1.Введение

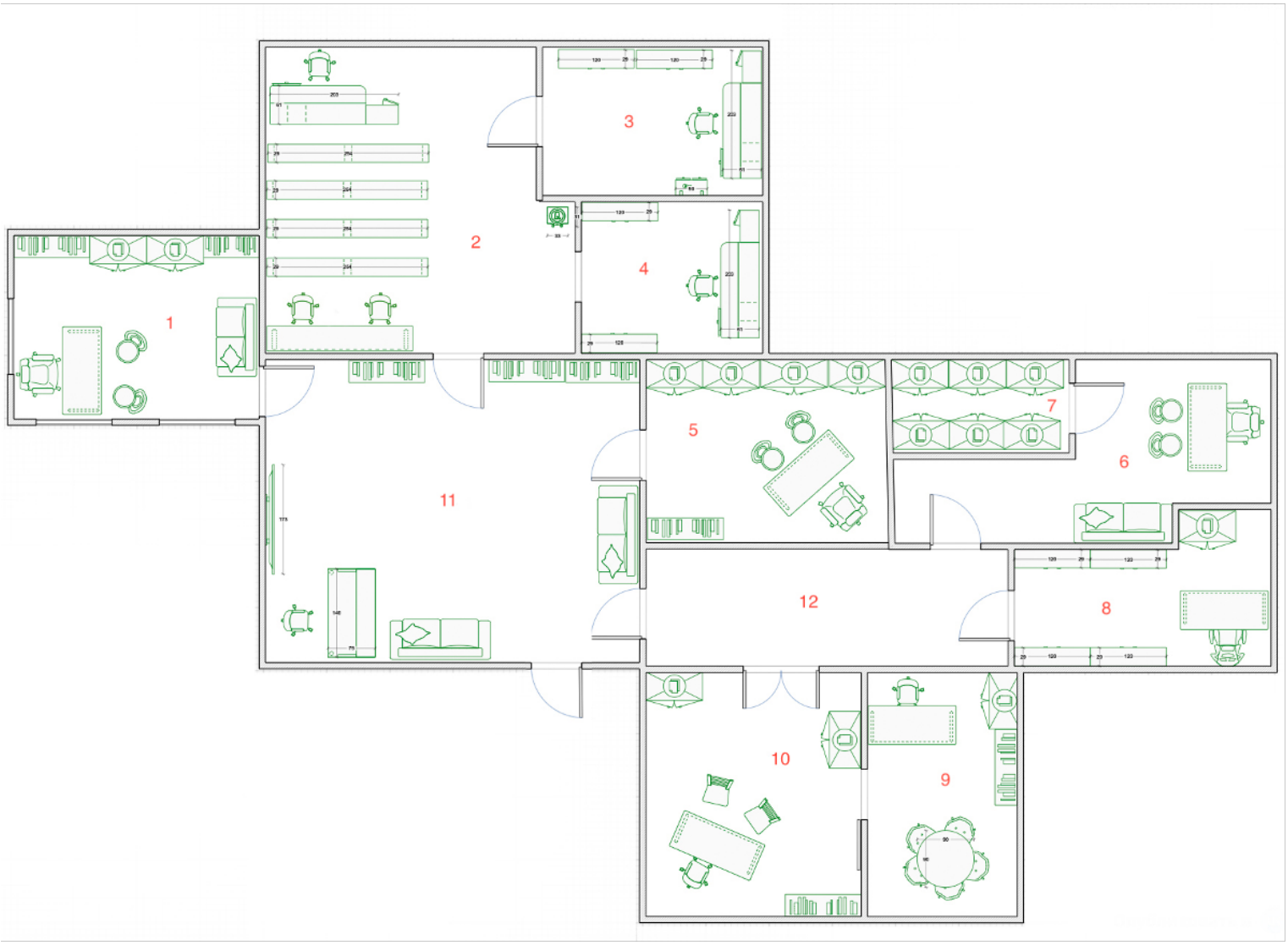
В качестве объекта исследования мной была выбрана организация ООО «ОптиксПЛЮС».
Основным видом деятельности данной организации является:
- Торговля оптовая фармацевтической продукцией (ОКВЭД: 46.46.1)
Дополнительные виды деятельности:
- Ремонт электронного и оптического оборудования (ОКВЭД: 33.13)
- Производство оптических приборов, фото- и кинооборудования (ОКВЭД: 26.70)
Организация предоставляет своим клиентам – оптикам полное сопровождение изготовление их заказов:
- Закупка очковых линз
- Обточка, установка очковых линз в оправу
- Покраска очковых линз
- Ремонт оправ

2. Структура компании

В организации ООО «ОптиксПЛЮС» работают 11 сотрудников:
- Генеральный директор
- Главный бухгалтер
- Главный юрист
- Системный администратор
- Главный мастер
- Мастер по ремонтам и покраскам
- Мастер по обработке линз
- Сотрудник ОТК
- Начальник отдела продаж
- Менеджер по продажам
- Офис-менеджер

Изображение 1. Структура компании

Далее рассмотрим план офиса и зоны доступа



Изображение 2. План офиса с зонами доступа

Название зон доступа:
1 – Кабинет генерального директора
2 – Мастерская
3 – Кабинет мастера по покраске линз
4 – Кабинет главного мастера
5 – Кабинет главного юриста
6 – Кабинет главного бухгалтера
7 – Архив бухгалтерии
8 – Кабинет системного администратора
9 – Кабинет начальника отдела продаж
10 – Кабинет менеджера отдела продаж
11 – Приемная (рабочее место офис-менеджера)
12 – Коридор

Должность	Зоны доступа	Вид деятельности
Генеральный директор	1 - 12	Управление организацией
Главный бухгалтер	2 - 12	Финансовая деятельность
Главный юрист	2 - 12	Составление юр.документов
Системный администратор	2 - 12	Обеспечение работы сервера и
Главный мастер	11, 2, 4	обеспечение штатной работы компьютерной техники, сети и программного обеспечения.
Мастер по ремонтам и покраскам	11, 2, 3	Покраска линз и ремонт оправ
Мастер по обработке линз	11, 2	Обработка линз
Сотрудник ОТК	11, 2	Проверка качества выполняемых работ
Начальник отдела продаж	11, 12, 10, 9	Координация коммерческой деятельности
Менеджер по продажам	11, 12, 10	Работа с клиентами
Офис-менеджер	11	Проведение заявок в БД, комплектования заказа для передачи в мастерскую, оформление первичных документов

Таблица 1. Соотнесение категорий персонала компании с зонами доступа

3.Модель угроз информационной безопасности

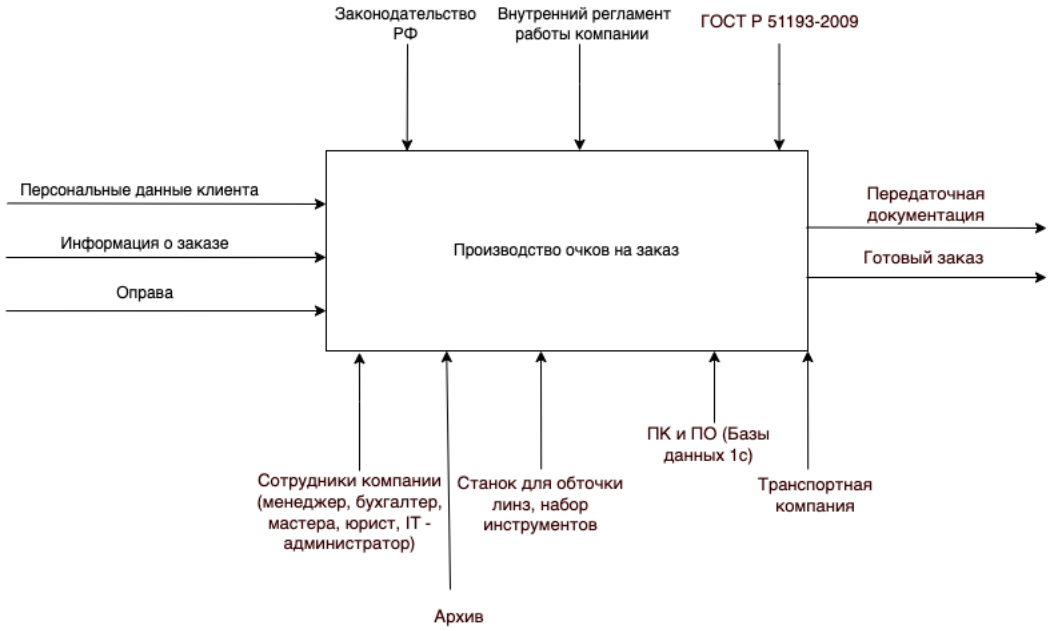
№	Элемент защиты	Угроза безопасности	Ущерб элементу защиты	Ущерб объекту защиты	Меры безопасности
1	Сотрудники организации	Шантаж, грабеж, кража, нападение	Моральный ущерб, травмы различной степени тяжести	Прекращение рабочего процесса	Усиленные меры безопасности, круглосуточное видеонаблюдение, тревожная кнопка, сигнализация
		Конфликтные ситуации	Моральный ущерб	Понижение эффективности рабочего процесса	Видеонаблюдение и создание охраны для быстрого реагирования и задержания нарушителя
2	Материальные ценности на охраняемой территории	Кража	Хищение элемента защиты (невозможность дальнейшего использования этого элемента)	Понижение эффективности рабочего процесса или его прекращение	Создание охраны, ограничение доступа персонала, круглосуточное видеонаблюдение для фиксации момента кражи и поимки нарушителя
		Порча имущества, вандализм	Ограничение возможности использовать элемент защиты, полная утра-та функциональных свойств элемента	Понижение эффективности рабочего процесса или его прекращение	Создание охраны, ограничение доступа персонала, круглосуточное видеонаблюдение для фиксации момента вандализма или порчи имущества и поимки нарушителя
		Пожар, стихийные бедствия, аварии на охраняемой территории	Полное уничтожение элемента защиты	Полная остановка рабочего процесса, так как помимо материальных ценностей вероятно было уничтожено и помещение организации	Страхование, установка датчиков дыма и систем пожаротушения, регулярные проверки оборудования, необходимого для предотвращения опасных ситуаций (огнетушители), периодическое проведение учений по эвакуации в случае ЧС, наличие схем здания с путями эвакуации

			(например, носителя информации)	процесса	круглосуточное видеонаблюдение, создание охраны, резервное копирование
		Несанкционированное ознакомление, изменение информации	Нарушение корректности данных, ведущее к ошибкам в ходе рабочего процесса	Материальный ущерб, распространение частной информации	Ограничение доступа к информации, пароли, шифрование данных, круглосуточное видеонаблюдение, создание охраны, резервное копирование
		Социальная инженерия	Похищение информации, манипуляция сотрудниками предприятия	Распространение частной информации, материальный ущерб, понижение эффективности рабочего процесса	Социально-психологические тренинги, ограниченный доступ в интернет на рабочем месте
3	Информация	Кража, копирование информации	Похищение информации	Распространение частной информации	Ограничение доступа к информации, пароли (желательно периодически меняющиеся, но не записывающиеся на видном месте), шифрование данных, круглосуточное видеонаблюдение, создание охраны, создание частной сети без постоянного выхода в интернет (на случай хакерских атак с целью кражи или копирования информации)
		Уничтожение информации	Полное уничтожение объекта защиты	Невозможность продолжения рабочего	Ограничение доступа к информации, пароли, шифрование данных,

			(например, носителя информации)	процесса	круглосуточное видеонаблюдение, создание охраны, резервное копирование
		Несанкционированное ознакомление, изменение информации	Нарушение корректности данных, ведущее к ошибкам в ходе рабочего процесса	Материальный ущерб, распространение частной информации	Ограничение доступа к информации, пароли, шифрование данных, круглосуточное видеонаблюдение, создание охраны, резервное копирование
		Социальная инженерия	Похищение информации, манипуляция сотрудниками предприятия	Распространение частной информации, материальный ущерб, понижение эффективности рабочего процесса	Социально-психологические тренинги, ограниченный доступ в интернет на рабочем месте
4	Автоматизированные средства обеспечения информации	Вирусы	Вывод из строя ПК	Полная остановка рабочего процесса	Антивирусное ПО, межсетевые экраны, ограничение свободного доступа в интернет для сотрудников
		Перепад напряжения, обесточивание помещения	Потеря несохраненных данных	Остановка рабочего процесса, ограничение деятельности, материальные затраты	Установка источника бесперебойного питания
		Вредоносные программы, переносимые на USB-устройствах	Вывод из строя ПК	Остановка, ограничение рабочего процесса, материальные затраты	Проведение инструктажа безопасности персонала, регулярная проверка имеющихся на предприятии USB-устройств

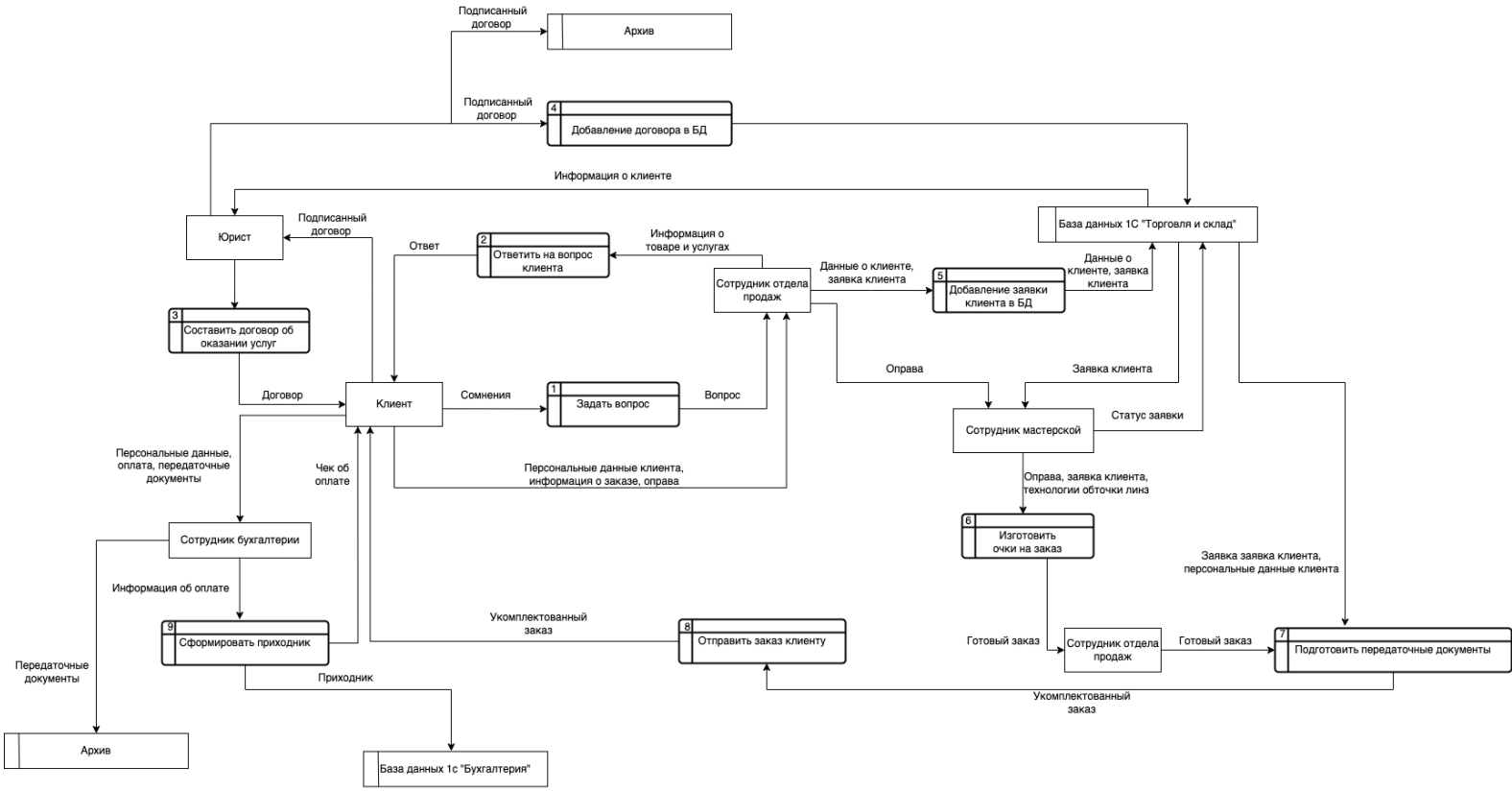
4. Описание производственных процессов компании

Контекстная диаграмма (нотация IDEF0)



Описание контекстной диаграммы:

Декомпозиция контекстной диаграммы (нотация DFD)



Описание декомпозиция контекстной диаграммы:
Сомнения клиента порождают вопросы, которые он задают сотруднику отдела продаж. После того как ответы на вопросы были получены, клиент готов сделать заказ. Для этого клиент обращается к юристу и передает свои персональные данные, юрист составляет договор, который отправляет клиенту. После юрист получает подписанный договор, который сохраняет в БД и оригинал кладет в архив. Теперь сотрудники отдела продаж получают информацию о заказе клиента, добавляют ее в базу данных 1с «Торговля и склад». Из этой базы сотрудник мастерской получает информацию о заказе и начинает изготавливать заказ, после чего передает готовый заказ сотруднику отдела продаж. Тот в свою очередь подготавливает передаточные документы, получая всю нужную информацию из базы данных 1с «Торговля и склад». Укомплектованный заказ отправляют клиенту. После получения заказа, клиент отправляет оплату, а сотрудник бухгалтерии подготавливает приходник в базе 1с «Бухгалтерия», а оригиналы передаточных документов кладет в архив.

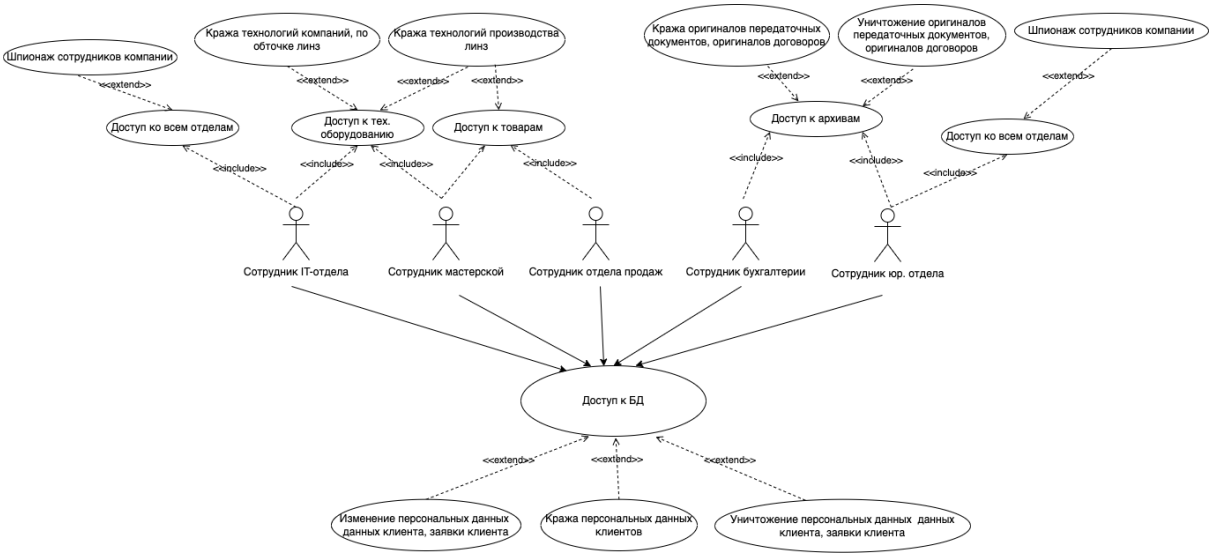
Элементы декомпозиции контекстной диаграммы:
Функции:
1 – Задать вопрос
2 – Ответить на вопрос
3 – Составить договор об оказании услуг
4 – Добавление договора в базу 1с «Торговля и склад»
5 – Добавление заявки в базу 1с «Торговля и склад»
6 – Изготовить очки на заказ
7 – Подготовить передаточные документы
8 – Отправить заказ клиенту
9 – Сформировать приходник

Сущности:
Клиент
Сотрудник отдела продаж
Юрист
Сотрудник мастерской
Бухгалтер

Хранилища данных:
БД 1С «Торговля и склад»
БД 1С «Бухгалтерия»
Архив

4. Описание нарушителей

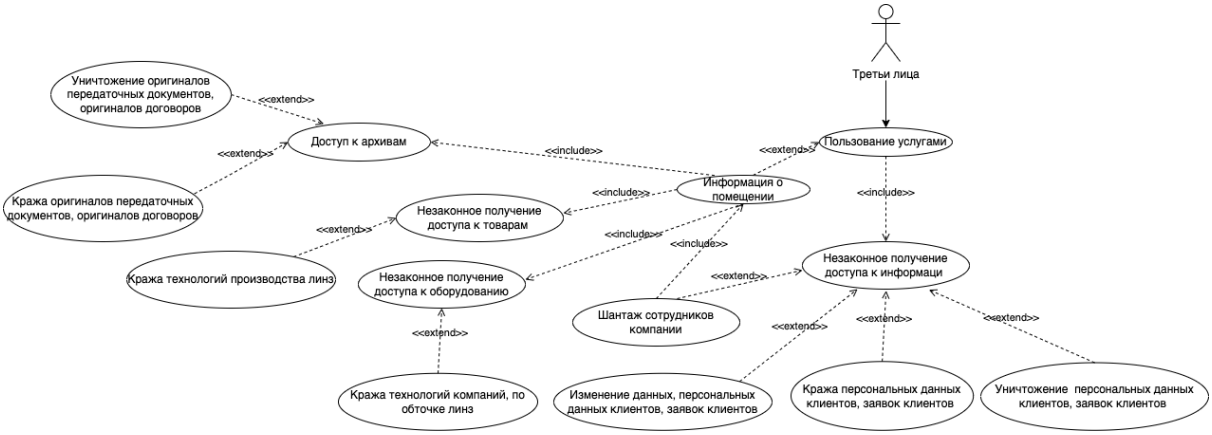
Use-case диаграмма - внутренний нарушитель



Описание Use-case диаграмма - внутренний нарушитель:

Все сотрудники имеют доступ к БД, вследствие чего они могут изменить, украсть, уничтожить, персональные данные клиентов и их заявки. Сотрудник IT-отдела имеет доступ ко всем отделам, тем самым может заниматься шпионажем сотрудников, а доступ к тех.оборудованию дает ему доступ к технологиям компании по обточке линз. Поскольку база развернута на оборудование сторонней организации, IT сотрудник не сможет удалить базу полностью или ограничить к ней доступ Так же доступ к тех.оборудованию и товару есть у сотрудников мастерской, что позволяет им украсть технологии по обточке линз и технологии по производству линз. Сотрудники бухгалтерии и юр. отдела имеют доступ к архивам, где хранятся оригиналы передаточных документов (Реализаций, актов об оказании услуг, договоров), тем самым они могут украсть и уничтожить данные документы. Также данные сотрудники имеют доступ ко всем зонам офиса, тем самым они могут совершить шпионаж за сотрудниками

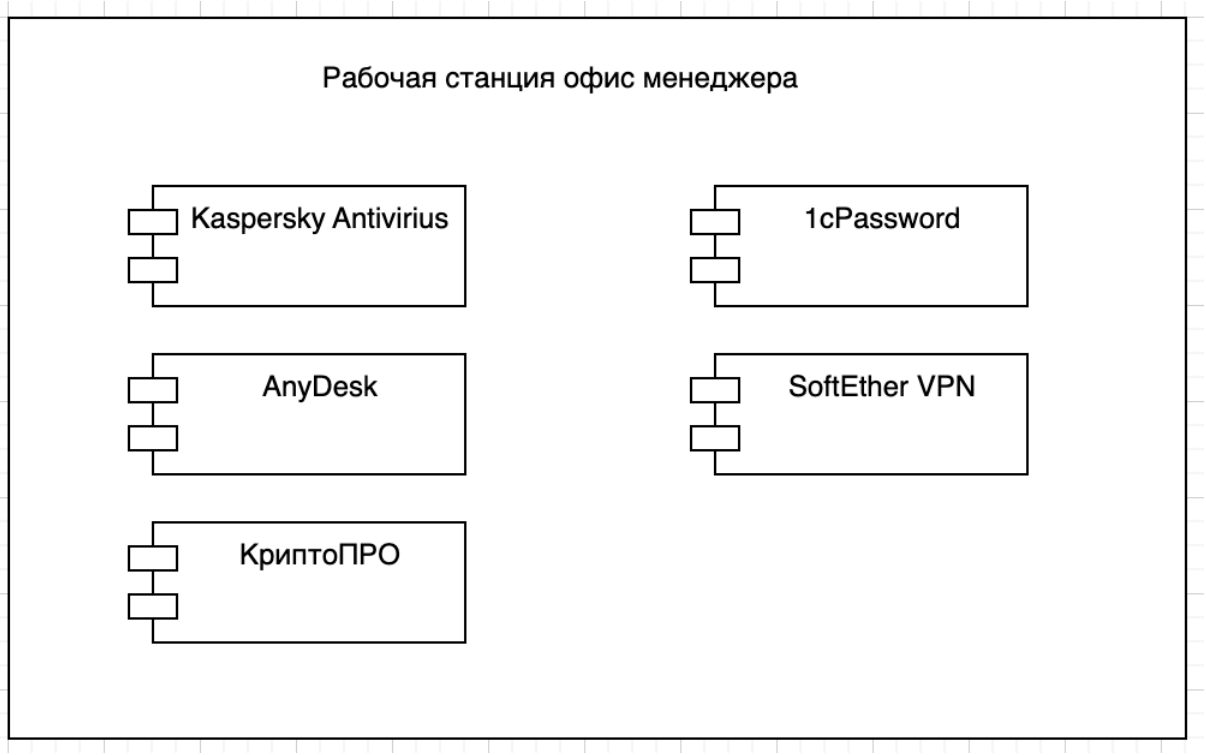
Use-case диаграмма – внешний нарушитель



Описание Use-case диаграмма – внешний нарушитель:

Третьи лица могут воспользоваться нашими услугами, тем самым получить незаконными путями доступ к информации в БД. Они могут украсть, уничтожить, изменить персональную информацию о клиентах и информацию по их заявкам. Также они могут получить информацию о помещении компании, благодаря шантажу сотрудников или если они клиенты компании. Благодаря этому они могут незаконно получить доступ к товарам и тех.оборудованию, тем самым украсть технологии компании по производству линз и технологии по производству заказов. Так же они могут незаконно получить доступ к архивам компании и украсть, уничтожить оригиналы передаточных документов компании, договоров.

5. Диаграммы компонентов



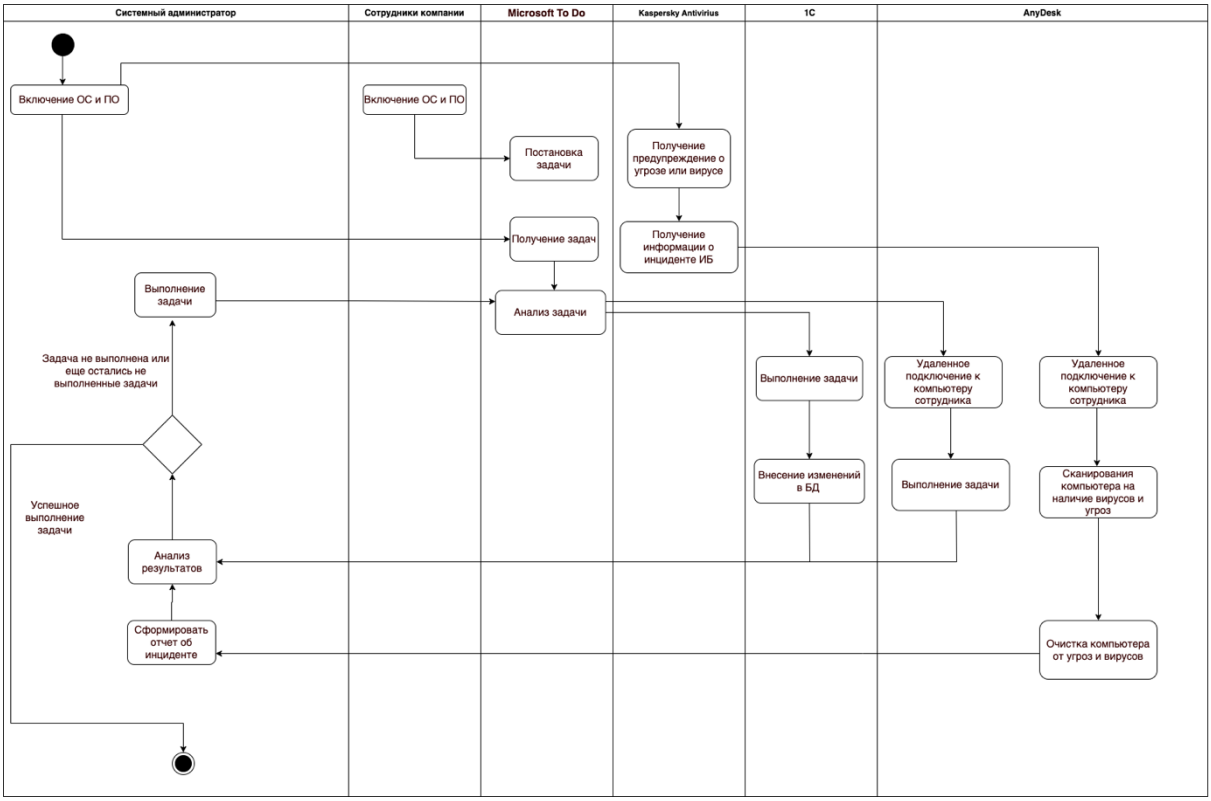
Описание компонентов

1. Kaspersky Antivirius – антивирус. Благодаря гибким условиям тарифам и возможностью управления удаленной настройки антивирусной защиты на компьютерах, которые были активированы с помощью корпоративной лицензии, выбор пал на данный продукт. Также часто обновляются базы данных вирусов и угроз.
2. КриптоПРО - комплекс систем шифрования, для работы с цифровыми подписями. Лицензия для данного ПО предоставляет поставщик электронных подписей. Тем самым это является самым доступным способ работы с эл.подписями.
3.AnyDesk – программа для удаленного доступа к компьютеру. Удобный интерфейс и возможность контроля доступа (подключиться можно только с определенных IP адресов), так же имеет собственное приложение для мобильных телефонов, тем самым IT-сотрудники могут подключиться удаленно к любому компьютеру в офисе и провести обслуживание пк, имея доступ только к своему смартфону.
4. 1cPassword – программа для хранения паролей. Данная программное обеспечение имеет интеграцию с 1с, которая используется в компании. Данный способ хранения паролей удобен и безопасен для сотрудников.

5. SoftEther VPN – VPN для подключения к удаленному серверу, где находится БД. Данное программное обеспечение имеет возможность гибких настроек сервера, настроек доступа, а также возможность создать отдельные аккаунты, для каждого сотрудника компании. Тем самым повышая шанс инфицирования сотрудников, при совершении инцидентов ИБ.

6. Диаграмма активности сотрудников

Для диаграммы активности был выбран системный администратор:



Описание диаграммы активности системного администратора:

После включения ОС и ПО, системный администратор проверяет список задач, которые в свою очередь добавляют пользователи. Если сис.администратор получает уведомление об угрозе или вирусе, то он удаленно подключается к зараженному компьютеру, получает информацию о инциденте ИБ, сканирует компьютер и очищает вирусы или угрозы, пишет отчет об инциденте ИБ. После выполнения задачи, результат анализируется, если задача выполнена, то работа закончена. Если нет, то алгоритм запускается по новой.