Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Организационное и правовое обеспечение информационной безопасности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

«Создание организационной подсистемы информационной безопасности предприятия»

Выполнили:

Чу Ван Доан, студент группы N3347

(подпись)

Проверил:

Карманова Наталия Андреевна

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Введение

Цель работы – Освоить методику оформления организационно-распорядительных документов, регламентирующих работу по защите информации в организации.

Ход работы

1. Структура предприятия

Рисунок 1 - Структура предприятия

2. Положение «Политика безопасности предприятия»

- Цель документа: Установить общие принципы и подходы к обеспечению информационной безопасности в компании SIMEXCO.
- Содержание документа:
  - Определение информационной безопасности: Информационная безопасность – это состояние защищенности информационных ресурсов компании, при котором обеспечивается конфиденциальность, целостность и доступность информации.
  - Объекты информационной безопасности компании:
    - ERP-система;
    - CRM-система;
    - Файловые серверы;
    - Базы данных персонала и клиентов;
    - Финансовые и бухгалтерские данные.
  - Принципы политики безопасности:
    - Соблюдение российского законодательства и международных стандартов (ГОСТ Р 57580-1-2017, ISO 27001);
    - Регулярное обучение и повышение осведомленности персонала;

        - Применение сертифицированных средств защиты информации;
        - Недопущение несанкционированного доступа и распространения информации.
    - Ответственность за нарушения: Предусмотрены дисциплинарные меры за нарушение политики безопасности.

3. Распоряжение о распределении ответственности за обеспечение безопасности

- Цель документа: Определить ответственность конкретных сотрудников за защиту информационных ресурсов.

Таблица 1 - Содержание документа

Информационный ресурс	Ответственный сотрудник	Отдел
ERP-сервер	Иванов Сергей Дмитриевич	ИТ-отдел
CRM-сервер	Смирнова Елена Петровна	Отдел продаж
Финансовые данные	Петрова Анна Сергеевна	Бухгалтерия
Данные сотрудников	Кузнецов Иван Васильевич	Отдел кадров

- Для каждого ресурса утверждается матрица доступа (чтение, запись, изменение, удаление);
- Документ утверждается генеральным директором.

4. Инструкция по внедрению новой информационной системы

- Цель документа: Регламентировать процесс внедрения новых информационных систем.
- Содержание документа:
    - Этапы внедрения:

1. Подготовка и утверждение заявки на внедрение;
2. Анализ совместимости новой системы с существующей инфраструктурой;
3. Тестовое внедрение на отдельной площадке;
4. Проверка системы на отсутствие уязвимостей и ошибок;
5. Получение окончательного разрешения от генерального директора;
6. Полномасштабное внедрение и настройка системы.

- Требования к новой системе:

- Совместимость с действующей инфраструктурой;
- Наличие возможности оперативного отката при сбоях.

5. Инструкция по инвентаризации ресурсов

- Цель документа: Регулярная проверка и учет всех информационных ресурсов компании.
- Содержание документа:
  - Периодичность проведения: не реже одного раза в год.
  - Объекты инвентаризации:
    - Аппаратные ресурсы (серверы, ПК, сетевое оборудование);
    - Программные ресурсы (ERP, CRM, базы данных);
    - Информационные ресурсы (документы, договоры, базы клиентов).
- Порядок проведения инвентаризации:

1. Составление списка ресурсов;
2. Маркировка и регистрация ресурсов;
3. Подготовка итогового отчета о результатах инвентаризации.

6. Заключение соглашения о соблюдении режима информационной безопасности со всеми сотрудниками

- Цель документа: Формирование обязательств сотрудников по соблюдению режима информационной безопасности.
- Содержание документа:
  - Обязательства сотрудника:
    - Не раскрывать конфиденциальную информацию третьим лицам;
    - Использовать только утвержденное программное обеспечение;
    - Не подключать личные устройства к корпоративной сети;
    - Согласие на мониторинг рабочей переписки и переговоров.

Подписывается каждым сотрудником при приеме на работу и ежегодно обновляется.

7. Инструкция о порядке реагирования на инциденты в области информационной безопасности, а также на сбои и неисправности

- Цель документа: Определение последовательности действий при возникновении инцидентов.

- Содержание документа:
    - Действия при инциденте:
    1. Фиксация симптомов и времени инцидента;
    2. Изоляция и отключение затронутых устройств от сети;
    3. Незамедлительное уведомление руководства и отдела ИТ;
    4. Проведение анализа причин инцидента;
    5. Составление подробного отчета об инциденте;
    6. Принятие корректирующих мер.
- Меры ответственности: Дисциплинарная ответственность сотрудника при установлении вины.

8. Инструкция по защите от вредоносного ПО (вирусов, троянских коней)

- Цель документа: Недопущение заражения систем вредоносными программами.
- Содержание документа:
    - Основные требования:
    - Установка и регулярное обновление антивирусного ПО;
    - Запрет установки и запуска неутвержденного ПО;
    - Обязательная проверка всех внешних накопителей на вирусы перед подключением.
- Действия при обнаружении заражения:
    - Немедленная изоляция компьютера от сети;
    - Удаление вирусов с помощью специального программного обеспечения;
    - Информирование ИТ-службы компании.

9. Инструкция о безопасности носителей данных

- Цель документа: Обеспечение безопасности и контроля за носителями данных.
- Содержание документа:
    - Типы носителей: Съемные жесткие диски, USB-накопители, CD/DVD-диски, магнитные ленты.
    - Требования безопасности:
    - Использование только утвержденных и промаркированных носителей;
    - Хранение носителей в запираемых помещениях;
    - Шифрование данных, выносимых за пределы организации.

- Порядок уничтожения носителей данных:
  - Составление акта о выводе носителей из эксплуатации;
  - Физическое уничтожение (дробление, уничтожение дисков и лент).
- Правила работы с бумажными документами:
  - Регистрация и маркировка всех документов;
  - Ограничение доступа к конфиденциальным документам.

Заключение

Разработанный пакет документов обеспечивает всесторонний контроль за информационной безопасностью компании SIMEXCO, четко распределяет ответственность и регламентирует действия сотрудников во всех ситуациях, связанных с защитой информации. Внедрение данных документов позволит компании соответствовать российскому законодательству и международным стандартам безопасности.