Проектирование системы информационной безопасности отдела продаж ООО «Э.П.Ф.» с применением программно-аппаратных средств защиты информации

Соколова Я.П.
информатика
3 курс, Многопрофильный колледж ФГБОУ ВО «ТГТУ», г. Тамбов, Тамбовской области
Научный руководитель: Мосягина Н,Г., Многопрофильный колледж ФГБОУ ВО «ТГТУ», г. Тамбов, Тамбовской области

ВВЕДЕНИЕ

С каждым днем тенденция зависимости человечества от информационных технологий и ресурсов неумолимо растет, однако, вместе с ней увеличивается количество угроз безопасности и целостности данных. Именно поэтому в последние годы информационная безопасность является одной из самых актуальных и важнейших в современном мире тем.

Информационная безопасность – одна из важнейших составляющих работы любого предприятия или организации. На данный момент существует множество способов защиты информации, такие как использование шифрования данных, создание надежных паролей, использование процедур аутентификации и идентификации, установка обновлений безопасности на компьютеры и программное обеспечение, ограничение физического доступа к важным данным, обучение сотрудников предприятия правилам информационной безопасности.

Цель работы: изучить возможности современных программно-аппаратных средств защиты информации, осуществить проектирование системы информационной безопасности отдела продаж предприятия ООО «ЭПФ» [1].

Задачи исследования:

— оценить вероятные угрозы информационной безопасности объекта информационной защиты;

— сформировать требования к системе информационной безопасности;

— осуществить выбор программных и программно-аппаратных средств системы информационной безопасности;

— разработать систему информационной безопасности отдела продаж ООО «ЭПФ» с использованием программных и программно-аппаратных средств защиты информации.

В качестве средства проектирования используется программный комплекс ViPNet Client 4.

Основная часть.

Характеристика объекта информационной защиты.

Основная сфера деятельности компании ООО «Э.П.Ф.» – оптовая неспециализированная торговля. Данная компания является поставщиком техники, запасных частей и агрохимии сельхозпроизводителям. Предприятие обеспечивает сервисное обслуживание и ремонт сельскохозяйственной техники.

В сети предприятия обрабатывается и хранится информация разных уровней конфиденциальности: персональные данные, коммерческая тайна (деловая, техническая информация) и программное обеспечение компьютеров.

Определение модели вероятного нарушителя.

Вероятные нарушители информационной безопасности предприятия можно разделить на две основные категории:

— внешние нарушители, осуществляющие атаки из-за пределов контролируемой зоны предприятия, к таковым относятся бывшие сотрудники и посторонние лица, которые могут нанести ущерб, перехватывая информацию или атакуя системы удаленно;

— внутренние нарушители, которые осуществляют атаки, находясь в пределах контролируемой зоны предприятия, к ним относятся нынешние сотрудники предприятия.

Оценка угроз информационной безопасности.

В ходе работы были рассмотрены угрозы информационной безопасности [2]. На основе рассмотренных угроз была рассчитана

вероятность их реализации и сформирована модель информационной безопасности. В результате анализа информационной системы по Методике ФСТЭК от 14 февраля 2008 года [3] был сделан вывод о том, что объект исследования обладает средним уровнем исходной защищенности и наиболее вероятными угрозами являются:

— осуществление необнаруженной несанкционированной модификации целевой информации;

— преднамеренные действия сотрудников, допущенных к материальным, финансовым ресурсам, приводящие к затратам ресурсов, утратам и хищениям;

— просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации;

— использование информации идентификации/аутентификации, заданной по умолчанию;

— осуществления несанкционированного доступа к компьютерам;

— внедрение вредоносного программного обеспечения в сеть предприятия.

Проектирование системы и технологии обеспечения информационной безопасности отдела продаж ООО «ЭПФ».

Исходя из требований информационной безопасности для предприятия, был произведен выбор программных средств для защиты информации от несанкционированного доступа и ее утечки. Основой для построения системы защиты послужил программный комплекс VipNet [4].

Программный комплекс ViPNet Client 4 предназначен для защиты рабочих мест корпоративных пользователей. Он надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика, обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, что необходимо для предприятия ООО «ЭПФ», имеющее филиалы в нескольких городах России.

Для обеспечения защиты информации от несанкционированного доступа с помощью VipNet Client 4 был выполнен ряд действий:

— создание клиентов и пользователей;

— создание электронной цифровой подписи (ЭЦП).

Создание клиентов в VipNet Client.

Для создания нового клиента необходимо открыть VipNet Administrator с правами администратора и на вкладке Клиенты нажать кнопку создания нового клиента.

В окне Новый клиент произведен выбор координатора и проставлен переключатель «Создать одноименного пользователя на новом узле автоматический».

На вкладке Связи с узлами автоматически были созданы связи между данным клиентом и центральным координатором, и администратором сети, также были созданы связи с координатором 1 и одним из клиентов. Настроены роли клиента, адреса во внешней сети и выполнена настройка межсетевого экрана, согласно параметрам с сервера IP-адреса клиента. Создан пароль администратора на основе парольной фразы для доступа к сетевому узлу клиента, а также установлен его срок действия на 365 дней (рисунок 1).

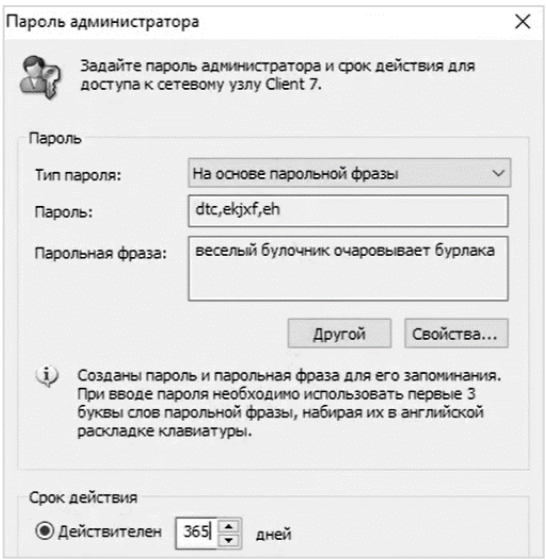

Рисунок 1 – Установка пароля администратора

В качестве завершения создания клиента ему был выдан новый дистрибутив ключей.

Создание электронной цифровой подписи в VipNet.

Для создания электронной подписи в программный пакет VipNet предусмотрена программа Создание запроса на сертификат. После запуска утилиты необходимо настроить Параметры сертификата согласно рекомендациям. Был выбран криптопровайдер, алгоритм шифрования, назначение сертификата (рисунок 2).

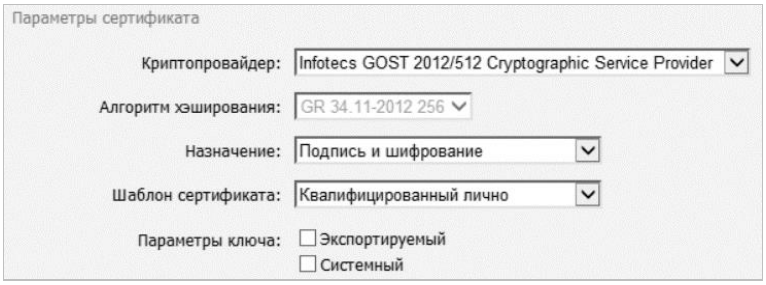

Рисунок 2 – Настройка параметров сертификата

Далее были заполнены Данные о владельце сертификата. В поле сохранения запроса выбрано удобное место сохранения запроса (рисунок 3).

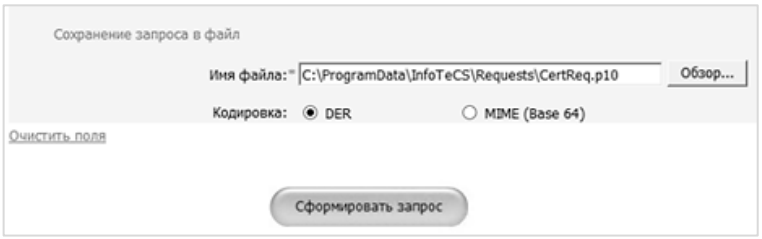

Рисунок 3 – Формирование и сохранение запроса

В результате выполения данных операций появится окно «ViPNet CSP – инициализация контейнера ключей», в котором будет сформировано имя контейнера ключа (рисунок 4).

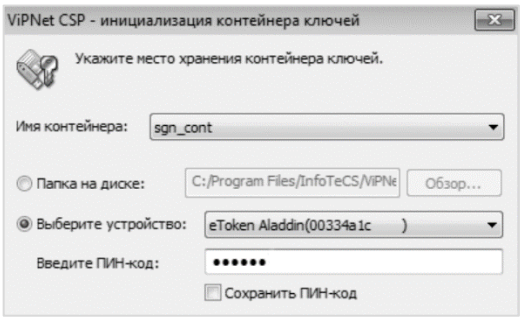

Рисунок 4 – Окно ViPNet CSP – инициализация контейнера ключей

Запрос успешно создан и сохранен в указанную ранее папку, а контейнер электронной подписи (закрытый ключ) успешно размещен в памяти токена.

Защита баз данных.

В качестве защиты баз данных предприятия была установлена парольная защита на доступ к данным, хранящимся в программе «1С: Предприятие 8». Для того, чтобы автоматизировать механизм генерации пароля и повысить безопасность аккаунтов сотрудников в работе была использована программа, написанная на языке программирования C++, которая генерирует уникальные и сложные пароли с помощью использования комбинации букв латинского алфавита верхнего и нижнего регистра, цифр и специальных символов. Программа позволяет создавать необходимое количество паролей в текстовый файл, что удобно для хранения и управления большим количеством паролей. Кроме того, в программе реализована возможность указания длины пароля. Фрагмент кода данной программы представлен на рисунке 5.

```cpp
#include <iostream>
#include <fstream>
#include <random>
#include <Windows.h>
using namespace std;

class PassGen {
public:
    void displayMessage()
    {
        int passLength;
        int numOfPasswords;
        char filename[100];
        cout << "Введите длину пароля для генерации: ";
        cin >> passLength;
        cout << "Введите количество паролей для генерации: ";
        cin >> numOfPasswords;
        cout << "Введите имя файла для записи: ";
        cin >> filename;
        ofstream outFile(filename);
        for (int k = 0; k < numOfPasswords; k++)
        {
            char* generatedPassword = passwordGenerator(passLength);
            outFile << generatedPassword << endl;
        }
        outFile.close();
        cout << "Пароли успешно сгенерированы и записаны в файл " << filename << endl;
    }

    char* passwordGenerator(int passLength) {
        char alphabet[] = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*";
        char* password = new char[passLength + 1];
        random_device rd;
        mt19937 generator(rd());
        uniform_int_distribution<int> distribution(0, sizeof(alphabet) - 2);
        for (int i = 0; i < passLength; i++) {
            int index = distribution(generator);
            password[i] = alphabet[index];
        }
        password[passLength] = '\0';
        random_shuffle(&password[0], &password[passLength]);
        return password;
    }
};

int main()
{
    SetConsoleCP(1251);
    SetConsoleOutputCP(1251);
    srand(time(NULL));
    PassGen pass;
    pass.displayMessage();
    return 0;
}
```

Рисунок 5 – Программа генерации пароля на C++

Использование такой программы повышает безопасность аккаунтов пользователей, уменьшает риск фишинга и социальной инженерии.

ЗАКЛЮЧЕНИЕ

Предложенная система информационной безопасности отдела продаж эффективно защищает конфиденциальность и целостность данных различной важности, обеспечивая надежную основу для ведения бизнеса. Данная система дала предприятию уверенность в том, что их данные и операции достаточно защищены, что позволяет сосредоточиться на достижении поставленных бизнес-целей.

СПИСОК ЛИТЕРАТУРЫ

1. Агроснабженческая компания ООО «Э.П.Ф». – [Электронный ресурс]. Режим доступа: https://agrotambov.ru/?ysclid=ltclsitvrl76695511

2. БДУ - Угрозы. – [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/threat?ysclid=lu31lb4brt39607102

3. Методика от 14 февраля 2008 г. - ФСТЭК России. – [Электронный ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g?ysclid=lw1yenkr95712837284

4. Программный комплекс для защиты рабочих мест корпоративных пользователей ViPNet Client 4. ИнфоТеКС. – [Электронный ресурс]. Режим доступа: https://infotecs.ru/products/vipnet-client-/?ysclid=lufkdbdmvj567739731