**ЗВІТ З ЛАБОРАТОРНОЇ РОБОТИ №1**

**дисципліна «Захист інформації»**

**тема «Політика безпеки»**

**студента групи ПК-15-1**

**Гулого Тараса Олександровича**

# 1. Постановка задачі

Розробити політику безпеки для будь-якої інформаційної системи (за своїм вибором).

# 2. Опис інформаційної системи

Приватне ательє «Водевіль», яке спеціалізується на пошивці чоловічої, жіночої та дитячої одежі, консультації по ремонту та пошиву сценічного одягу, має один багатокористувацький комп’ютер. Комп’ютер під’єднується до мережі лише один раз у місяць для здачі місячної або квартальної звітності через програмне забезпечення «M.E Doc». Також на підприємстві використовується пакет безкоштовного програмного забезпечення «Open Office.org» для ведення бази даних, підрахунку зарплатні, видачі товарних чеків та формування звітів.

У ательє працюють наступні працівники, які користується спільним комп’ютером: директор, спеціаліст, головний бухгалтер. Функції, які виконують працівники занесені у таблицю 1.

|  |  |
| --- | --- |
| Працівник | Призначення |
| Директор | аналіз роботи підприємства, планування діяльності, видача деяких додаткових документів і.т.д.. |
| Головний бухгалтер | Розрахунок заробітної плати, облік виконаних послуг, введення складу, облік грошових операцій з клієнтами, облік грошових витрат ательє, формування звітності до податкової інспекції. |
| Спеціалісти | Прийом замовлень, реєстрація клієнтів, проведення грошових операцій. |

*Табл1 Функції працівників, які мають доступ до персонального комп’ютера.*

Для роботи з клієнтами на кожне замовлення генерується унікальний п’яти значний номер за яким можна отримати своє замовлення, якщо клієнт зробить більш ніж три замовлення для нього генерується постійний код завдяки якому клієнт може отримати знижку.

Для захисту від несанкціонованого взлому в фойє закладу встановлена камера відеоспостереження, після завершення робочого дня вмикається сигналізація і на комп’ютері встановлено пароль із 6 літер.

Будівля ательє розташована у спальному районі міста у торгівельному комплексі, який складається з окремих невеликих панельно-каркасних споруд. Відкриття торгового комплексу відбулося нещодавно тому проводка і опалювальна система тільки почали працювати. До найближчого ательє один кілометр, але конкуруюча фірма «Fashion&Cow» планує відкриття свого ательє в тому ж самому комплексі.

# 2. Аналіз загроз

## 2.1 Порушення конфіденціальності системи

Так як фірма є відкритою вдень до порушення конфіденціальності можемо віднести такі загрози:

* Передача конфіденціальної інформації під час діалогів (спілкування с клієнтом, спілкування про робочі аспекти в людних місцях, розголошення таємних технологій, розголошення інформації про постачальників матеріалів.)
* Передача копій або скріншотів конфіденціальних документів, корпоративних таємниць, паролів від обчислювальних приладів тощо
* Необережне поводження з носіями інформації.
* Публікування документів фірми у відкритий доступ в мережі інтернет.
* Мережеві атаки на обчислювальний прилад системи під час здачі звітності.
* Порушення системи та крадіжка інформації в неробочий період.
* Витік інформації через незахищеність програмного забезпечення яким користується фірма.

Данні загрози можливі через недбале поводження з інформацією розголошення її вголос стороннім суб’єктам, недбале поводження з обчислювальним приладом, необережність під час роботи в мережі інтернет, а також через використання неперевіреного або неліцензійного ПО та через відсутність будь-яких захисних програм в операційній системі обчислювального приладу.

## 2.2 Порушення цілісності системи

Зважаючи на те що приміщення у якому знаходиться обчислювальний прилад перебуває під цілодобовим наглядом охоронної фірми можливість фізичного пошкодження інформації через незаконне втручання у будівлю можна виключити.

Як і у попередньому випадку порушення цілісності інформації може відбитися через недбалість працівників або через помилку у фізичних логічних процесах самого приладу.

Такі помилки можуть ставатися через неправильні конфігурації програми, перевантаження окремих фізичних компонентів, завантаження неперевірених файлів та встановлення неперевірених програм у операційну систему.

Основні порушення цілісності можуть відбуватися під час сеансу з’єднання з податковою

## 2.3 Аналіз програм інформаційної моделі

**M.E.d.o.c** – українське програмне забезпечення для електронного документообігу. Програма прийшла на заміну старшої системи «Бест Звіт Плюс», яку з 1998 року розробляло ТОВ «БЕСТ ЗВІТ». За словами розробників, вони стали «першою та єдиною» компанією в Україні, яка створила можливість подачі звітності в електронному вигляді в державні контролюючі органи.

Як зазначено на офіційному сайті «M.E.doc=Надійність». В програму вбудовано засіб криптографічного захисту за допомогою цифрового підпису, який відповідає всім вимогам законодавства.

Для забезпечення конфіденціального зв’язку усі повідомлення шифруються за допомогою криптографічного алгоритму який затверджено державою (ДСТУ ГОСТ 28147:2009). Для шифрування використовується свій окремий відкритий сертифікат ключа шифрування, який не використовується для накладання підпису.

Сервер електронного документообігу (СДО) є окремою гордістю фірми адже він:

* Забезпечує автентифікацію контрагента тільки по унікальному поєднанню полій ЕДРПОУ + код філіалу
* Доступ до документів можливий тільки після входу в систему з діючими сертифікати ЕЦП (електронного цифрового підпису).
* Не потрібно знати електронну пошту контрагента
* Не потрібно зв’язуватися з контрагентом для передачі документів.
* Документ передається автоматично на прийомі пошти в програмі.

Сервер використовує HTML або e-mail зв’язок в залежності від швидкості інтернету.

Не дивлячись на всі міри збереження даних M.E.doc виявися уразливим зі сторони вихідного коду адже саме завдяки необачності працівників фірми на Україні сталася наймасштабнішою інформаційна катастрофа.

На початку року більшість користувачів програми M.E.doc які встановили оновлення програми стали жертвами вірусної атаки криптографічного вірусу відомого під іменами NePetya, Petya.A, ExPetya и WannaCry-2.

Хакери внесли зміни до динамічної бібліотеки яка працювала з регістром HKCU\SOFTWARE\WC. Саме такий самий регістр використовується і вищезгаданими вірусами.

**OpenOffice.org –** вільний у доступі пакет офісних застосунків. На відміну від Microsoft Office є безкоштовним та має код у відкритому доступі. Даний офісний пакет стає більш популярним і його починають використовувати в школах, вузах, державних бюджетних та комерційних організаціях.

Розробники програми дуже серйозно ставляться до захисту програми тому с кожним оновленням команда закриває всі можливі «дірки» у захисній системі програми. Записи всіх можливих проблем у програмі які було виправлено можна переглянути у вільному доступі.

В деяких програмах даного офісного пакету є захисні функції (зашифрування бази даних, встановлення паролю на документи).

# 3. Модель порушника

Розглянемо таких порушників

1) **Аматор –** особа яка намагається взламати інформаційну систему лише заради досвіду у даній сфері діяльності. Аматори зазвичай не мають бюджету атаки тому використовують безкоштовне програмне забезпечення.

В даному випадку аматор може спромогтися вкрасти деяку річ за допомогою підробки унікального п’яти значного номеру, перехопити повідомлення під час сеансу з’єднання з сервером програми M.E.doc за допомогою методу *ARP-sproofing*, підбор паролів за допомогою програм *BrutusA2* чи *Raptor* під час інтернет сеансу, відправка троянів за допомогою яких проводяться D-Dos атаки чи накручується криптовалюта.

2) **Професіонал –** особа яка взламує систему за для грошової вигоди тому використовує професійні інструменти. На відміну від аматора професіонали не будуть використовувати безкоштовні програми, а із бюджетом можуть розробити власні програми та використовувати власні застосунки.

Професіонал може написати фальшиве оновлення однієї із програм з шкідливими вмістом який потім буде вимагати гроші з зараженого комп’ютера, сканування жорсткого диск комп’ютера та збір «сміття» за допомогою програми *Actual Spy*, часткове або повне викрадення бази даних за допомогою програми *The Fat Rat* з підбором паролю за допомогою *OpenOffice Password Cracker*. Фальсифікування контрольних сум електронного підпису за для перехоплення документів

3) **Хакер найнятий конкурентами –** особи, які саботують роботу даної фірми за для забезпечення процвітання конкуруючої фірми. Зусилля даного типу порушників направлені на дестабілізацію інформаційної системи фірми та порушення внутрішнього документообігу фірми. Дані особи мають деякий бюджет, який конкуруюча фірма виділяє на реалізацію хакерської атаки.

Для дестабілізації системи хакер може використовувати вірус атаки з вірусами *Petya* чи іншими шифрувальними троянами, пошкодження бази даних після несанкціонованого доступу який був описаний вище. і.т.д

# 4. Політика безпеки

## 4.1 Політика безпеки до атаки

1. Обов’язкове встановлення паролів на всі документи фірми, на облікові записи та операційну систему в цілому. Паролі повинні складатися з речення із 4 або більше слів написаних в англійській розкладці. При такому підборі пароля ентропія підвищиться значно у порівнянні з паролем складеним із ллітер.
2. Встановлення антивірусного програмного забезпечення, фаєрволу та додаткових програмних забезпечень для захисту окремих папок. У цей пункт також входить щорічна або щопіврічна перевірка на віруси, та своєчасне оновлення захисного програмного забезпечення.
3. Користування лише перевірними та ліцензійними засобами захисту. Серед безкоштовних антивірусних програм можна обрати AVG, вбудований фаервол у Windows чи Linux, [AxCrypt](http://www.melinfo.ru/detailfile.php?id=155) для безкоштовного програмного шифрування даних.
4. Використовувати підпис на чеках та талонах на видачу товару. Данна міра забезпечить від підробки унікальних талонів на видачу товару.
5. Аналізувати кожне оновлення операційної системи чи програми Читати відгуки про оновлення та новини, перевіряти легальність оновлення.
6. Перевіряти кількість користувачів активних у певний період часу для запобігання неавторизованих користувачів.
7. Резервне збереження ключових даних на комп’ютері.
8. Бажаний перехід на безкоштовну операційну систему Linux так як кількість вірусів на ній значно менша.

## 4.2 Політика безпеки під час атаки

Так як комп’ютер не є сервером бажано відімкнути його від електромережі або від інтернету для у разі перехоплення повідомлення для завершення всіх нелегальних процесів.

Якщо атака є фізичною бажано викликати правозахисні органи до місця злочину порушення інформації.

## 4.3 Політика безпеки після атаки

1. Відновлення втрачених даних та перевірка цілісності існуючих даних. Якщо у операційній системі була встановлена функція відновлення за датою то можна нею скористатися. Або відновлення даних через резервну копію.
2. Зміна всіх паролів які були встановлені користувачами.
3. Зміна методу шифрування даних.
4. Відкат програмного забезпечення до функціонуючої версії.
5. Звернення до служби підтримки програмного забезпечення.
6. Проведення непланової перевірки комп’ютера на вірусні програми.

## 4.4 Аналіз місць ураження даних

У даному випадку треба викликати спеціаліста для проведення детального аналізу місця у якому система була уражена. Для запобігання повторного ураження рекомендуються замовити незацікавлену фірму для проведення ряду атак які можна контрольовано видалити.