МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

 ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**ЛАБОРАТОРНА РОБОТА №2**

Роботу виконала:

студентка групи ПМІ-44,

 Ковальчук С. А.

Львів ЛНУ 2020

Тема: Дослідження методів захисту інформації на підприємстві.

Мета: Отримати навички щодо аналізу та вибору різних аспектів захисту інформації підприємства.

**Хід виконання лабораторної роботи**

1. Зі списку, наведеного у завданні до лабораторної, я обрала Варіант 10: Підприємство з обробки алмазів. Дане підприємство займається обробкою видобутих алмазів.
2. Правовий захист інформації:

* Проаналізувавши з [джерел](http://search.ligazakon.ua/l_doc2.nsf/link1/JG3TH00A.html), яким законам та стандартам України у галузі ІБ повинно підпорядковуватись підприємство, варто зазначити, що підприємства з каменообробки в Україні повинні підпорядковуватись закону від **28.05.2014 № 4949, який** відповідно до Конституції України визначає основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, системи суб'єктів забезпечення інформаційної безпеки та засади їх функціонування в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору.

### Проаналізувавши класи інформаційної системи підприємства відповідно до “Помаранчевої книги”, я зробила висновки, що підприємство з обробки алмазів належить до класу В2, а саме структурованого захисту. Усі вимоги класу [В1](https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D1%96%D1%97_%D0%BE%D1%86%D1%96%D0%BD%D0%BA%D0%B8_%D0%B7%D0%B0%D1%85%D0%B8%D1%89%D0%B5%D0%BD%D0%BE%D1%81%D1%82%D1%96_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D1%97_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8) мають виконуватися для системи класу В2. У системах класу В2 TCB заснована на чітко визначеній і формально задокументованій моделі, в якій управління доступом поширюється на всі суб'єкти й об'єкти даної системи автоматичної обробки даних. Крім цього, має бути проведений аналіз, пов'язаний із наявністю побічних каналів витоків. Необхідно провести розбивку структури TCB як за критичними із погляду захисту елементами, так і за некритичними. Інтерфейс TCB добре визначений, а її проект і реалізація виконані так, що вони дозволяють проводити ретельне тестування і повний аналіз. Механізми аутентифікації посилені, управління захистом передбачається у вигляді засобів, що призначаються для адміністратора системи і для оператора, а на управління конфігурацією накладаються жорсткі обмеження. Система відносно стійка до спроб проникнення в неї.

* Щодо напрямків та механізмів забезпечення ІБ на підприємстві відповідно до специфіки роботи підприємства та правових норм України, то я вважаю необхідним укладення договорів між замовниками та виконавцями щодо кожного проєкту, взятого виробництвом. Загалом ж організація повинна дотримуватися існуючих законів, та повинна дати собі відповідь за допомогою керуючих органів на наступні питання:
  1. Хто має право доступу до об'єктів, підтримуваних сервісом?
  2. За яких умов можна читати і модифікувати дані?
  3. Яким чином організовано віддалений доступ до сервісів підприємства?

1. Адміністративний захист інформації

Розробка комплексної системи захисту інформації на підприємстві або окремих заходів щодо її доповнення є необхідною на підприємстві такого типу, адже окрім інформаційних ресурсів також важливим є збереження ресурсу без зайвих втрат на підприємстві.

* Дослідивши основні заходи організаційного рівня, що діють на підприємстві, я вирішила, що підприємству з обробки алмазів буде характерно підключити принцип розділення обов’язків та принцип мінімізації привілеїв.
* Обґрунтувати вибір принципів керування персоналом підприємства можу наступним чином: перший принцип зобов’язує так розподіляти ролі і відповідальність, щоб одна людина не могла порушити критично важливий для організації процес. Наприклад, процедурні обмеження дій суперкористувача. Можна штучно “розділити” пароль суперкористувача, повідомивши першу його частину одному співробітнику, а другу – іншому. Тоді критично важливі дії з адміністрування ІС вони зможуть виконати тільки удвох, що знижує вірогідність помилок і зловживань.  
  Другий же полягає у виділенні користувачам тільки тих прав доступу, які необхідні їм для виконання службових обов’язків. Призначення цього принципу очевидне – зменшити збиток від випадкових або навмисних некоректних дій.
* Також опісля я обрала за належне наступні заходи фізичного захисту та керування доступом:
  1. контролювати і, в разі необхідності, обмежувати вхід і вихід співробітників і відвідувачів (зокрема для планових перевірок у разі втрати сировини на підприємстві);
  2. виключити можливості таємного проникнення на територію та у приміщення сторонніх осіб;
  3. забезпечити зручність контролю проходу і переміщення співробітників і відвідувачів;контролювати і, в разі необхідності, обмежувати вхід і вихід співробітників і відвідувачів;
  4. створити окремі виробничі зони за типом конфіденційних робіт із самостійними системами доступу;
  5. контролювати дотримання часового режиму праці і перебування на території персоналу фірми;
  6. організувати і підтримувати надійний пропускний режим.
  7. захищати устаткування від крадіжок і пошкоджень. Для підтримки доступності слід вибирати устаткування з максимальним часом напрацювання на відмову, дублювати важливі вузли і завжди мати під рукою запчастини;
  8. захист від перехоплення даних можна забезпечити використанням криптографії, максимальним розширенням контрольованої території, контролем лінії в’язку (наприклад, укладати їх в надувну оболонку з виявленням проколювання). Однак найрозумніше – усвідомити, що для комерційних систем забезпечення конфіденційності є все-таки не головним завданням;

Загалом підсумуючи, при виборі засобів фізичного захисту слід проводити аналіз ризиків. Так, ухвалюючи рішення про закупівлю джерела безперебійного живлення, необхідно врахувати якість електроживлення в будівлі, займаній організацією, характер і тривалість збоїв електроживлення, вартість доступних джерел і можливі втрати від аварій (поломка техніки, припинення роботи організації тощо). В той же час, у багатьох випадках рішення очевидні. Заходи протипожежної безпеки обов'язкові для всіх організацій. Вартість реалізації багатьох заходів (наприклад, установлення звичайного замка на двері серверної кімнати) мала або явно менша, ніж можливий збиток.

* Якщо поміркувати щодо правил заохочення та покарання працівників, що стосуються порушень інформаційної безпеки, то можна зробити наступні висновки:

Заходи реагування на порушення режиму безпеки повинні забезпечити:

* локалізацію інциденту і зменшення шкоди, що завдається;
* виявлення порушника;
* попередження повторних порушень.

В організації повинна бути людина, доступна 24 години на добу (особисто, по телефону або електронній пошті), яка відповідає за реагування на порушення. Всі повинні знати координати цієї людини і звертатися до неї при перших ознаках небезпеки. Загалом, як при пожежі, потрібно знати, куди дзвонити, і що робити до приїзду пожежної команди.

Часто вимога локалізації інциденту і зменшення шкоди, що завдається, вступає в конфлікт з бажанням виявити порушника. В політиці безпеки організації пріоритети повинні бути розставлені наперед.

Щоб запобігти повторним порушенням, необхідно аналізувати кожен інцидент, виявляти причини, накопичувати статистику. Які джерела шкідливого ПЗ? Які користувачі мають звичай вибирати слабкі паролі? На подібні питання і повинні дати відповідь результати аналізу.

* Наостанок я розробила спрощену структуру служби безпеки заданого підприємства, з урахуванням його структури, діяльності, оцінених ризиків та політики безпеки.

Служба безпеки є самостійною організаційною одиницею підприємства, що підкоряється безпосередньо керівнику підприємства. Очолює службу безпеки начальник служби в посаді заступника керівника підприємства з безпеки.

Організаційно служба безпеки складається з таких структурних одиниць:

* підрозділу режиму й охорони;
* спеціального підрозділу обробки документів конфіденційного характеру;
* інженерно-технічного підрозділу;
* інформаційно-аналітичного підрозділу.

У такому складі СБ здатна забезпечити захист конфіденційної інформації від будь-яких загроз.

1. Інженерно-технічний захист інформації

Дослідивши інженерно-технічні рішення щодо захисту підприємства відповідно до розробленої політики безпеки, я вважаю за потрібно ввести на підприємстві такого типу:

* Контроль території підприємства (встановлення сигналізації, охоронного телебачення та освітлення, посилення бар’єру у вигляді ґрат та високих парканів, в’їзд на територію за спецпропусками);
* Контроль за пересуванням персоналу за допомогою охоронного телебачення на території підприємства;
* Технічні засоби захисту (відеоспостереження, пожежна сигналізація, магнітні картки для автентифікації на вході тощо);

1. Програмно-технічний захист інформації

Для захисту підприємства відповідно до розробленої політики безпеки я вирішила запропонувати наступні програмні рішення:

* антивірусний контроль (пакети антивірусного захисту Trend Micro NetSuite, Symantec Multi-Tier Protection, Kaspersky Total Space Security; Dr.Web Enterprise Suite, Eset тощо);
* шифрування вхідних та вихідних даних підприємства, встановлення систем розпізнавання працівників (користувачів системи), перевірка ідентифікаторів користувачів під час обміну великими обсягами даних;
* автентифікація на робочому місці та пропуск до конкретних секторів підприємства через пропуски певних рівнів з різними правами доступу.

Повторно оцінивши ризики з урахуванням всіх запропонованих організаційних та інженерно-програмних рішень, я можу стверджувати, що єдиною прогалиною у системі все ж залишиться людський фактор, який не дозволить системі даного класу стати найвищою мірою стійкою відносно спроб проникнення в неї.

Висновки: ефективність запропонованого захисту відносно початкового рівня захисту дасть змогу ускладнити можливість проникнення зловмисників у систему та фізичні приміщення підприємства у півтора рази. Подальше вдосконалення захисту підприємства немає сенсу, адже це лише значно підвищить фінансові витрати компанії без уникнення бажаної можливості захистити підприємство найвищою мірою.