. Платежі можуть бути обов’язковими та за вибором, а саме початковий є обов’язковим і в режимі реального часу за вибором учасника. Учасники системи, який знаходиться в СЕП в файловому режимі зобов’язаний забезпечити приймання платежів які були призначенні на його адрес іншими учасниками.

"У файловому режимі обмін міжбанківськими електронними розрахунковими документами здійснюється шляхом приймання-передавання документів, згрупованих у файли. Тривалість технологічного циклу становить 15 – 20 хвилин. Кошти списуються з технічного рахунку учасника СЕП у момент приймання початкових платежів до Центру оброблення СЕП та зараховуються на технічний рахунок учасника-отримувача у момент надходження до Центру оброблення СЕП квитанції про успішне приймання файла платежів у відповідь.

У режимі реального часу кошти списуються з технічного рахунку учасника СЕП-платника і зараховуються на рахунок учасника-отримувача одночасно.

СЕП приймає початкові платежі від учасника системи в межах поточного значення його технічного рахунку. У СЕП немає пріоритетів оброблення платежів, крім черговості їх надходження.

СЕП визнана системно важливою платіжною системою в Україні. Системна важливість СЕП обумовлена тим, що вона забезпечує здійснення 97% міжбанківських переказів у національній валюті в межах України. СЕП є системою класу RTGS.

Правова основа функціонування СЕП

Базовим законом, що визначає загальні засади функціонування платіжних систем в Україні та загальний порядок проведення переказу коштів у межах України, є Закон України "Про платіжні системи та переказ коштів в Україні".

Цим Законом СЕП визначено державною системою міжбанківських розрахунків, а Національний банк України – платіжною організацією та розрахунковим банком СЕП. Порядок функціонування СЕП визначається Національним банком України. " [16]

Також необхідно розглянути програмне забезпечення та характеристики СЕП. "Програмне забезпечення СЕП складається із програмно-технічних комплексів — автоматизованих робочих місць (АРМ), що відповідають трьом рівням структури СЕП: Центральна розрахункова палата — АРМ-1, АРМ ІПС; розрахункова палата — АРМ-2; банківська установа — учасник СЕП — АРМ-НБУ. " [17]

"Характеристика 1-го рівня СЕП НБУ

Система міжбанківських електронних платежів має трирівневу ієрархічну структуру.

На 1-му, верхньому рівні СЕП міститься Центральна розра-хункова палата. Вона обслуговується програмно-технічним ком-плексом АРМ-1, що виконує такі основні функції:

1) «пересилання» міжрегіональних електронних документів засобами електронної пошти Національного банку України;

2) перевірку правильності формування електронних документів;

3) формування й підтримання в робочому стані основних до-відників НБУ;

4) захист електронних документів і системи в цілому від не-санкціонованого доступу;

5) диспетчеризація (бухгалтерський технологічний контроль) проходження міжрегіональних платежів і синхронізація закриття дня банку.

Характеристика 2-го рівня СЕП НБУ. На 2-му рівні мережі перебувають регіональні розрахункові палати, які обслуговуються своїми програмно-технічними комп-лексами АРМ-2.

АРМ-2 — це програмно-технічний комплекс — ПТК,уста-новлений у РРП і призначений для обслуговування певної кілько-сті банків цього регіону та організації взаємодії з іншими АРМ-2. РРП може експлуатувати один чи кілька АРМ-2 залежно від кількості банків регіону та активності проведення ними міжбанківських платежів.

Кожне АРМ-2 забезпечує виконання таких основних операцій:

1) обмін електронними документами між самою РРП і банками — учасниками міжбанківських розрахунків;

2) формування та відправлення міжрегіональних платежів до ЦРП;

3) отримання міжрегіональних платежів від ЦРП та їх аналіз;

4) обмін електронними документами з іншими АРМ-2 своєї РРП.

5) захист електронних документів і їх обробка від несанкціо-нованого втручання.

Характеристика 3-го рівня СЕП НБУ. На 3-му, нижньому рівні СЕП перебувають учасники міжбан-ківських електронних розрахунків, які діють на підставі угод із РРП на проведення розрахунків та Положення про міжбанківські розрахунки в Україні згідно з Регламентом функціонування ме-режі розрахункових палат України. Учасниками електронних платежів можуть бути, і здійснювати за допомогою СЕП міжбан-ківські розрахунки, будь-які кредитно-фінансові підприємства й організації, котрі мають відкриті КР у відповідних РУ НБУ та за-довольняють вимоги, що їх висуває НБУ до учасників СЕП.

Юридичні особи ще не є учасниками мережі електронних пла-тежів і можуть користуватися її послугами лише через посеред-ництво безпосередніх «учасників», укладаючи з ними відповідні договори.

У розпорядження кожного з учасників платежів надається єдина копія програмно-технічного комплексу з умовною назвою АРМ-3(або інакше АРМ НБУ), через який банк обмінюється ін-формацією із СЕП за допомогою файлів,

структура та функціональне призначення яких визначені в документі «Інтерфейс між САБ і АРМ-3 системи електронних платежів (СЕП)».

АРМ-3 на рівні банку — учасника розрахунків забезпечує виконання таких основних операцій:

1) перевірку пакетів платіжних документів, які підготовлені панком, що експлуатує даний АРМ-3;

2) обмін електронними документами з відповідною РРП;

3) захист системи від несанкціонованого втручання. " [18]

4.4 Поняття та характеристика банківських електронних документів

4.4.1 Поняття банківських електронних документів

Банківський електронний документ являє собою повідомлення спеціально встановленого виду (формату) з інформацією про кошти їх перерахування. Зберігається на машинних носіях.

Учасник отримавши платіжні документи передає назад учаснику відправнику квитанцію з інформацією про характеристики первинного файлу та рішення позитивне чи негативне щодо прийняття обробки файлу.

"Банківські повідомлення у вигляді електронних документів мають задовольняти таким головним вимогам:

1. Бути підготовлені, передані та прийняті з використанням програмно-технічних засобів, які сертифіковані й затверджені НБУ.

Кожному електронному платіжному документу в АІС КБ автоматично присвоюється ідентифікатор, який включається до його складу і є унікальним у межах даної банківської установи протягом одного банківського дня.

2. Банківські електронні документи мають бути захищені спе-ціальними засобами, які надаються централізовано Національним банком України, згідно з Положенням про систему захисту електронних банківських документів в

обчислювальній мережі Наці-онального банку України та Положенням про арбітражні послуги служби захисту електронних банківських документів в обчислю-вальній мережі НБУ. Їх захист ґрунтується на використанні методів ідентифікації вузлів відправника та одержувача повідомлення, його шифрування і дешифрування на основі використання методів криптографії у вузлах адресатах, а також під час передавання по каналах ЕП, накладання електронного підпису й авторизації відправника та одержувача електронного банківського до-кумента. " [18]

4.4.2 Загальна характеристика програмних та апаратних методів захисту електронних документів

Банківські електронні документи повинні бути захищеними засобами, які надає Національний банк України, згідно з положеннями про арбітражні послуги та систем захисту ЕБД (електронні банківські документи) в обчислюваних мережах НБУ.

"Для шифрування і дешифрування ЕД застосовуються:

Програмні методи - в АРМ-3 комерційних банків використовується програма шифрування і дешифрування з іменем TRESOR. Вона встановлюється для кожного КБ і його АРМ-3 індивідуально, захищена від можливості копіювання і працює (шифрує або розшифровує підготовлені чи отримані ЕД) з використанням спеціальних індивідуальних «ключів», серед яких не-має двох однакових (їх через певний проміжок часу змінює служба безпеки НБУ).

Апаратні методи - система використання апаратного захисного обладнання так званих модулів шифрування, які працюють з використанням шифрувального «ключа», що міститься на спеціальній пластиковій картці. Цю картку (вона має вбудований мікропроцесор і забезпечує високий рівень захи-сту «ключів») видають відповідальним працівникам банку, які мають право підпису банківських платіжних документів.

Використання самої картки передбачає введення додаткової системи паролів для авторизації її користувача.

Крім того, у СЕП існує також система захисту платіжних документів, яка ґрунтується на проведенні постійного оперативного банківського обліку, контролю та аналізу обсягів і напрямів руху і грошових коштів, які «несуть» ЕД на всіх етапах маршруту їх переміщення. " [18]

4.4.3 Загальна характеристика інформаційних потоків в СЕП НБУ

Під час роботи в системі електронних платежів в ній знаходяться інформаційні потоки різного призначення. Найголовнішим є потік інформації з файлів платіжних документів які відповідають за перенесення грошових коштів.

"Файли-квитанції, які забезпечують і підтверджують правильність проходження потоків платіжних документів, у своїй сукупності створюють потоки підтвердження платежів і є другими після них за потужністю.

Така складна система, як СЕП потребує високого рівня синхронізації роботи її елементів, тому в системі існують потоки зазначеної синхронізації. Файли цих потоків несуть у собі повідомлення ЦРП (воно регламентує регіональним ланкам СЕП характер технологічного режиму та його зміну), а також дані про вибрані режими роботи елементів системи.

У системі електронних міжбанківських платежів циркулюють також потоки аварійних сигналів і контрольної інформації, що присутні на всіх її рівнях. " [18]

В системі електронних платежів банківська інформація захищається за допомоги комплексу дій пов’язаних із шифруванням яка знаходиться в системі. Шифруванню підлягають усі файли СЕП.

"Усі платіжні документи СЕП перед відправленням з банку обробляються апаратно-програмними засобами захисту інформації, що забезпечують виконання таких вимог з точки зору безпеки інформації:

- інформація, що передається, має бути закритою, тобто повідомлення може бути прочитане лише тим, кому воно адресоване;
- цілісність — випадкове чи навмисне пошкодження повідомлення на етапі його передачі буде виявлене під час його прийому;
- автентичність відправника (під час прийому повідомлення можна однозначно визначити, хто його відправив).

Крім перерахованих основних вимог, необхідно виконувати низку допоміжних, що дає змогу більш детально аналізувати можливі нестандартні ситуації:

- засобами захисту інформації ведеться шифрований арбітражний журнал, в якому зберігається протокол обробки інформації, а також вміст файлів, що обробляються;
- у шифроване повідомлення включені поля дати та часу обробки.

В основу роботи засобів захисту інформації в СЕП покладено алгоритм шифрування із закритими ключами відповідно до ДЕСТ 28147-89. Цей метод характеризується високою надійністю з точки зору його дешифрування, але ставить дуже високі вимоги до процедури транспортування та зберігання закритих ключів, секретність яких забезпечує на практиці стійкість системи шифрування.

Основними засобами захисту інформації в СЕП є апаратні засоби. Секретність ключів у них забезпечується технологічно:

- ключі зберігаються в спеціальній електронній картці, прочитати їх можна тільки за допомогою спеціального блоку, що виконує процес шифрування інформації. Прочитати ключі іншими засобами неможливо;
- електронна картка видається банку з попередньою прив’язкою її до конкретного блоку шифрування цього ж банку; втрачена чи викрадена картка

не буде працювати в іншому шифро-блоці (наприклад, в апаратурі іншого банку);

- у випадку крадіжки одночасно блоку і картки у конкретного банку передбачено режим виключення цієї апаратури зі списку користувачів СЕП; банк може продовжити роботу в СЕП після вирішення юридичних та фінансових питань, пов’язаних з втратою апаратури та отриманням нового комплексу. " [19]

ВИСНОВОК

В першому розділі мною були визначені основні поняття технічного захисту інформації в банківських системах. Були визначені основні задачі та цілі, які необхідно вирішити системі технічного захисту інформації.

В другому розділі було описано, які технічні канали витоку можуть знаходитися в банківських системах та на об’єктах інформаційної діяльності. Були розглянуті моделі загроз систем технічного захисту інформації та моделі разом з класифікацією порушників.

В третьому розділі було проведено дослідження та моделювання відділення ТВБВ №10003/0467 АТ «Ощадбанк». Описано основні завдання відділення та його структуру. Розроблено план відділення як об’єкту захисту. Були зібрані та наведенні результати обстеження приміщення. Огляд та опис технічних засобів які використовуються у відділенні.

В четвертому розділі на основі проведеного технічного аналізу були наданні рекомендації щодо застосування нового обладнання та програмного комплексу.

Підводячи підсумки в даній роботі було спроектовано сучасна система аналізу технічної і фізичної охорони відділення ТВБВ №10003/0467.

В кінці хочу додати, як би добре не була захищена система, все одно вона буде вразлива. Блокуючи підступи до одних каналах витоку, інші залишаються менш захищеними. Так само можна відзначити, що зловмисники теж не сидять на місці, коли удосконалюється та чи інша система захисту вони вдосконалюють методи злому і проникнення. Кожна система має «двері», через яку входять авторизовані користувачі системи, і зловмисники цим користуються, як би добре не була захищена «двері» вона в будь-якому випадку відкривається. Потрібно пам'ятати, що не потрібно будувати дорогу системи на тому місці, де охороняється інформація не настільки важлива, потрібно раціонально розподіляти кошти по всій системі і підсилити захист в тих місцях, де це дійсно потрібно.

СПИСОК ПОСИЛАНЬ

1. http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=44842
   Семінар “Захист інформації в інформаційно-телекомунікаційних системах
   та на об'єктах інформаційної діяльності” Степанов Володимир Дмитрович, начальник Головного управління технічного захисту інформації ДСТСЗІ СБ України.
2. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=020061DB2719E6510453B1278E814097?art_id=51431&cat_id=38710
   Аналіз регуляторного впливу проекту “Положення про державний контроль за станом технічного захисту інформації”
3. http://dspace.onua.edu.ua/bitstream/handle/11300/11111/%D0%9E%D0%86%D0%91%20%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf?sequence=1&isAllowed=y
   Заплотинський Б.А. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
4. https://studfile.net/preview/7475501/page:16/ Возненко А. Д. Стасюк О. І,Коваль Ю. О. «Основи захисту інформації».
5. http://www.100balov.com/data/ukr/Materialij_po_navchannu_pakynok_12/ROMAKA_2.doc
6. https://helpiks.org/6-26905.html
7. http://5fan.ru/wievjob.php?id=39490 Проектування системи аналізу технічного захисту і фізичної охорони об’єкта (на прикладі ТОВ «Ласунка»)
8. http://a.lekciya.com.ua/pravo/726/index.html?page=6
9. https://zakon.rada.gov.ua/laws/show/2121-14 ЗАКОН УКРАЇНИ Про банки і банківську діяльність
10. https://sirius.kiev.ua/datchik-ruhu

11. http://www.ohrana-ua.com/articles/814-spovschuvach-v-sistem-ohoronnoyi-signalzacyi-chastina-1.html
12. http://www.klaster-plus.ua/ua/shop/ohranno-pozharnaya-signalizaciya/datchiki-ops/datchiki-razbitiya/
13. https://auchan.ua/ua/besprovodnoj-datchik-razbitija-stekla-ajax-glassprotect-chernyj-249829/?gclid=CjwKCAiAluLvBRASEiwAAbX3GWWaqN9bxSYlG-EoO1laW2xVyxk2K1dfvzCH0FeIucqd5tYJg5HpHRoCM_UQAvD_BwE
14. http://www.klaster-plus.ua/ua/shop/ohranno-pozharnaya-signalizaciya/pozharnye-datchiki/datchiki-dymovye/
15. https://buklib.net/books/25510/
16. https://old.bank.gov.ua/control/uk/publish/article?art_id=53859&cat_id=36045
17. https://zakon.rada.gov.ua/laws/term/ru/27227:37782/sp?sp=s:max20
18. https://studopedia.com.ua/1_51308_harakteristika-strukturi-sep-nbu.html
19. http://ru.osvita.ua/vnz/reports/bank/20375/
20. http://www.dut.edu.ua/uploads/n_7756_35369915.docx

ЗАХИСТ ІНФОРМАЦІЇ В БАНКІВСЬКИХ СИСТЕМАХ ТА НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ Реков Дмитро Валерійович