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 №1

«Закрепление права предприятия на защиту информации в нормативных документах»

Выполнили:

Чу Ван Доан, студент группы N3347

(подпись)

Проверил:

Карманова Наталия Андреевна

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Введение

Цель работы – Освоение метода правовой защиты информации ограниченного доступа на предприятии.

1. **Задание**
    - Определение названия организации
    - Разработка организационной структуры предприятия, описание направлений работы организации и основных функций её подразделений.
    - Разработка схемы информационных потоков предприятия
    - Проведение анализа защищаемых информационных ресурсов предприятия
    - Проведение анализа защищаемых информационных ресурсов предприятия
2. **Ход работы**

2.1. Определение названия организации

Я выбрал экспортную компанию, занимающуюся поставками кофе во Вьетнаме - Simexco.

2.2. Разработка организационной структуры предприятия, описание направлений работы организации и основных функций её подразделений.

2.2.1. Структура предприятия

2.2.2. Описание направлений работы предприятия

- Экспорт всех видов кофе (чистый кофе, жареный кофе, молотый кофе, растворимый кофе...)

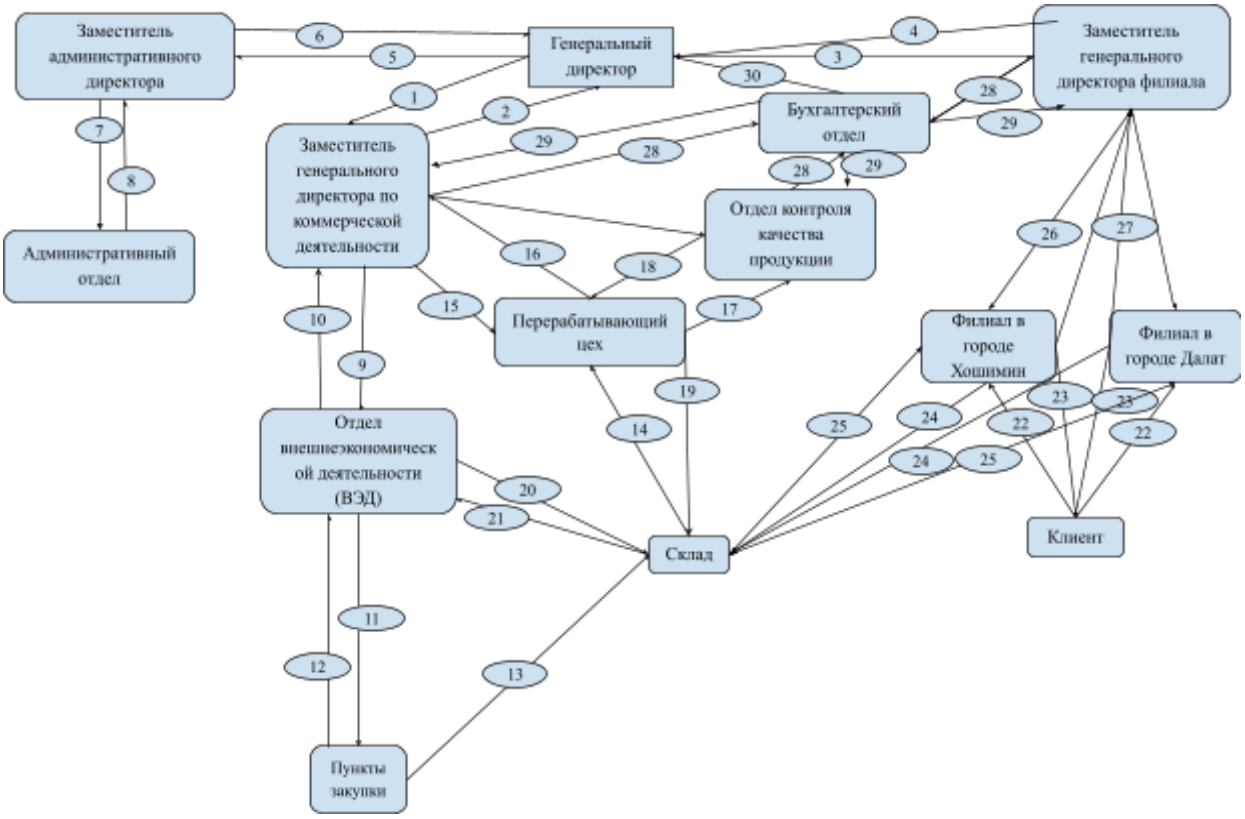
2.2.3. Описание основных функций подразделений предприятия.

- Генеральный директор: Генеральный директор осуществляет непосредственное управление и руководство всеми отделами и подчиненными подразделениями.
- Заместители генерального директора: Оказывают помощь генеральному директору в профессиональных вопросах, разрабатывают планы, предлагают решения в пределах своей компетенции и полномочий, а также помогают генеральному директору в контроле за деятельностью подчиненных отделов и исполнением решений компании.
- Административный отдел: Осуществляет функции управления персоналом, ведет административную и организационную работу, координирует кадровую политику для повышения эффективности работы. Отвечает за административное управление, ведение документации, архивирование деловой корреспонденции и других сопутствующих документов. Кроме того, несет ответственность за условия труда, соблюдение трудового законодательства сотрудниками компании.
- Бухгалтерский отдел: Управляет финансовой деятельностью компании, выполняет финансовые операции, связанные с денежными потоками, использованием капитала и управлением финансовыми ресурсами. Осуществляет бухгалтерский учет, контроль задолженности и управление финансовыми потоками компании.
- Отдел внешнеэкономической деятельности: Консультирует руководство компании по вопросам переговоров и заключения контрактов с отечественными и зарубежными партнерами, проводит маркетинговые исследования, организует экспорт товаров. Этот отдел является ключевым подразделением компании и включает в себя две подструктуры:
    - Пункты закупки: Отвечают за закупку сельскохозяйственной продукции, преимущественно кофе, взаимодействуют с производителями, обеспечивая информационную связь между компанией и поставщиками, а также организуют транспортировку товаров на склады.
    - Склад: Является местом хранения продукции, поступающей с пунктов закупки, и подготовки товаров к экспорт
- Отдел контроля качества продукции: Осуществляет проверку и сертификацию качества продукции компании перед выпуском на рынок или экспортом.

- Ферма: Занимается выращиванием кофе, черного перца и каучуковых деревьев для последующего экспорта.
- Перерабатывающий цех: Осуществляет первичную обработку и подготовку сельскохозяйственной продукции для экспорта.
- Филиалы в городах Хошимин и Далат: Выполняют функции координации работы с партнерами, служат логистическими узлами для транспортировки товаров из складов и отвечают за внешнеэкономическую деятельность
- Транзитный склад: Используется для централизованного сбора и подготовки товаров к отправке на экспорт.

2.3. Разработка схемы информационных потоков предприятия

2.3.1. Схема информационных потоков предприятия



2.3.2. Анализ информационных потоков предприятия

Таблица 1 – Анализ информационных потоков предприятия

№	Наименование информационного потока	Описание
1	Бизнес-стратегия	Генеральный директор передает бизнес-стратегию и цели развития компании заместителю генерального директора по бизнесу. Контролирует и утверждает бизнес-план.
2	Отчет о бизнес-стратегии	Заместитель генерального директора по бизнесу отчитывается о бизнес-планах, анализирует состояние бизнеса компании.
3	Управление филиалами	Генеральный директор координирует деятельность филиалов. Контролирует эффективность их работы.
4	Отчет о деятельности филиалов	Заместитель генерального директора филиала отчитывается о текущем состоянии бизнеса в филиалах.
5	Административное управление	Генеральный директор управляет кадровыми ресурсами и административной деятельностью компании.
6	Отчет о деятельности административного отдела	Заместитель генерального директора по административным вопросам отчитывается по вопросам, связанным с персоналом, документами и т. д.
7	Управление персоналом	Заместитель генерального директора по административным вопросам координирует кадровую работу, подбор персонала и систему льгот. Управляет документацией и внутренними административными процессами через административный отдел.

8	Отчет по управлению персоналом	Административный отдел отправляет отчет заместителю генерального директора по административным вопросам о наборе персонала, документации сотрудников и компании.
9	Контракты и рынок	Заместитель генерального директора по бизнесу разрабатывает экспортные контракты, исследует международный рынок кофе. Ищет новых клиентов и партнеров.
10	Отчет о внешнеэкономической деятельности	Отдел внешнеэкономической деятельности отчитывается о закупке сырья, заключении контрактов на экспорт и импорт.
11	Закупки и поставки	Поиск поставщиков кофе. Взаимодействие с поставщиками, обновление закупочных цен.
12	Отчет о поставках кофе	Поставщики сообщают о текущем состоянии закупок кофе из различных источников.
13	Импорт товаров	Транспортировка товаров с места закупки на центральный склад.
14	Сырье для производства	Обеспечение сырьем кофе для производственного процесса.
15	Производство и переработка	Заместитель генерального директора по бизнесу координирует процесс переработки кофе для экспорта.
16	Отчет о состоянии производства и переработки	Заводы отчитываются перед заместителем генерального директора по бизнесу о переработке и производстве.
17	Контроль качества	Заводы отправляют образцы продукции в отдел контроля качества перед поступлением на склад.
18	Результаты проверки качества	Отдел КСО (контроль службы качества) выдает результаты проверки с решением о принятии партии на склад или отказе.

19	Завоз товаров на склад	Транспортировка переработанных товаров на склад для подготовки к экспорту.
20	Координация склада	Отдел бизнес-операций и ВЭД (внешнеэкономической деятельности) контролирует количество поступающих и отправляемых товаров.
21	Отчет о состоянии склада	Склады отчитываются в отдел бизнеса и ВЭД о количестве поступивших и отправленных товаров, а также о состоянии складских помещений.
22	Заказ и покупка товаров	Клиенты приходят в филиалы для заказа кофе (количество, тип товара, срок доставки). Согласовываются экспортные контракты или дистрибуция на внутренний рынок.
23	Доставка и оплата	Филиалы забирают товар со склада и доставляют клиентам по заказам. Производится обработка платежей и задолженностей.
24	Запрос на получение товара	Филиалы запрашивают у складов поставку товаров в филиалы.
25	Транспортировка товаров в филиалы	Склады отправляют товары в филиалы.
26	Операционная деятельность	Заместитель генерального директора филиала управляет деятельностью филиалов.
27	Отчет о бизнес-операциях	Филиалы отчитываются о бизнес-операциях в своих подразделениях.
28	Финансовый отчет	Департаменты предоставляют финансовые отчеты в бухгалтерию.
29	Распределение финансов	Бухгалтерия распределяет финансовые средства между департаментами для их деятельности.

30	Финансовый отчет	Бухгалтерия подготавливает финансовый отчет для генерального директора.

2.4. Проведение анализа защищаемых информационных ресурсов предприятия

2.4.1. Группа информационных потоков высшего управленческого уровня (1, 2, 3, 4, 5, 6)

- Поток 1: «Бизнес-стратегия»
- Данные/Информационные активы: Бизнес-стратегия, цели развития, общие планы компании.
- Уровень конфиденциальности: Высокий (ключевая информация о направлениях и планах компании).
- Основные угрозы:
    - Утечка информации конкурентам или в СМИ.
    - Несанкционированное изменение данных, искажение стратегии.
- Поток 2: «Отчёт о бизнес-стратегии»
- Данные: Отчёты по реализации бизнес-планов, анализ состояния бизнеса.
- Уровень конфиденциальности: Высокий (отражает результаты деятельности, финансовые показатели, рыночный анализ).
- Угрозы:
    - Раскрытие внутренней информации, утечка конкурентам.
    - Подделка или искажение отчёта.
- Поток 3: «Управление филиалами»
- Данные: Информация о планах, управленческих решениях, ключевых показателях эффективности (KPI) филиалов.
- Уровень конфиденциальности: Средний – Высокий (зависит от деталей, но в целом серьёзно влияет на работу филиалов).
- Угрозы: Несанкционированный доступ к операционным планам и показателям филиалов.
- Поток 4: «Отчёт о деятельности филиалов»

- Данные: Сводная отчётность по состоянию бизнеса в филиалах (объёмы продаж, расходы и т. д.).
- Уровень конфиденциальности: Высокий (детализированные финансовые и коммерческие сведения).
- Угрозы: Утечка или раскрытие финансовых показателей, стратегий филиала.

- Поток 5: «Административное управление»
- Данные: Документы по управлению персоналом, административные регламенты, кадровые договоры.
- Уровень конфиденциальности: От среднего до высокого (включает персональные данные сотрудников).
- Угрозы: Утечка личных данных и нарушение законодательства о защите персональной информации.

- Поток 6: «Отчёт о деятельности административного отдела»
- Данные: Регулярные отчёты по персоналу, внутренним процессам, документам компании.
- Уровень конфиденциальности: Средний (может включать персональные данные).
- Угрозы: Несанкционированный доступ к базе данных о сотрудниках.

2.4.2. Группа информационных потоков, связанных с персоналом и административными вопросами (7, 8)

- Поток 7: «Управление персоналом»
- Данные: Информация о приёме на работу, зарплате, льготах, кадровых процессах.
- Уровень конфиденциальности: Высокий (содержит личные и конфиденциальные сведения о сотрудниках).
- Угрозы:
    - Кража персональных данных.
    - Утечка информации о зарплатах или планах по найму.

- Поток 8: «Отчёт по управлению персоналом»
- Данные: Отчёты по кадровым вопросам, найму, трудовым договорам.
- Уровень конфиденциальности: Высокий (аналогично потоку 7).

2.4.3. Группа информационных потоков по внешнеэкономической деятельности и контрактам (9, 10, 11, 12, 13)

- Поток 9: «Контракты и рынок»
- Данные: Экспортные контракты, исследования рынка, потенциальные клиенты/партнёры.
- Уровень конфиденциальности: Высокий (коммерческие тайны, сведения о цене и контрагентах).
- Угрозы:
    - Кража контрактов, раскрытие коммерческих условий, хищение клиентской базы.
    - Подделка документов.
- Поток 10: «Отчёт о внешнеэкономической деятельности»
- Данные: Отчёт по закупке сырья, экспорту, импорту, финансовым результатам сделок.
- Уровень конфиденциальности: Высокий.
- Угрозы: Утечка стратегических данных о внешнеэкономической деятельности.
- Поток 11: «Закупки и поставки»
- Данные: Информация о поставщиках, котировках, графике поставок.
- Уровень конфиденциальности: Средний (некоторые ценовые сведения важны в конкурентной среде).
- Угрозы:
    - Несанкционированное изменение графика поставок, вмешательство в цепочку поставок.
    - Утечка ценовой политики конкурентам.
- Поток 12: «Отчёт о поставках кофе»
- Данные: Отчёт о состоянии поставок, объёмах и качестве закупаемого сырья.
- Уровень конфиденциальности: Средний – Высокий (финансово-коммерческий контекст).
- Угрозы: Утечка информации о поставщиках и объёмах поставок.

Поток 13: «Импорт товаров»

- Данные: Транспортные накладные, логистика, маршрут, таможенные документы.
- Уровень конфиденциальности: Средний (кроме случаев, когда содержатся особые коммерческие условия).
- Угрозы: Искажение данных о логистике, задержки в поставках, кража товаров.

2.4.4. Группа информационных потоков по производству и контролю качества (14, 15, 16, 17, 18, 19)

- Поток 14: «Сырьё для производства»
  - Данные: Сведения об объёмах и качестве сырья, необходимого для производства.
  - Уровень конфиденциальности: Средний (внутренние производственные данные).
  - Угрозы: Подделка или искажение сведений, приводящее к ошибкам планирования.
- Поток 15: «Производство и переработка»
  - Данные: Технологии, рецептуры, графики переработки, производственные процессы.
  - Уровень конфиденциальности: Высокий (возможны уникальные ноу-хау).
  - Угрозы: Кража технологических секретов.
- Поток 16: «Отчёт о состоянии производства и переработки»
  - Данные: Показатели объёмов производства, эффективность переработки, качественные показатели.
  - Уровень конфиденциальности: Средний – Высокий (содержит коммерчески важные данные).
  - Угрозы: Утечка производственных показателей, что может повлиять на конкурентные преимущества.
- Поток 17: «Контроль качества»
  - Данные: Результаты тестирования, лабораторные анализы, контрольные протоколы.
  - Уровень конфиденциальности: Средний (важно для внутренней оценки и юридических аспектов).
  - Угрозы: Фальсификация результатов тестов, пропуск некачественной продукции.
- Поток 18: «Результаты проверки качества»
  - Данные: Окончательные выводы о качестве партий, разрешение или отказ в приёмке на склад.
  - Уровень конфиденциальности: Средний, но влияет на бизнес-решения.
  - Угрозы: Подделка итоговых заключений, пропуск брака в производство.
- Поток 19: «Завоз товаров на склад»
  - Данные: Сведения о партии товара, количестве, времени поступления на склад.
  - Уровень конфиденциальности: Низкий – Средний (внутренние логистические процессы).
  - Угрозы: Ошибки в учёте и управлении складскими запасами.

2.4.5. Группа информационных потоков по складской логистике и филиалам (20, 21, 24, 25, 26, 27)

- Поток 20: «Координация склада»
  - Данные: Информация об учёте поступающего и отгружаемого товара между складом и отделами (бизнес, ВЭД).
  - Уровень конфиденциальности: Средний (учёт остатков и планирование продаж).
  - Угрозы: Изменение данных о складских запасах, дезорганизация поставок.
- Поток 21: «Отчёт о состоянии склада»
  - Данные: Отчёт о количестве товаров, их движении, состоянии складских помещений.
  - Уровень конфиденциальности: Средний.
  - Угрозы: Утечка данных об объёмах запасов и динамике поставок.
- Поток 24: «Запрос на получение товара»
  - Данные: Заявка филиала на поставку (количество, вид товара, сроки).
  - Уровень конфиденциальности: Низкий – Средний (внутренняя информация о заказах).
  - Угрозы: Подделка заявок, хищение товара или срыв поставок.
- Поток 25: «Транспортировка товаров в филиалы»
  - Данные: Логистика, графики отправки, номера транспортных средств, данные водителей.
  - Уровень конфиденциальности: Низкий – Средний.
  - Угрозы: Мошенничество во время перевозки, хищение партии.
- Поток 26: «Операционная деятельность» (управление деятельностью филиалов)
  - Данные: Сведения о продажах, обслуживании клиентов, местной стратегии дистрибуции.
  - Уровень конфиденциальности: Средний – Высокий (зависит от детализации).
  - Угрозы: Раскрытие бизнес-процессов, схем продаж, доходов филиалов.
- Поток 27: «Отчёт о бизнес-операциях» (от филиалов)
  - Данные: Доходы, расходы, показатели продаж, результаты транзакций.
  - Уровень конфиденциальности: Высокий (финансовая отчётность филиалов).
  - Угрозы: Несанкционированный доступ, утечка финансовых данных.

2.4.6. Группа информационных потоков, связанных с клиентами и сделками (22, 23)

- Поток 22: «Заказ и покупка товаров»
- Данные: Заявки на покупку, контракты, сведения о клиентах (имя, контакты, реквизиты, объём заказа).
- Уровень конфиденциальности: Высокий (персональные данные и информация о контракте).
- Угрозы:
    - Кража клиентских данных, нарушение законодательства о защите ПДн.
    - Подделка заказов и финансовых обязательств.
- Поток 23: «Доставка и оплата»
- Данные: Подробности доставки, адреса, платёжные данные, счета-фактуры.
- Уровень конфиденциальности: Высокий (персональные и финансовые сведения).
- Угрозы: Кража платёжной информации, мошенничество.

2.4.7. Группа информационных потоков финансово-бухгалтерского характера (28, 29, 30)

- Поток 28: «Финансовый отчёт (департаменты → бухгалтерия)»
- Данные: Финансовые отчёты от отделов (выручка, затраты, зарплаты и т. д.).
- Уровень конфиденциальности: Высокий (вся финансовая информация компании).
- Угрозы: Утечка внешним лицам, подделка данных бухгалтерского учёта.
- Поток 29: «Распределение финансов»
- Данные: Решение о распределении финансовых ресурсов, бюджета по отделам и филиалам.
- Уровень конфиденциальности: Высокий (напрямую связано с движением денежных средств).
- Угрозы: Несанкционированная корректировка сумм, хищение средств.
- Поток 30: «Финансовый отчёт (бухгалтерия → генеральный директор)»
- Данные: Сводная финансовая отчётность для руководства.
- Уровень конфиденциальности: Критически высокий (всеобъемлющие финансовые показатели).
- Угрозы: Утечка может негативно повлиять на репутацию, конкурентоспособность, стоимость акций и т. д.

2.5. Проведение анализа защищаемых информационных ресурсов предприятия

2.5.1. Правовые основы защиты информации

Право предприятия на защиту информации ограниченного доступа основано на международных, национальных и отраслевых правовых актах. Основные нормативно-правовые документы, регулирующие защиту информации, включают:

- Международные стандарты:
  - ISO/IEC 27001 – система управления информационной безопасностью.
  - Конвенция о киберпреступности (Будапештская конвенция) – противодействие преступлениям в сфере информационной безопасности.
- Национальные законы (пример для России):
  - ФЗ №149 «Об информации, информационных технологиях и о защите информации» – регулирует права и обязанности в области обработки и хранения информации.
  - ФЗ №152 «О персональных данных» – устанавливает требования к обработке и защите персональных данных.
  - ФЗ №98 «О коммерческой тайне» – защищает конфиденциальные сведения, имеющие коммерческую ценность.

2.5.2. Категории информации ограниченного доступа

На предприятии может быть несколько категорий информации, нуждающейся в защите:

1. Коммерческая тайна:
   - Договоры с клиентами и партнерами.
   - Бизнес-стратегия, маркетинговые исследования.
   - Информация о ценообразовании и технологиях.
2. Персональные данные сотрудников и клиентов:
   - ФИО, контакты, паспортные данные.
   - Данные о заработной плате, трудовые договоры.
3. Финансовые данные:
   - Финансовая отчетность, налоговые документы.
   - Банковские счета, транзакции.
4. Производственные и технологические сведения:

- Рецептуры, схемы переработки, уникальные ноу-хау.
- Данные о цепочках поставок, логистике.

5. Данные о клиентах и партнерах:
   - Заказы, платежные сведения.
   - Контрактные обязательства.

2.5.3. Право предприятия на защиту информации

Опираясь на действующую правовую базу, предприятие имеет следующие основания для защиты информации:

1. Защита коммерческой тайны:
   В соответствии с ФЗ №98 «О коммерческой тайне» (или аналогичными законами в других странах), предприятие может устанавливать режим коммерческой тайны, что дает ему право:
   - Ограничивать доступ к информации.
   - Заключать соглашения о неразглашении (NDA).
   - Привлекать к ответственности за нарушение режима тайны.
2. Защита персональных данных:
   Предприятие обязано обеспечивать конфиденциальность персональных данных сотрудников и клиентов согласно GDPR, ФЗ-152 или аналогичным нормам.
3. Защита финансовых данных:
   Данные о доходах, расходах, налогах являются финансовой тайной. Их защита регулируется законами о бухгалтерском учете и аудите (например, SOX в США).
4. Защита от киберугроз и корпоративного шпионажа:
   Согласно ISO/IEC 27001 и национальным стандартам, предприятие вправе использовать средства киберзащиты для предотвращения утечек данных и атак.

2.5.4. Основные угрозы и ответственность за их предотвращение

Без соответствующих мер защиты предприятие рискует потерять конкурентные преимущества, подвергнуться штрафам и судебным разбирательствам. Возможные угрозы включают:

- Утечку информации конкурентам.
- Несанкционированный доступ к данным.

- Взлом IT-инфраструктуры.
- Нарушение законодательства о защите данных (штрафы по GDPR могут достигать 4% от годового оборота).

В связи с этим предприятие имеет полное право применять правовые, технические и организационные меры для защиты своей информации.

Защита информации ограниченного доступа является законным правом предприятия, основанным на международных и национальных правовых актах. Реализация мер защиты не только помогает компании сохранить конкурентные преимущества, но и позволяет избежать юридической ответственности за утечку данных.

Заключение

В ходе проведённого лабораторного анализа структуры предприятия SIMEXCO и его информационных потоков были выявлены основные направления деятельности, функциональные обязанности подразделений, а также потоки информации внутри компании. Анализ показал, что предприятие активно занимается экспортом и переработкой сельскохозяйственной продукции, а также ведёт внутреннюю торговлю и управляет филиальной сетью.

Исследование информационных потоков позволило выявить ключевые каналы передачи данных, определить их уровень конфиденциальности и потенциальные угрозы безопасности. Были рассмотрены основные категории информации ограниченного доступа, включая коммерческую тайну, персональные данные, финансовую отчетность, производственные технологии и информацию о клиентах.

На основании анализа нормативно-правовой базы были обоснованы права предприятия на защиту информации ограниченного доступа. Основными юридическими основаниями для защиты информации являются международные стандарты (ISO/IEC 27001, GDPR), национальные законы (ФЗ №149, ФЗ №152, ФЗ №98) и корпоративные политики безопасности.

Выявленные угрозы включают утечку коммерческой информации конкурентам, несанкционированный доступ к данным, фальсификацию отчетности и возможные кибератаки. В связи с этим предприятию рекомендуется внедрить комплексную систему защиты информации, включающую юридические, технические и организационные меры.

Таким образом, проведённый анализ позволил детально изучить информационные потоки предприятия, оценить их безопасность и разработать рекомендации по защите критически важной информации, что способствует повышению устойчивости компании и снижению рисков потери данных.

.

Список использованных источников

1. Федеральный закон №149-ФЗ "Об информации, информационных технологиях и о защите информации": текст закона

2. Федеральный закон №152-ФЗ "О персональных данных": текст закона

3. Федеральный закон №98-ФЗ "О коммерческой тайне": текст закона

4. ISO/IEC 27001 – Система менеджмента информационной безопасности: описание стандарта

5. GDPR – Общий регламент по защите данных: текст регламента на русском языке
6. https://simexcodl.com.vn/
7. https://www.studocu.vn/vn/document/dai-hoc-dong-nai/abcdefgh/ha-xuan-duc-dieu-chinh/98294650
8. http://tailieuso.udn.vn/bitstream/TTHL_125/5861/2/TranSang.TT.pdf