МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологий
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой к.п.н., доцент Бердибаев Р.Ш.
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Проектирование системы обеспечения информационной безопасности предприятие

Специальность Системы Информационной Безопасности

Выполнил(а) Еркегалиев Бахтияр Серикович Группа СИБ-16-2
(Ф.И.О.)

Научные руководители: д.т.н., профессор Маркосян М.В., к.п.н., доцент Бердибаев Р.Ш.
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент кафедры БТИЭ Приходько Николай Георгиевич

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: ст.п.,Дмитриева Маргарита Валерьевна
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Рецензент: зав. Кафедрой «Кибербезопасность, обработка и хранение информации» КазНИТУ имени К.И. Сатпаева, к.т.н., доцент
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных Технологий

Кафедра «Системы Информационной Безопасности»

Специальность «Системы Информационной Безопасности»

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Еркегалиеву Бахтияру Сериковичу

(Ф.И.О.)

Тема проекта Проектирование системы обеспечения информационной безопасности предприятие

Утверждена приказом по университету №147 от «11» ноября 2019 г.

Срок сдачи законченного проекта «1» июня 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): – проекция здания «Микрофинансовой организации»:

- уровень защищенности на физическом доступе;
- уровень защищенности программно-аппаратными средствами;
- система контроля управления доступом;
- уровни доступа сотрудников к системам информационной безопасности;
- наличие видеокамер, бесперебойной системы питания организации;
- наличие возможности работать с КИ и документами;
- количество: рабочего персонала, рабочих станций, установленного программного обеспечения.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель дипломного проекта заключается в изучение предметной области, то есть проведение анализа предприятия и выявление недостатков в текущей системе обеспечения информационной безопасности, ну и как следствие организации защите информации, а также активов, представляющие коммерческую тайну и ценность организации. Помимо вышеперечисленного необходимо подробное обоснование выбора основных проектных решений, экономическая эффективности и просчет рисков. В данном дипломном проекте были

разработаны технические и правовые требования для защиты информационных систем.

Перечень графического материала (с точным указанием обязательных чертежей): 56 изображений, 25 таблиц

Основная рекомендуемая литература: Садердинов А.А. Информационная безопасность предприятия, Игнатьев В.А. Информационная безопасность современного коммерческого предприятия, Гришина Н.В. Организация комплексной системы защиты информации

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент кафедры БТИЭ Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Проектирование организации	17.02.2020 – 20.02.2020	
Организации и составление плана по организации СОИБ	21.02.2020 – 28.02.2020	
Физический доступ	01.03.2020 – 08.03.2020	
Политика и концепция безопасности организации	09.03.2020 - 18.03.2020	
Аудит. Стандартный аудит.	19.03.2020 – 27.03.2020	
Организация защиты сети	28.03.2020 - 07.04.2020	
Парольная защита	08.04.2020 - 18.04.2020	
ПО от вторжений (DLP)	19.04.2020 - 30.04.2020	
Рекомендации для организаций по СОИБ	01.05.2020 -	

	09.05.2020	

Дата выдачи задания «7» ноября 2019г.

Заведующий кафедрой _____ (Бердибаев Рат Шындалиевич)
(подпись) (ФИО)

Научный руководитель проекта _____ (Маркосян М.В.)
(подпись) (ФИО)

Задание принял к исполнению студент _____ (Еркегалиев Бахтияр Серикович)
(подпись) (ФИО)

Аннотация

Предметом дипломной работы является процесс организации обеспечения системы информационной безопасности на предприятии, а объектом – «Микрофинансовая организация».

В данном дипломном проекте были разработаны технические требования для защиты информационных систем. Проведено исследование и изучение научного материала по теме исследования, а также нормативно-правовой базы, аналитический и сравнительный методы, методы системного анализа, методы функционального моделирования, экономические и математические методы. Конкретные предложения были подготовлены в соответствии с организационными и техническими требованиями по защите информации.

Аңдатпа

Дипломдық жұмыстың мақсаты кәсіпорында ақпараттық қауіпсіздік жүйесін қамтамасыз етуді ұйымдастыру процесі, ал объект – "Микроқаржы ұйымы" болып табылады.

Бұл дипломдық жобада ақпараттық жүйелерді қорғау үшін техникалық талаптар әзірленді. Зерттеу тақырыбы бойынша ғылыми материалды нормативтік-құқықтық база зерттеліп, аналитикалық және салыстырмалы әдістер, жүйелік талдау әдістері, функционалдық модельдеу әдістері, экономикалық және математикалық әдістер қарастырылды. Нақты ұсыныстар ақпаратты қорғау бойынша ұйымдастырушылық және техникалық талаптарға сәйкес дайындалды.

Abstract

The subject of the thesis is the process of organizing the information security system at the enterprise, and the object is "Microfinance organization".

In this diploma project, technical requirements for the protection of information systems were developed. When writing the diploma project, research and study of scientific material on the research topic, as well as the legal framework, analytical and comparative methods, methods of system analysis, methods of functional modeling, economic and mathematical methods were conducted. Specific proposals have been prepared in accordance with the organizational and technical requirements for the protection of information.

Содержание

Введение

Целью дипломной работы является разработка проекта системы обеспечения защиты информации в «Микрофинансовой организации». Для достижения данной цели были поставлены следующие задачи:

- изучение предметной области и выявление недостатков и уязвимостей в существующей СОИБ и защите информации, определяющих необходимость разработки проекта;
- разработка постановки задачи проектирования;
- обоснование выбора основных проектных решений, а также эффективности проекта в вопросе БЖД и рисков.

Предметом дипломной работы является процесс организации комплексной системы защиты на предприятии, а объектом – «Микрофинансовая организация».

При написании дипломного проекта были применены такие методы исследования, как изучение профессиональной литературы по теме, нормативно-правовые акты, аналитический и сравнительный методы, методы системного анализа, методы функционального моделирования, экономический и математический методы.

На сегодняшний день в мире, рынок информационных технологий стремительно растет, а вместе и с ним люди в чьих экономических и государственных интересах конфиденциальная информация. Всем известно высказывание «Кто владеет информацией, тот владеет миром». Люди в свою очередь обладающие информацией о конкурентах, получает беспрецедентные преимущества в борьбе с ними. Одной из наиболее насущных проблем, решаемых руководством компаний, является сохранение целостности данных. Под сохранением целостности данных понимается не только предотвращение утечки личной и корпоративной информации, отражение атак на систему организации, но и конечно же оптимизация и бесперебойность работы системы в целом. Осталось позади то время, когда на решение ряда определенных задач тратились фантастические средства, развитие не стоит на месте и важно достигать пика результата при минимально возможных вложениях. Неоднородность сфер деятельности и структур организации делает практически невозможным выбор одного универсального решения. Здесь надо мыслить более масштабно и комплексно. Вопрос информационной безопасности становится краеугольным камнем в деятельности организации, но этот же прогресс предлагает решения, способные защитить данные от внешних посягательств.

Прежде чем приступить к созданию какой-либо системы защиты, необходимо произвести общий анализ объекта. Обзор и анализ содержит сведения о том, какие угрозы и уязвимости имеет данное предприятие, а также какие методы защиты нужно применять. В дипломном проекте в качестве объекта защиты будет рассматриваться организация, которой

необходимо внедрить комплексные меры защиты, такие как: корпоративная сеть, физический доступ

При соблюдении методов внутренней и внешней защиты информации, можно обеспечить надежную безопасность.

С этой целью, в данной дипломной работе рассматривается и анализируются вопрос о возможности внешней защиты информации.

Первым делом выбирается рабочее место определенной организации, изучаются источники утечки информации из данного помещения. В ходе этих исследований предусматриваются меры по защите открытых мест в помещении.

Цель проекта: анализ, исследование, практическое внедрение требований к защите информации, мер безопасности и оборудования с целью разработки требований к защите информационных систем на предприятии.

Задача проекта разработка процедур реализации следующих мероприятий:

- предотвращение информационного оттока, хищения, утраты, порчи, внесения изменений;
- предотвращение угроз информационной безопасности личности, предприятия, общества, государства;
- возврат поверхности несанкционированных действий, таких как удаление, модификация, повреждение, копирование, блокирование информации;
- защита информации от незаконных посягательств как объекта собственности; обеспечение защиты информации в соответствии с законодательством РК.

Актуальность темы проекта: реализация обеспечения системы защиты информации-разработка требований к защите информации; параллельная разработка технических мер защиты здания или помещения от внешних и внутренних угроз. Таким образом, закрытие каналов утечки информации, умение на практике демонстрировать ее и свободно внедрять в учебный процесс.

Современный этап развития информационных технологий тесно связан с развитием техники, которая широко применяется во всех отраслях жизнедеятельности. Большое количество обрабатываемой информации и большое количество ее видов не вызывают внешнего интереса к ней. В связи с этим в настоящее время, в целях обеспечения безопасности пользователей и информации на компьютерах, от сети до сих пор рассматриваются возможности защиты информации от угроз, возникающих на компьютере. Мы должны иметь в виду, что опасность для информации возникает со стороны простых пользователей, через корпоративную сеть. Также не стоит забывать, что «источником утечки информации» может быть помещение, где хранится и обрабатывается конфиденциальная информация. Есть источники, представляющие опасность информации, позволяющие ее похищать.

1 Анализ предметной области

1.1 Постановка задачи

Одной из главных целей разработки системы обеспечения информационной безопасности – это снизить и минимизировать уровень рисков по каждому активу и по всем информационным объектам в совокупности, которые представляют ценность для злоумышленников. Таким образом, необходимо решить следующий комплекс задач:

- возможность самостоятельно в привычной терминологии запрашивать, согласовывать и получать доступ к необходимым информационным ресурсам;
- возможность работать с конфиденциальной информацией и документами без нарушения уровня защиты и ее целостности;
- возможность непрерывно контролировать все изменения прав доступа к информационным ресурсам части и другие изменения значимых настроек; иметь всю необходимую информацию для оперативного реагирования на инциденты с последующим её расследованием, связанных с несоблюдением правил внутренней политики и концепции безопасности предприятия.

В первой части дипломной работы необходимо произвести анализ деятельности «микрофинансовой организации», описать и проанализировать ИС, выявить информационные активы организации, оценить главные угрозы данным активам, произвести анализ рисков.

Основываясь на проведенном анализе необходимо определить наиболее ценные активы и наиболее вероятные риски.

Помимо этого, нужно провести анализ текущей СОИБ, выявить наиболее насущные вопросы и уязвимые места, а также определить необходимые шаги по улучшению системы безопасности «микрофинансовой организации» для обеспечения достаточного уровня ИБ.

1.2 Краткая характеристика «микрофинансовой организации»

Объектом исследования в дипломной работе является «микрофинансовая организация», которая осуществляет следующую деятельность:

- оказание финансовых услуг;
- финансирование субъектов малого предпринимательства;
- финансирование малых предприятий;
- финансово-кредитные отношения с малыми хозяйствованиями;
- оказание помощи начинающим предпринимателям в приобретении опыта получения прибыли и накопления капитала.

«Микрофинансовая организация» состоит из одноэтажного здания, с прилежающей рядом парковкой для клиентов и сотрудников организации.

Схема расположения объектов на территории организация представлена на рисунке 1.1.

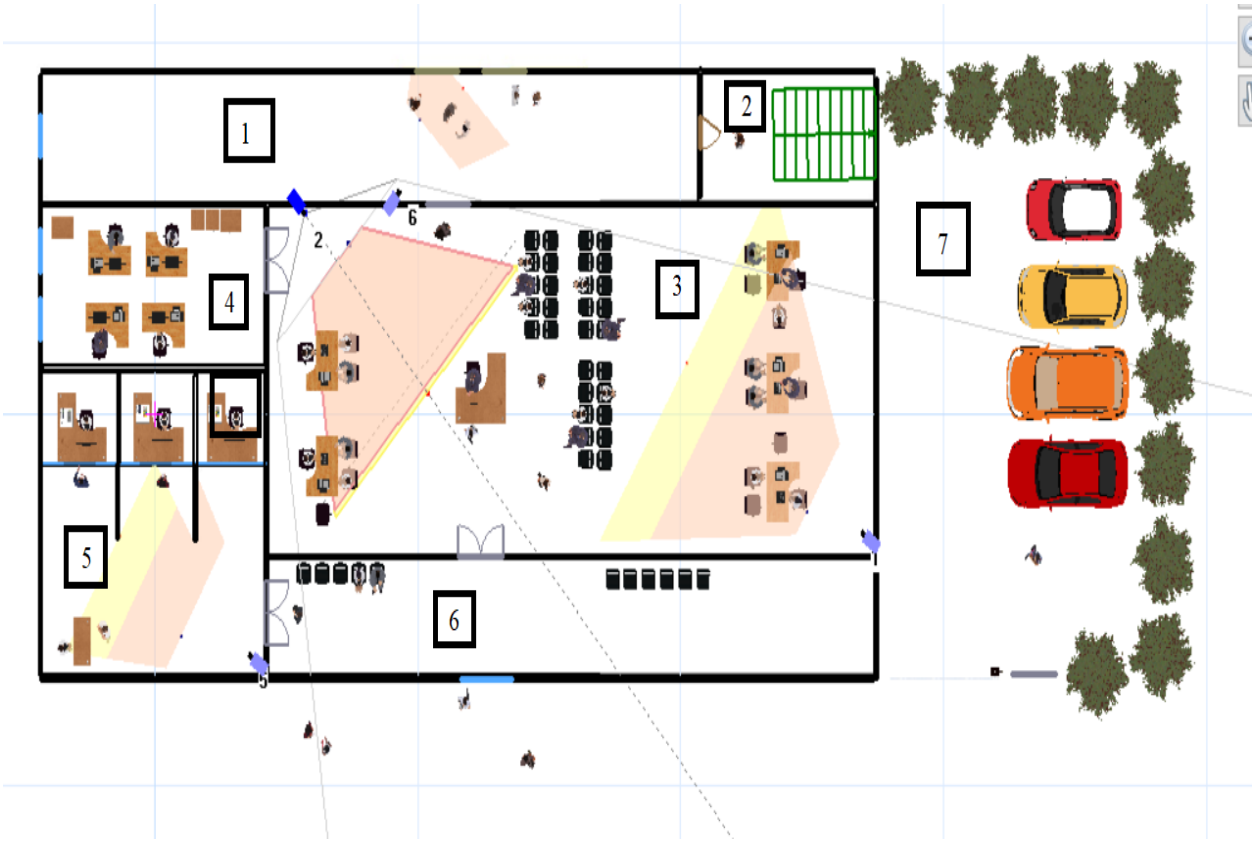

Рисунок 1.1 – схема расположения объектов

Одноэтажная организация располагается в здании площадью порядка 400. На одном этаже здания находятся: коридор, подсобное помещение, операционный зал, канцелярия, зал с кассами, коридор и прилегающая парковочная зона. Численность компьютеров, ноутбуков, планшетов в служебных помещениях около 50 шт. Ещё одна задача, которая возникает, это необходимость обеспечения доступа мобильных устройств к единой сети, а также обеспечения работоспособности.

1.3 Характеристика ИС «микрофинансовой организации».

Информационная система данной «микрофинансовой организации» представляет собой взаимосвязанный комплекс средств и мер, методов и сотрудников, используемых для хранения, обработки, и передачи конфиденциальной информации в интересах достижения поставленным задачам. [2, с.34]

У каждого сотрудника в организации имеется свое рабочее место, которое оснащено ПК. Помимо этого в организации имеются универсальные гаджеты. На каждую рабочую станцию внедрен комплект инструментов необходимого ПО. Структура стандартного рабочего места сотрудника продемонстрирована в таблице 1.1.

Таблица 1.1 – Состав рабочего места специалиста

Наименование подсистемы	Наименование компонента	Количество
Процессор	Intel Core i5 950 3267MHz,8Mb, WPX1347	1
Системная плата	ASUS P2D Delux V4, Intel X97	1
Оперативная память	6Gb (3*2Gb) DDR3 1600Mhz Corsair XMS3	1
Накопители HDD	1TB Western Digital-II 32mb	1
Видеокарта	1280Mb NVIDIA GeFor	1
Корпус без БП	MiditGigaByte GZ-GX9 Black ATX	1
Манипулятор	Defender Pluto 310 B, USB+PS⁄2	1
БП	Corsair CMPSU-850TX 850W	1
Клавиатура	KBS-8:Ветви сакуры	1
Видеомонитор	16" MONITOR ASUS VH232T BK	1

«Микрофинансовая организация» как и говорилось ранее, состоит из одноэтажного здания. Для организации сети используется топология «звезда», причем в каждом помещении или кассе, где число компьютеров превышает одного, имеется концентратор, он необходим для соединения рабочих станций внутри кабинета.

Все концентраторы подключаются к концентратору, находящемуся в подсобном помещении техников. Таким образом, в организации используется сеть «иерархическая звезда». Все компьютеры обладают одинаковыми характеристиками. Компьютеры в сети имеют типовую сетевую карту с разъемом RJ45 и сетевую операционную систему. В каждом кабинете расположены концентраторы SuperStack II Hub 100 Base T4 производства 3Com Corp. Техническая архитектура предприятия (на примере одного этажа) представлена на рисунке 1.2.

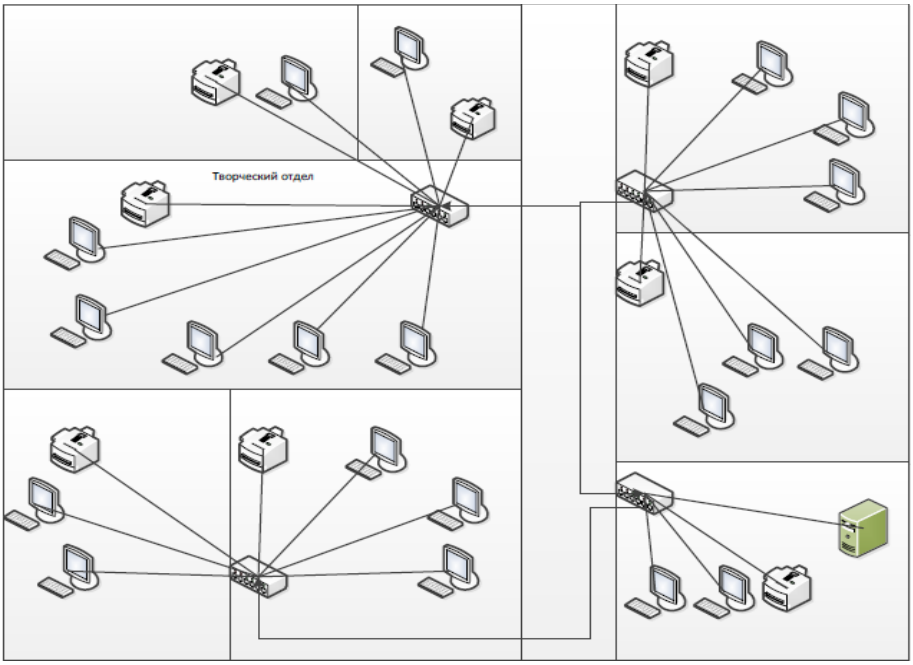

Рисунок 1.2 – Техническая архитектура «микрофинансовой организации»

В данной организации сотрудники пользуются разными по свойствам и функциям программными продуктами. Программные решения «микрофинансовой организации» продемонстрирована на рисунке 1.3.

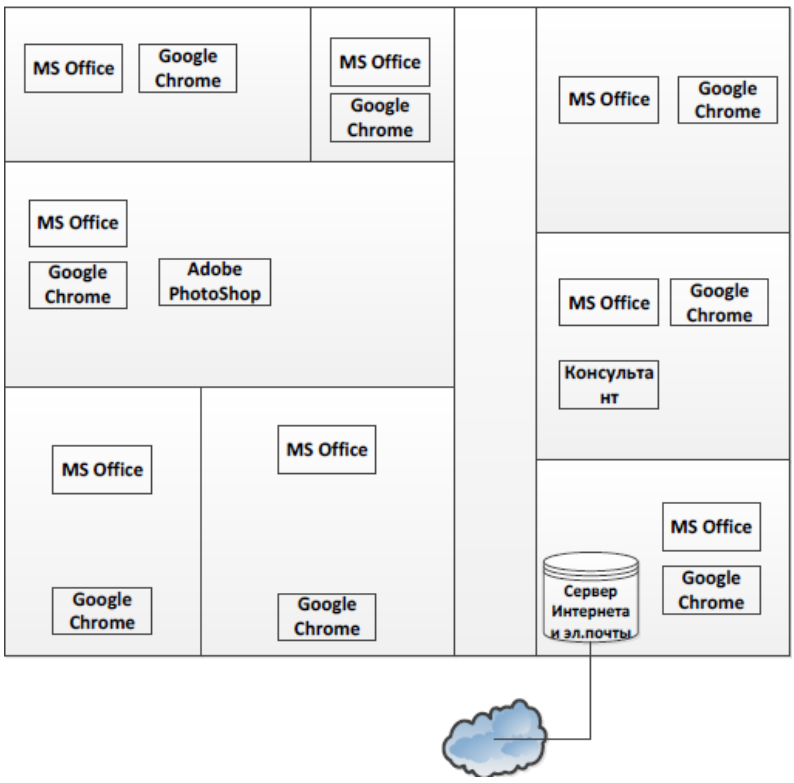

Рисунок 1.3 – Программная архитектура «микрофинансовая организация»

ПО организации включает в себя комплекс программных решений для реализации целей и задач ИС, связанных с главной отраслью компании, а также для нормального функционирования комплекса ТС. [14, с.21] Системное программное обеспечение компьютеров представлено в таблице 1.2.

Таблица 1.2 – Основное системное программное обеспечение

Обозначение	Количество
Операционная система Windows 7 Корпоративная	16
Антивирус ESET Nod32	16
Архиватор WinZip	16

Также в широком применении находят себя различного рода архиваторы, такие как: Rar, WinZip, WinRar. Всеми сотрудниками используется базовый текстовый редактор MicrosoftWord. В процессе работы, работники сталкиваются с необходимостью тщательного разбора и мониторинга всевозможных данных. Поэтому применение находит табличный редактор MicrosoftExcel, который позволяет реализовать наиболее «популярные» способы обработки результатов исследований.

Ещё один, не менее необходимый программный продукт, необходимый для «микрофинансовой организации» это 1С: «Бухгалтерия», данный продукт является общетиповым решением для автоматизации процесса бухгалтерского и налогового учета, включая подготовку обязательной отчетности. Конфигурация «Бухгалтерия» организации позволяет реализовать любую схему учета и может использоваться как автономно, так и совместно с другими компонентами.

Компьютеры подключаются к сети на основе технологии WiMAX. Схема сети представлена на рисунке 1.4.

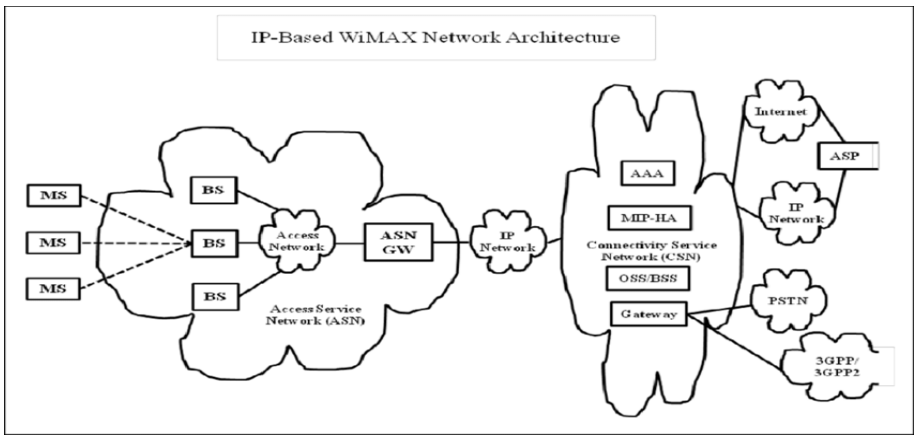

Рисунок 1.4 – Архитектура сети WiMax

Для организации такой сети на основе WiMAX были реализованы следующие задачи:

- заключение делового договора на получение услуг от поставщика;
- внедрение устройства WiMAX роутер, который обеспечит подключение всех устройств к единой сети;
- на каждое устройство установлены адаптеры, организованы точки доступа;
- установлены параболические антенны для усиления сигналов точек доступа, для более быстрой и качественной связи, удаленных компьютеров;
- все устройства и периферийное оборудование, находящиеся в здании, подключены к роутеру (маршрутизатору);
- настроена сеть Интернет, локальная сеть, принт-сервер.

Для того, чтобы можно было использовать локальную сеть и принт-сервер, был выбран гибридный роутер, модель которая позволит работать в сетях WiMax и Wi-fi. Этот роутер должен распространять Интернет между всеми компьютерами по технологии WiMax, а для организации локальной сети и принт-сервера будет использоваться технология Wi-fi.

Так как на 1 этаже здания организации, помимо рабочих кабинетов и касс, есть также и операционный зал, она же гостевая зона, где потенциальные клиенты находятся, ожидая свою очередь, то необходимо обеспечить общий доступ на использование интернета для гостей, но ограничить их доступ в локальную сеть. Всех посетителей «микрофинансовой

организации» со своими устройствами, которые оснащены модулями WiMax, которым необходимо воспользоваться услугой беспроводного интернета, нужно помещать в гостевую зону, которая будет ограничивать их, предоставляя им определенную скорость и запрашивая пароль доступа к системе, который они будут получать только при введение своего номера телефона, на который в течении минуты приходит код для аутентификации.

Для подключения устройств к единой сети на основе WiMAX были дополнительно приобретены адаптеры и точки доступа. Для организации сети было приобретено оборудование, перечень которого показана в таблице 1.3.

Таблица 1.3– Перечень оборудования для организации сети

Наименование	Кол-во	Дальность (м.)	Предназначение
Беспроводной USB-адаптер 802.11g, до 108 Мбит/с dwa-120	30	100	Внедряется в ПК для связи с беспроводными сетями
AirPremier N внешняя двухдиапазонная беспроводная 2,4 ГГц (802.11b/g/n)/ 5 ГГц (802.11a/n) точка доступа с поддержкой PoE, до 300 Мбит/с DAP-3520	2	100	Точка доступа Wi-Fi для связи между компьютерами внутри сети
RangeBooster N беспроводной 2,4 ГГц (802.11n) USB-адаптер, до 300 Мбит/с dwa-120	1	100	Передача больших объёмов информации

Роутер (или маршрутизатор) – устройство, служащее обеспечению многих функций, таких как: коллективный доступ в Интернет, IP-телефония и построение локальных сетей LAN. Именно роутер обеспечивает подключение всех устройств к единой сети и организации трафика между ними. Для организации сети понадобится роутер, характеристики которого показаны в таблице 1.4.

Таблица 1.4 – Перечень оборудования для организации сети

Наименование	Кол-во	Дальность (м.)	Предназначение
Роутер ASuS WX 500MWiMAXWi-fi до 20 mbit	1	100	Доступ в интернет. Преобразование сигнала в Wi-fi

При использовании этой модели роутера, скорость соединения с интернетом WiMAX доходит до 20 Мбит/сек. Данная модель маршрутизатора, поддерживающий 802.11n — универсален: он соединяется

также и с 802.11b/g, то есть может использоваться при передаче мультимедиа потоков.

Одной из основных задач проектируемых сетей – это необходимость обеспечивать хороший уровень сигнала. Однако, в связи с тем, что сеть охватывает большие расстояния, сигналы при передаче невольно могут ослабляться. Для того чтобы усилить сигнал точек доступа, надо использовать параболические антенны. Перечень оборудования приведен в таблице 1.5.

Таблица 1.5– Перечень оборудования для организации сети

Наименование	Количество	Дальность (м.)	Предназначение
Параболическая антенна с высоким коэффициентом усиления, 21 dBi ANT24-1800	4	100	Усиления сигнала точек доступа и удалённых компьютеров

D-Link ANT24-2100 подключается к беспроводным устройствам D-Link стандартов 802.11b и 802.11g (2.4 ГГц) и имеет коэффициент усиления 21 dBi.

Пассивная антенна также может быть подключена к беспроводному оборудованию 802.11b и 802.11g других производителей. D-Link ANT24-2100 предоставляет возможность существенно расширить площадь покрытия существующей беспроводной сети и/или создать беспроводной мост для передачи данных на большие расстояния.

На предприятии используется система видеонаблюдения для защиты конфиденциальной информации. Проанализируем существующую систему видеонаблюдения. Компания расположена на четырех этажах. Схема расположения видеокамер на первом этаже представлена на рисунке 1.6.

Пассивная антенна также может быть подключена к беспроводному оборудованию 802.11b и 802.11g других производителей. D-Link ANT24-2100 предоставляет возможность значительно расширить площадь покрытия существующей беспроводной сети или создать беспроводной мост для передачи данных на большие расстояния.

1.4 Анализ деятельности организации, выявление проблем ИБ

Необходимо рассмотреть идентификацию и оценку информационных активов предприятия. Активы (ресурсы) – это все, что имеет ценность или находит полезное применение для предприятия, ее деловых операций и обеспечения их непрерывности. Надлежащее управление и учет активов должны являться одной из основных обязанностей руководителей всех уровней в организации. [1] К одним из главных активов относятся информация, инфраструктура, рабочий персонал. Без инвентаризации активов на уровне служебной деятельности невозможно ответить на

поставленный вопрос, что именно крайне необходимо защищать в первую очередь.

Были выявлены следующие потоки информации:

- личные дела рабочего состава «микрофинансовой организаци»;
- информация о уже зарегистрированных клиентах организации;
- данные о сооружении и материальном обеспечении организации;
- данные по приказам, распоряжениям, мероприятиям, распорядку «микрофинансовой организации»;
- бухгалтерский учёт и управленческая отчетность.

Перечень информационных активов, обязательное разграничение доступа для сотрудников, к которым регламентируется действующим законодательством и правовыми актами РК, сведены в таблицу 1.6.

Таблица 1.6 – Перечень сведений конфиденциального характера

Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, № статей
Сведения, раскрывающие характеристики средств защиты ЛВС организации от НСД	Конфиденциально	Устав, политика и концепция информационной безопасности «микрофинансовой организации»
Требования по обеспечению сохранения служебной тайны работниками организации.	Конфиденциально	Закон Республики Казахстан от 24 июня 2002 года № 330-II секреты производства
Персональные данные полного состава сотрудников организации	Конфиденциально	В соответствии с Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»

Результат ранжирования активов представляет собой интегрированную оценку степени важности актива для предприятия, взятую по пятибалльной шкале. Ранжирование рисков представлено в таблице 1.7.

Таблица 1.7– Результаты ранжирования активов

Наименование актива	Ценность актива (ранг)
ПО организации	11
Сотрудники	10
Компьютерные средства	9
Информационные услуги	4
Текстовые сообщения	12
Личные дела сотрудников	6
Переписка внутри организации	8

Информация об аппаратуре внутри организации	2
Данные о сооружении здания и материальном положении «Микрофинансовой организации»	3
Инвентаризационная ведомость	7
Приходные накладные	4
Бухгалтерский учет и налоговая отчетность	5

Таким образом, были отмечены активы, имеющие наибольшую ценность: личные дела сотрудников, информация об аппаратуре внутри организации, данные о сооружении здания и материальном положении «Микрофинансовой организации».

Необходимо также рассмотреть процесс управления рисками.

Уязвимость – это событие, которое возникает как результат некоторого стечения обстоятельств, когда в силу каких-то причин используемые в системах обработки данных средства защиты информации не в состоянии оказать достаточного сопротивления различным дестабилизирующим факторам и нежелательного их воздействия на информацию, подлежащую защите.

Уязвимости информационной системы организации выявляется несколькими способами. Их может описать сотрудник компании (инженер, системный администратор или специалист службы информационной безопасности) на основании собственного опыта. Кроме того, могут быть приглашены сторонние специалисты для проведения технологического аудита информационной системы и выявления ее уязвимостей.

Угроза – это потенциальная причина инцидента, который может нанести ущерб системе или организации.

Инцидент информационной безопасности – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность организации или информационную безопасность.

Существуют пассивные и активные угрозы. Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов информационной системы, не оказывая при этом влияния на саму информацию, не вызывая искажений и нарушений информации. К пассивной угрозе можно, например, отнести прослушивание каналов связи, просмотр баз данных.

Далее осуществляется оценка существующих и планируемых средств защиты информации.

Задачи по обеспечению защиты конфиденциальной информации лежат на плечах сотрудников технического отдела части, а также на руководителей подразделений. Результаты оценки существующей системы обеспечения безопасности информации, демонстрирующие, насколько полно выполняются примитивные объективные функции при решении возникновении задач информационной безопасности, представлены в таблице 1.8.

Таблица 1.8 – Анализ выполнения задач по обеспечению ИБ

Основные задачи по обеспечению информационной безопасности	Степень выполнения
1 Обеспечение безопасности процесса управления «Микрофинансовой организации», защита информации и данных, являющихся коммерческой тайной и которая существенно может нанести вред деятельности организации, а также повлиять на авторитет организации	средняя
2 Организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной) защите коммерческой тайны	средняя
3 Организация специального делопроизводства, исключающего несанкционированный съём конфиденциальных данных, относящихся к тайным	средняя
4 Предотвращение преднамеренного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну для «Микрофинансовой организации»	низкая
5 Выявление и ликвидация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной работы, а также утечка техногенного и/или природного характера (авария, пожар и др.)	средняя
6 Обеспечение полной безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством, либо при заключении договора с подрядными организациями	высокая
7 Обеспечение физической охраны территории, здания, с защищаемой информацией	высокая

В первую очередь необходимо обратить внимание на те аспекты защиты информации, которые характеризуются низкой и средней степенью выполнения. Кроме того, важно обеспечить комплексный характер защиты.

1.5 Выводы

На основании оценки рисков наиболее ценным, для «микрофинансовой организации», информационным активам были выбраны главные задачи по модернизации системы обеспечения информационной безопасности.

Обеспечение целостности, доступности для сотрудников, а также конфиденциальности активов возможно за счет внедрения антивирусной защиты и не только. Помимо этого, важно проработать систему наблюдения

за рабочими станциями, чтобы максимально быстро и в короткое время среагировать, и локализовать вирусное и вредоносное ПО, также чтобы оно не могло быть принесено на флэшке или другом съёмном носителе информации.

Внедрением системы защиты на предприятии будет заниматься системный администратор (подбор, анализ установка, настройка и обслуживание технических и программных средств защиты), а также начальник службы безопасности (разработка положений, концепции, политики, приказов, распоряжений).

Решение задачи обеспечения информационной безопасности является критично необходимой для функционирования «микрофинансовой организации», поскольку есть вероятность распространения очень важных данных. Потеря информации приведет к выходу всей системы из строя, потере эффективности работы, разглашению служебной информации.

2 Разработка комплекса мер по обеспечению защиты информации

2.1 Постановка задачи

На основе проведенного в первой главе подробного анализа были выдвинуты следующие системы мер для обеспечения информационной безопасности «Микрофинансовой организации»:

а) технические меры защиты информации:

1) аппаратные меры защиты информации;

2) внедрить источник бесперебойного питания для сервера;

3) сменить старые и внедрить новые видеокамеры в организацию;

4) приобрести сейфы и другие устройства для хранения ценных документов;

б) программные меры защиты информации:

1) внедрить систему SpiceWorks;

2) установить программное средство SpiceWorks;

3) установить на рабочие места пользователей антивирусные пакеты. Наиболее удобной будет такая система: на сервере устанавливается антивирус-сервер, а на рабочих местах – клиентские приложения, работой которых управляет сервер. Это сравнительно недорогое решение, а главное, что администратор сможет управлять проверкой всех компьютеров с сервера;

4) усовершенствовать политику парольной защиты. Предлагать сотрудникам смену пароля раз в месяц, рекомендовать использование сложного пароля, с добавлением элементов разных символов, а также заглавных букв;

5) выполнить разграничение доступа к документам на сервере;

6) выделять разное количество трафика разным группам пользователей интернета, а также определить некоторый набор ресурсов, к которым можно получить доступ.

При введении этих мер необходимо взять у сотрудников каждого отдела письменное соглашение о соблюдении правил работы с информацией и техникой, которые могут быть изложены в трудовом договоре или отдельным документом, а также взять роспись на соглашение о персональной ответственности в случае не соблюдении данных мер по обеспечению информационной безопасности.

Существуют три основные стратегии системы обеспечения информационной безопасности: оборонительная, наступательная, упреждающая.

В рамках данной «микрофинансовой организации» была выбрана наступательная стратегия ИБ. Эта стратегия предполагает реакцию персонала организации на одни из распространенных угроз, которые оказывают наиболее сильное влияние на информационную безопасность организации. Наступательная стратегия предусматривает применение таких мер, как установка дополнительных программно-аппаратных средств аутентификации и авторизации сотрудников, внедрение гораздо лучшиъ технологий разгрузки

и восстановления данных, увеличение доступности системы с использованием горячего и холодного резервирования.

2.2 Комплекс организационных мер СОИБ организации

В Республике Казахстан к нормативно-правовым актам в области информационной безопасности относятся акты республиканского законодательства:

а) конституция РК;

б) законодательство Республики Казахстан (включая законодательно конституционные законы, кодексы);

в) указы Президента РК;

г) постановления правительства РК;

К нормативно-методическим документам можно отнести:

а) методические документы государственных органов Казахстана:

б) закон РК «Об информатизации»;

в) закон РК «О национальной безопасности Республики Казахстан»;

г) закон РК «О персональных данных и их защите»;

д) закон РК «О коммерческой тайне»:

1) концепция информационной безопасности РК;

2) руководство имеющимся международным опытом в области обеспечения информационной безопасности РК;

е) стандарты ИБ, из которых выделяют:

1) международные стандарты (ISO/IEC 27000, BS 7799;

2) государственные стандарты РК (СТ РК 1697-2007);

3) рекомендации по стандартизации;

4) «О концепции информационной безопасности Республики Казахстан» (Указ Президента Республики Казахстан от 14 ноября 2011 года №174). [3]

Защита конфиденциальной информации предусматривает селекцию различных мер по обеспечению СОИБ. По статистике, нарушения в сфере ИБ совершаются, как правило, преимущественно, сотрудниками предприятия/организации (81%) или прежними его сотрудниками (6%). Процентное соотношение нарушений информации, произведенных разными группами лиц, представлено на круговой диаграмме на рисунке 2.1.

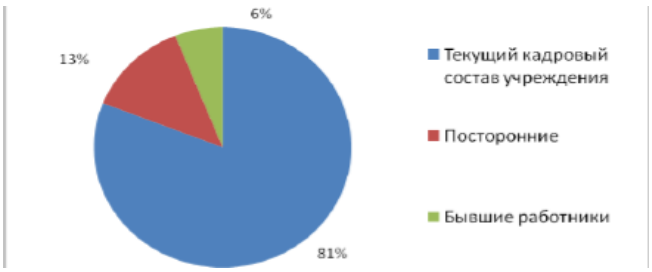

Рисунок 2.1 – Процентное соотношение нарушений целостности и доступности информации произведенных разными видами нарушителей

Таким образом, руководствуясь статистикой, можно сделать вывод, что примерно 80% всех преступлений в сфере информационной безопасности, а именно нарушения конфиденциальной информации осуществляются либо работниками организации, либо с их помощью, а иногда и вследствие халатности и невнимательности работников. Именно поэтому крайне необходимым направлением обеспечения защиты конфиденциальной информации является административная ИБ, которая снабжается за счет применения организационных мер. Организационные параметры предусматривают внедрение безопасных способов ведения документации, применение методов разработки, внедрения и тестирования дополнительных программных средств, а также процедур обработки инцидентов в случаях нарушения систем безопасности. Обеспечение административной составляющей информационной безопасности предполагает также выбор определенной стратегии защиты информации в компании.

К организационно-административным мероприятиям защиты информации относятся:

- выделение специальных защищенных помещений для размещения ЭВМ и средств связи, и хранения носителей информации;
- выделение отдельных ЭВМ для обработки конфиденциальной информации;
- организация укрытия конфиденциальной информации на специальных промаркированных съёмных носителях;
- эксплуатация в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;
- организация специального делопроизводства для конфиденциальной информации регулирующего порядок подготовки, использования, сохранения, уничтожения и учета документированной информации;
- организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;
- установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;
- разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех отделов объекта защиты в процессе обработки, хранения, передачи и использования информации;
- постоянный контроль за соблюдением установленных требований по защите информации.

На основе анализа существующей системы безопасности было выдвинуто решение на реализацию административных мер безопасности:

а) разработать и утвердить приказом по предприятию:

1) положение о защите данных, содержащих коммерческую тайну, и другой информации ограниченного пользования, определённые законодательством РК;

2) инструкцию по правилам работы со сведениями, содержащими коммерческую тайну;

3) инструкцию по делопроизводству с документами ограниченного пользования;

б) издать приказ по предприятию, в котором:

1) на руководителей подразделений возложить обязанность проведения мероприятий, направленных на обеспечение сохранности коммерческой тайны;

2) определить меры административного наказания за нарушение правил работы с документами и сведениями, содержащими коммерческую тайну;

3) на службу безопасности возложить обязанность по выявлению возможных нарушений, в результате которых возможна утечка охраняемых сведений;

в) ввести запрет на хранение личной информации на компьютере;

г) установить правила копирования документов, исключающих изготовление копий важных документов без санкции руководителя;

д) от работников, по должности обладающих сведениями коммерческой тайны, при заключении трудового договора брать письменные обязательства о неразглашении. В случае увольнения работника, требовать от него передачи всех носителей информации, составляющих коммерческую тайну, которые находились в его распоряжении;

е) изготовить выписки, содержащие выдержки из положения о конфиденциальной информации для использования работниками в повседневной деятельности;

ж) разработать журнал учета персональной информации;

и) разработать правила работы с электронной почтой;

к) при включении компьютера перед вводом пароля программным способом выдавать пользователю сообщение, напоминающее пользователю о правилах работы с компьютером. Организационно-административные меры защиты информации позволят избежать части непреднамеренных угроз, а также преднамеренных угроз безопасности информации со стороны работников предприятия. Кроме того, грубый регламент обращения с информационными ресурсами дисциплинирует сотрудников, приучает их более внимательно работать с открытой информацией и относиться к ней как к ценному ресурсу. [5]

2.3 Комплекс проектируемых программно-аппаратных средств СОИБ организации

Следует приступить к реализации инженерно-технических мер для СОИБ организации. В результате проведения внешнего аудита

информационной безопасности «микрофинансовой организации», были выявлены основные пробелы информационной системы видеонаблюдения. Учитывая вышеперечисленное, разработаны меры для повышения эффективности функционирования системы видеонаблюдения организации:

а) замена более устаревших моделей видеокамер на новые, адаптивные;

б) установка камер в помещении здания и на прилегающей парковке, а также территорию по периметру здания организации;

в) замена монитора видеооператора;

г) установка сервера в подготовленном помещении с ограниченным доступом для рядовых сотрудников организации;

д) установка видеомонитора в центральном помещении организации;

е) замена программного обеспечения вывода видеосигнала;

ж) замена соединительного кабеля, а также обоснование типа кабеля.

Далее будет проведена прокладка кабелей, расчет трафика и объема диска для видеонаблюдения. Благодаря предложенным мероприятиям будет развернута эффективная система видеонаблюдения внутри организации, которая значительно уменьшит риски на потерю конфиденциальной информации. Рассмотрим более подробно, что будут охватывать в себя предложенные мероприятия.

Первое – это замена устаревших камер. Срок службы электронных компонентов системы охранного видеонаблюдения в среднем составляет порядка 7 лет. В организации используются камеры производителя mintron. На основании документации о монтаже системы видеонаблюдения, закупленные камеры были не новыми. Уже использовались ранее, т.е. срок их службы может быть более 7 лет. Для замены данных видеокамер выбраны взрывозащитные камеры производителя Relion. Видеокамеры модели Relion отличаются повышенной чувствительностью и разрешением, что позволит в более качественном виде производить видеофиксацию.

Второе – это установка камер в кабинетах организации. Для установки камер в кабинках касс организации было принято решение выбрать камеру Relion-Trassir -H-50-IP-4MP. Видеокамеры серии Relion-Trassir -H-50-IP-4MP обладают повышенной чувствительностью и разрешением. Эта модель видеокамеры зарекомендовала себя как очень надежная и неприхотливая. Она способна дать четкое и контрастное изображение и обладает очень умеренными габаритами. Производитель фирма Relion (Россия), разрешение FullHD (1920×1080). Объектив фиксированный 3,6 мм., чувствительность 0,005 лк. Питание 12V DC. Маркировка взрывозащиты 1Ex. Камера близка по своим характеристикам других камер данной фирмы и серии. Основное отличие – это меньшие габариты, но несколько более высокая цена. Между собой видеокамеры серии Relion-Trassir отличаются объективами и чувствительностью. В комплекте с камерой входит П-образный кронштейн.

На предприятии используется система видеонаблюдения для защиты конфиденциальной информации. Необходимо проанализировать

существующую систему видеонаблюдения. Компания расположена на одном этаже. Схема расположения видеокамер представлена на рисунке 2.2.

Рисунок 2.2 – Схема расположения камер внутри организации

Стоит отметить, что система видеонаблюдения включает камеры в коридорах, в гостевом зале (операционный зал), в зале с кассами, но не предполагает видеонаблюдения непосредственно в кабинках каждого кассира, в канцелярии, ну и у входа в здание, то есть камеры на парковочную зоне также нет. В связи с тем, что необходимо обеспечить защиту целостности и конфиденциальности обрабатываемой информации, с которыми сотрудники «микрофинансовой организации» ежедневно работают в кабинетах, необходимо обеспечить видеонаблюдение внутри рабочих кабинок. Т.к. имеется 3 кабины с кассирами, то требуется установить дополнительно туда, а также две камеры по периметру здания. Дополнительно внедренные камеры продемонстрированы на рисунке 1.6.

Кабины касс. Причина установки камеры: кассовый узел интересует в первую очередь грабителей банка. Помимо внешних угроз, здесь необходимо уделять пристальное внимание работе с персоналом и внедрять строгие регламенты обращения с ценностями. В кабинах установлены камеры модели Relion-Trassir -H-50-IP-4MP, как показано на рисунке 2.3 (на рисунке добавляемые камеры выделены красным квадратом).

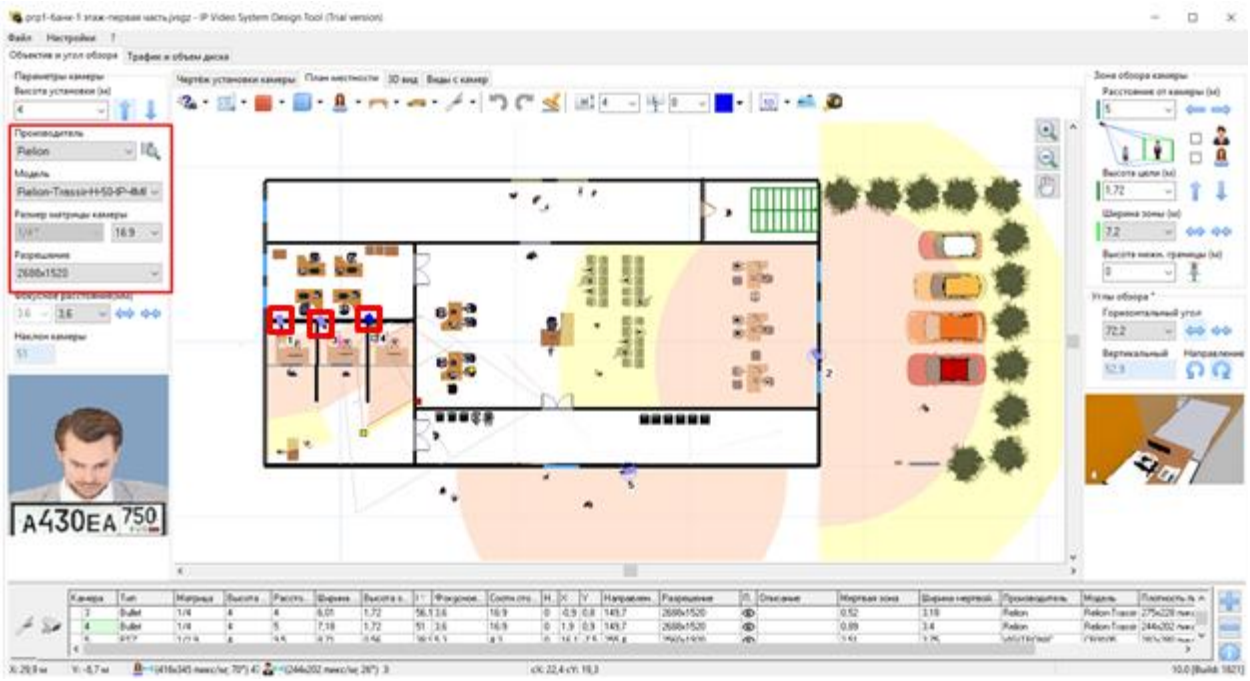

Рисунок 2.3 – Установка камер в кабинах касс

Relion-Trassir -H-50-IP-4MP (кол-во: 3) - IP-видеокамера с разрешением 4 Мп и питанием по технологии PoE, взрывозащищённая со встроенной ИК-подсветкой для систем охранного и технологического видеонаблюдения во взрывоопасных зонах. Внешний вид камеры показан на рисунке 2.4.

Рисунок 2.4 – Relion-Trassir -H-50-IP-4MP

Технические характеристики:
- маркировка взрывозащиты: PB Exd I / 1ExdIICT5/T6;
- температурный диапазон, ºС: -40 ÷ +60;
- для взрывоопасных зон классов: «1» и «2»;
- материал корпуса: Нержавеющая сталь 08Х18Н10Т;
- мощность потребления, не более, Вт: 4;
- макс. ток потребления, А: -;
- степень защиты оболочкой по ГОСТ 14254, не ниже: IP68;
- подключение: Внутренний клеммный отсек;

- режим работы: непрерывный;
- разрешение, Мп: 4;
- матрица: 1/3" CMOS 4 Мп;
- система сканирования: Прогрессивная развёртка;
- тип объектива: Фиксированный мегапиксельный;
- фокусное расстояние объектива, мм: 3,6;
- порог включения ИК-подсветки, лк: 3;
- количество ИК-излучателей: 2;
- дальность ИК-подсветки, до, м: 20;
- компенсация засветки: BLC;
- шумоподавление: 3DNR;
- динамический диапазон: REAL WDR 120Дб;
- дополнительные функции: Функция "Антитуман"ROI до 4-х зон H.264/H.265;
- функция день/ночь: Механический ИК-фильтр (ICR);
- минимальная чувствительность, лк: 0,005;
- питание: PoE;
- масса видеокамеры, не более, кг: 6,9.

Особенности:

- маркировка взрывозащиты PBExdI / 1ExdIICT5/T6 позволяет применять видеокамеру во взрывоопасных зонах классов «1» и «2», а также в подземных выработках шахт, рудников и их наземных строениях;
- два встроенных ИК-излучателя с фокусирующими линзами обеспечивают круглосуточное качественное видеонаблюдение в зонах с недостаточным освещением или отсутствием освещения в темное время суток на расстоянии до 20 метров;
- полная пыле и водонепроницаемость позволяет применять видеокамеру в помещениях с влажностью до 100%, сильной запыленностью, а также на открытых площадках в сложных погодных условиях;
- исполнение видеокамеры с питанием по технологии PoE отвечает современным требованиям системы видеонаблюдения;
- для автоматического включения/выключение ИК-подсветки в конструкции видеокамеры предусмотрено сумеречное реле;
- небольшие габаритные размеры облегчают установку видеокамеры в ограниченных пространствах [11] (таблицы 2.1, 2.2, 2.3).

Таблица 2.1 – Описание камеры 3

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
Relion-Trassir -H-50-IP-4MP-PoE	4	2688x1520	3,6	¼ 16:9	274x227 пикс/м

Таблица 2.2 – Описание камеры 4

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
Relion-Trassir -H-50-IP-4MP-PoE	4	2688x1520	3,6	¼ 16:9	243x201 пикс/м

Таблица 2.3 – Описание камеры 1

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
Relion-Trassir -H-50-IP-4MP-PoE	4	2688x1520	3,6	¼ 16:9	211x175 пикс/м

Камеры Relion-Trassir -H-50-IP-4MP являются аналоговыми. Для подключения аналоговых камер наиболее часто используется коаксиальный кабель для видеонаблюдения, вроде того, по которому внешняя антенна подключается к телевизору или приемнику. Этот тип кабеля представляет собой медную жилу, заключенную в толстый слой пенистого диэлектрика, который покрыт снаружи экранирующей защитной оболочкой, благодаря которой обеспечивается хорошая защита от помех и возможных потерь сигнала. Наиболее часто для видеонаблюдения используются отечественные марки РК-75-2-13,РК-75-4-12 (РК – радиочастотный кабель), или импортные аналоги – RG-59, RG-6, RG-11. При выборе коаксиального кабеля необходимо учитывать такие немаловажные параметры, как длина и место прокладки (внутри помещения или на улице), и в зависимости от этого приобретать подходящую марку провода. При значительном удалении камер от видеорегистратора и друг от друга (длина линии более 200-300 метров), передаваемый сигнал может значительно ослабнуть: здесь действует простая аксиома – чем кабель длиннее и тоньше, тем больше потерь сигнала. Так что при выборе очень важно учитывать расстояние прокладки, и, исходя из него, уже выбирать подходящий кабель для систем видеонаблюдения. Краткие характеристики камеры показаны на рисунке 2.5.

Рисунок 2.5 –Характеристики камер, установленных в кабинах касс

На рисунке 2.6 представлен вид кабеля, который был выбран для соединения камер внутри кабин. На таблице 2.4 зависимость типов кабелей.

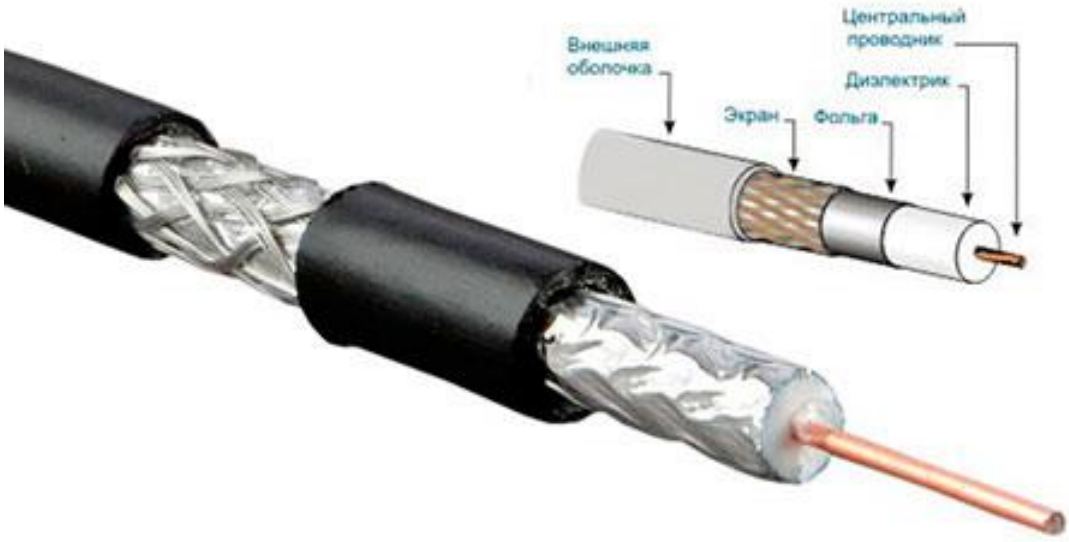

Рисунок 2.6 – Коаксиальный кабель

Таблица 2.4 – Зависимость типа провода от расстояния

Марка кабеля	Рекомендуемое расстояние до видеокамеры, не более, м
РК-75-1,5-11	50
РК-75-2-11	300
РК-75-2-11а	200
РК-75-2-13	350
РК-75-3-32	450
РК-75-3,7-322а	600
РК-75-4-11	600
РК-75-4-11а	600
РК-75-4-12	600
РК-75-4-15	600
РК-75-4-16	600
РК-75-4,9-322а	750
РК-75-9-12	Магистральный
РК-75-9-13	Магистральный
RG-59	600
RG-6U	650
RG-6WE	
RG-11	Магистральный

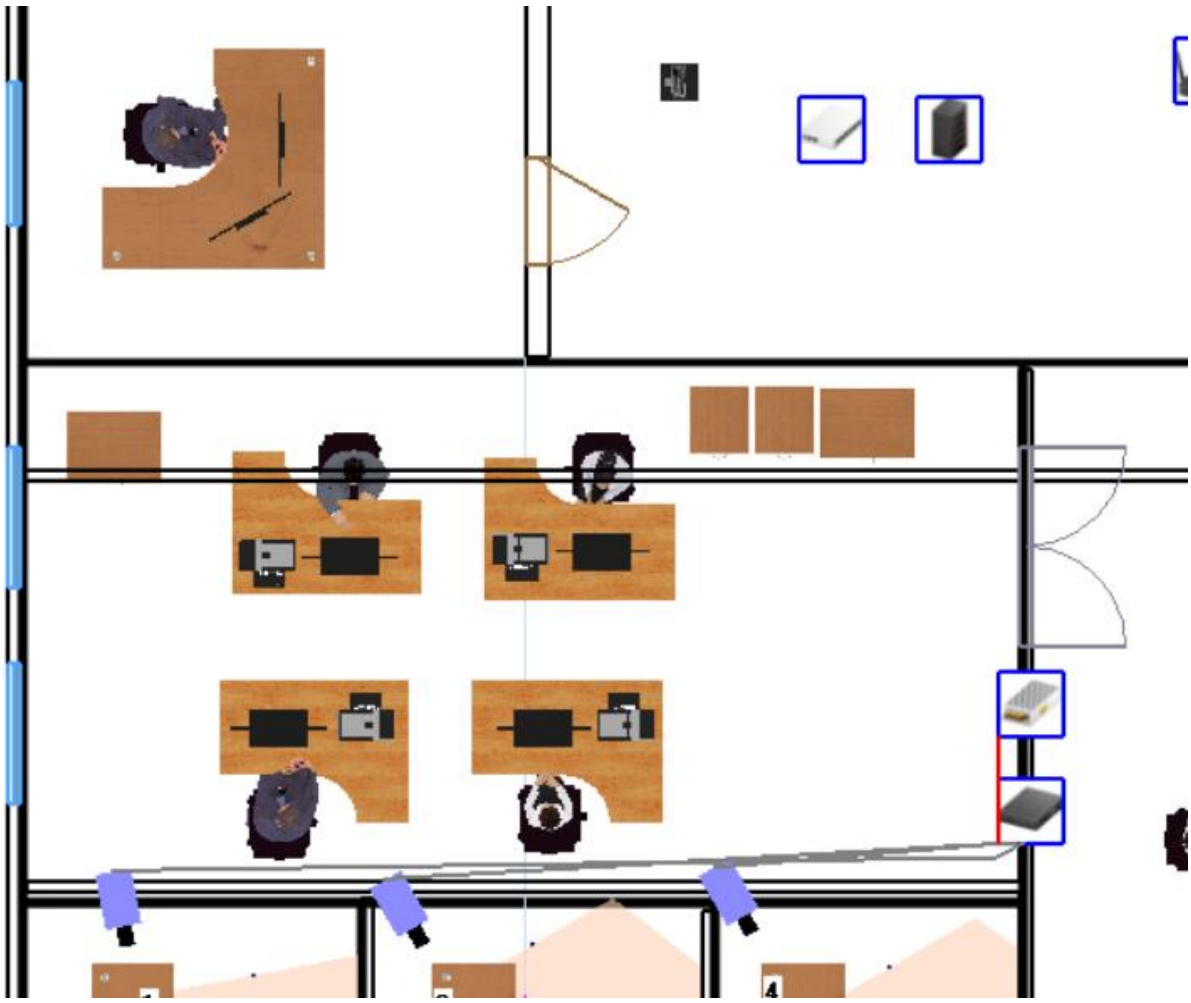

Рисунок 2.7– Прокладка кабеля

Камеры 1,4,3 соединены коаксиальным кабелем с видеорегистратором, который подключен к источнику питания. Видеорегистратор в свою очередь соединен с монитором компьютера находящегося в комнате видеонаблюдения. Используется кабель марки РК-75-1,5-11(общая длина кабеля для 3-х камер: 22,09 м.). Диагональ монитора компьютера, к которому подключён видеорегистратор 22’’.

Операционный зал. Причина установки камеры: Данная зона характеризуется свободным доступом и обширной территорией контроля. Помимо самых бытовых ситуаций проявления недовольства и агрессии со стороны посетителей банка, здесь возможны угрозы террористической характера. Именно в эту зону возможно свободное проникновение злоумышленников. Помимо задач безопасности, операционный зал является объектом пристального внимания службы по работе с персоналом и службы маркетинга. Установлены камеры модели HD камера HiWatch DS-T507C (кол-во: 2) - 5Мп внутренняя купольная HD-TVI аналоговая камера с ИК-подсветкой до 30м. Установка камер представлена на рисунке 2.8. Камера модели HiWatch DS-T507C представлена на рисунке 2.9. Описание камеры на таблицах 2.5, 2.6.

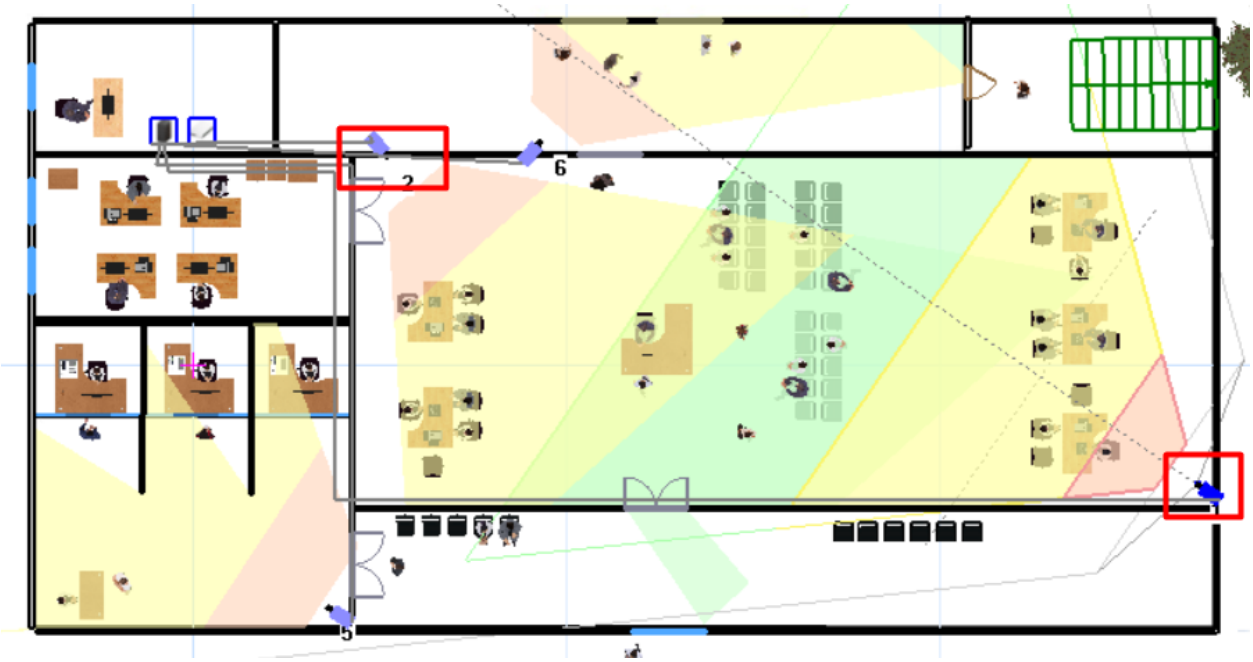

Рисунок 2.8 – Установка камер в операционном зале

Рисунок 2.9 – HiWatch DS-T507C

Таблица 2.5 – Описание камеры 2

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
HiWatch DS-T507C	4	2560x1944	3	1/2,7 4:3	90 пикс/м

Таблица 2.6 – Описание камеры 3

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
HiWatch DS-T507C	4	2560x1944	2,7	1/2,7 4:3	81 пикс/м

Краткая характеристика представлена на рисунках 2.10, 2.11, 2.12, а также в таблице 2.7, 2.8.

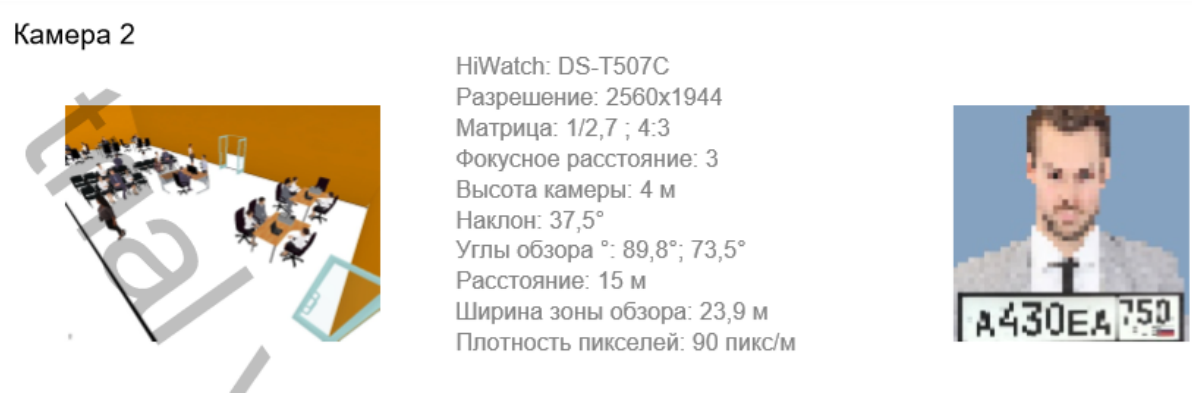

Рисунок 2.10 – Характеристики камеры 2

Рисунок 2.11 – Характеристики камеры 1

Операционная зона. Причина установки камер: основные угрозы – это действия преступного характера и вооруженные ограбления. Описание камеры таблица 2.7, 2.8.

Рисунок 2.12 – Характеристики камеры 5

Таблица 2.7 – Описание камеры 5

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
HiWatch DS-T507C	4	2560x1944	2,7	1/2,7 4:3	88 пикс/м

Таблица 2.8 – Описание камеры 6

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
HiWatch DS-T507C	4	2560x1944	2,7	1/2,7 4:3	83 пикс/м

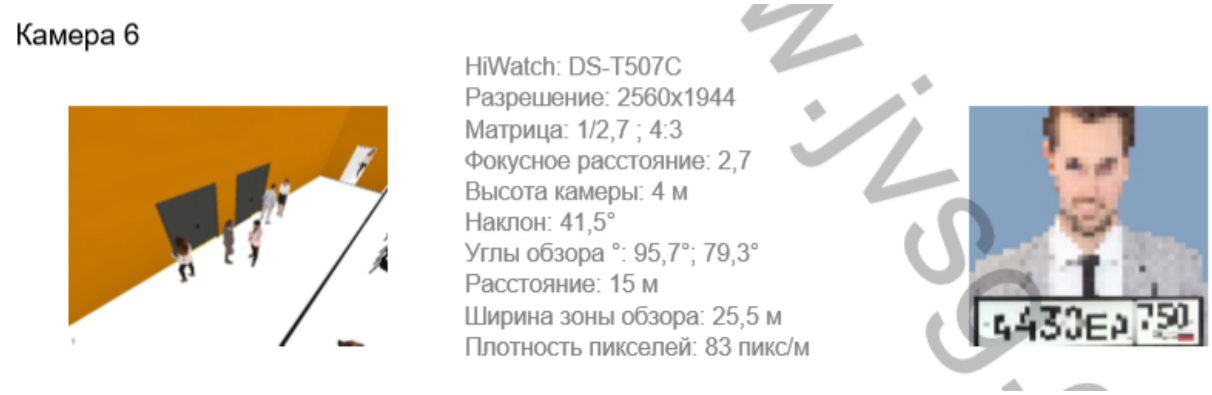

Рисунок 2.13 – Характеристики камеры 6

Камеры 1,2,5,6 соединены коаксиальным кабелем с видеорегистратором, который подключен к источнику питания. Видеорегистратор соединен с монитором компьютера находящегося в комнате видеонаблюдения. Используется кабель марки РК-75-1,5-11. Диагональ монитора компьютера, к которому подключен видеорегистратор 22’’.

Внутренний двор (Парковочная зона). Причина установки камер: здесь располагается автостоянка корпоративного транспорта, входы в подсобные помещения хозяйственного назначения, объекты инфраструктуры и жизнеобеспечения. Зачастую именно здесь располагается дизельная установка аварийного электроснабжения, въезд в зону инкассации. В этой зоне возможны диверсии и отсюда может быть попытка проникновения со стороны злоумышленников.

У входа в «микрофинансовую организацию» и на парковке установлены камеры модели Mobotix VD-4-IR. Сетевая камера VD-4-IR - всепогодная купольная камера ONVIF S / G со встроенными ИК-светодиодами (до 30 м) для работы в дневное и ночное время. Рисунок 1.17 и краткая характеристика камеры на рисунке 2.15,также характеристика камеры на рисунке 2.16. Также описание камер на таблицах 2.9; 2.10.

Перейдем к выбору видеокамер для охраны периметра. При модернизации системы видеонаблюдения периметра нужно устранить существующие проблемы:

- ненадлежащая защита камер от условий внешней среды;
- повышение информативности изображения камер, наблюдающих за въездом на территорию организации.

Для защиты камеры от мороза, осадков и прочих неблагоприятных условий. Возможно использование кожухов для стандартных безкорпусных камер или использование готовых уличных камер уже укомплектованных термокожухом.

Для этого была выбрана цветная камера Mobotix VD-4-IR. Видеокамера для уличной установки Mobotix VD-4-IR, уличная камера видеонаблюдения, с автоподогревом; CCD Sharp 1/3"; 420 ТВЛ; 0,1 люкс; диапазон рабочих температур -45...+45°C, DC12V/0,27A. Угол обзора, град.: 21, 56, 78, 90, 110 на выбор. Описание камер на таблицах 2.9, 2.10.

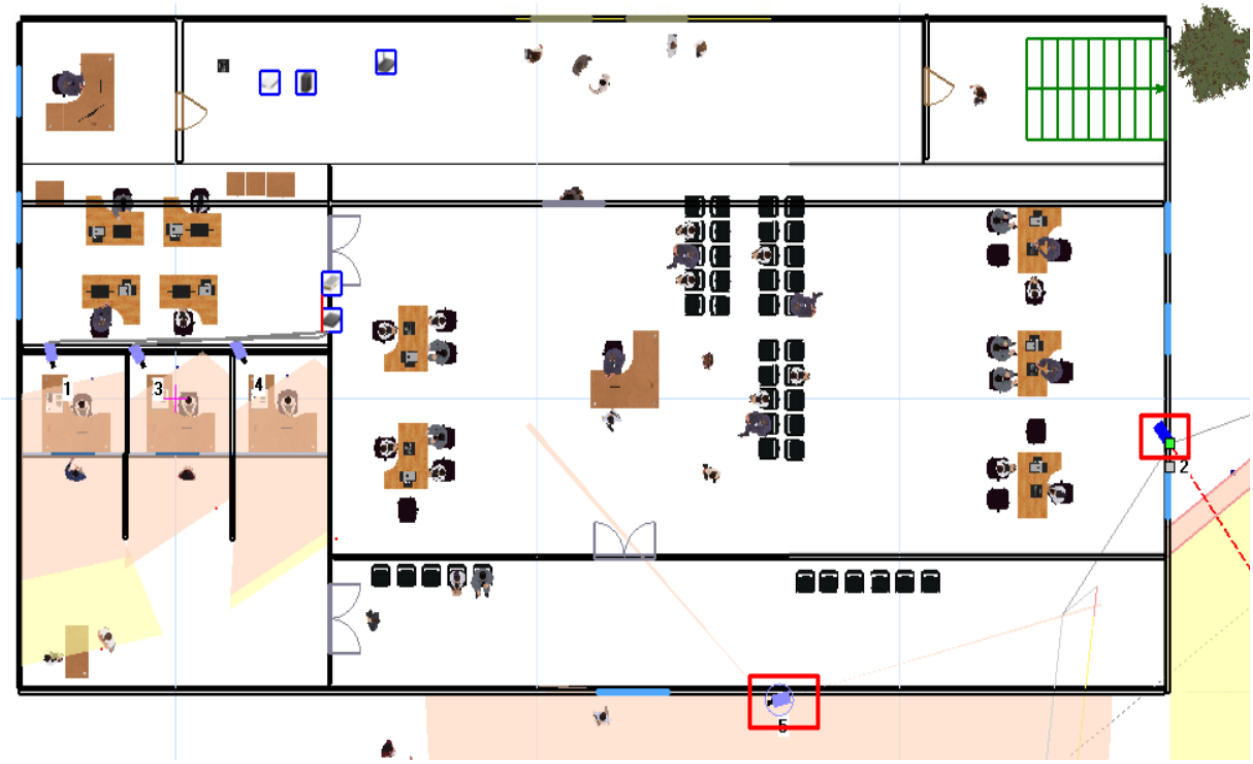

Рисунок 2.14 – Установка внешних камер, по периметру

Таблица 2.9 – Описание камеры 2

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
MOBOTIX VD-4-IR	4	2688x1512	3	1/3 16:9	110 пикс/м

Таблица 2.10 – Описание камеры 5

Модель	Высота камеры, м	Разрешение	Фокусное расстояние	Матрица	Плотность пикселей
MOBOTIX VD-4-IR	4	2688x1512	3	1/3 16:9	76 пикс/м

Характеристики камер продемонстрированы на рисунках 2.15, 2.16.

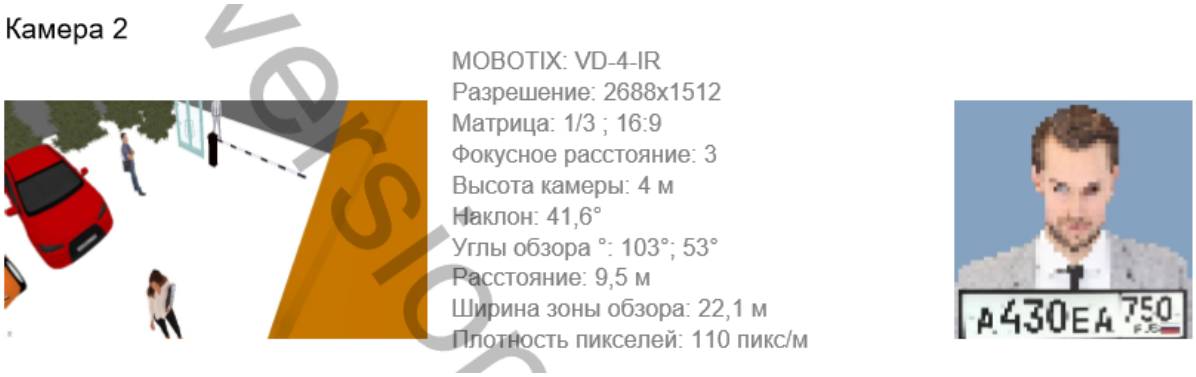

Рисунок 2.15 – Характеристики камеры 2

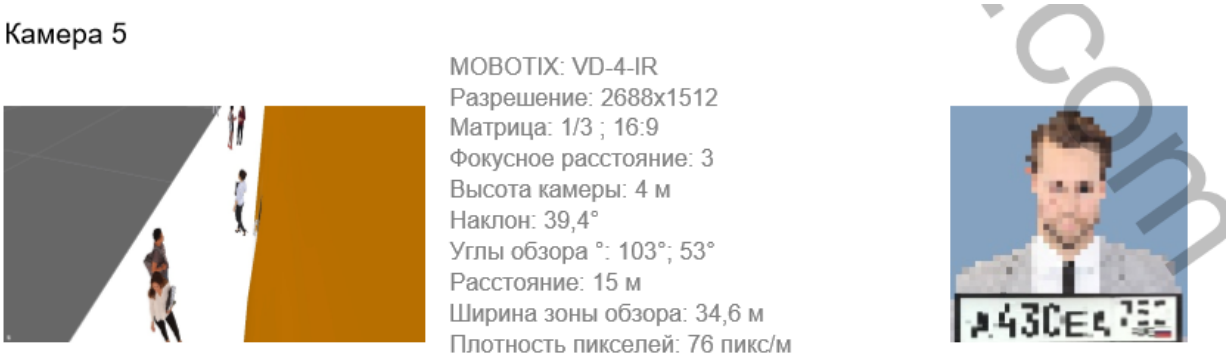

Рисунок 2.16 – Характеристики камеры 5

При использовании IP-камер запись настраивается на SD-карту или сервер. Но на карту много не запишешь. Ею могу завладеть злоумышленники и информация, которая принадлежит вам, будет безвозвратно утеряна. Запись на сервер имеет свои минусы: сбои, ошибки, сторонние процессы, перегружающие систему и т.д.

Чтобы избежать этих проблем и решить задачу управления, настройки и записи IP-камер, придумали устройство NVR.

NVR - цифровой видеорегистратор, предназначенный для работы с IP-камерами по витой паре (компьютерным кабелем).

Вот преимущества NVR:

- подключение жестких дисков больших объемов;
- подключение от одного до четырех жестких дисков, с объемом каждого до 6 ТБ;
- регистратор не загружен лишними процессам, работает быстро и без сбоев;
- через NVR вы управляете IP-камерами и используете тонкие настройки: детектор движения, детекция лиц, тревожные выходы и т.д.;
- чтобы не искать возможность подключения камеры к питанию, в некоторых моделях регистраторов есть PoE-выходы и камеры подключаются без блока питания. Тогда подачу питания подает регистратор по витой паре;
- пропускная способность (количество данных, которые единовременно потребляет или отдает регистратор) от 25 до 400 Мб/с. Камеры,

подключаемые к NVR, часто лучше, чем подключаемые к DVR. Вплоть до разрешения 4К (Ultra HD). Итоговый результат установки внешних камер на рисунке 2.17. Схема подключений камер продемонстрирована на рисунке 2.18.

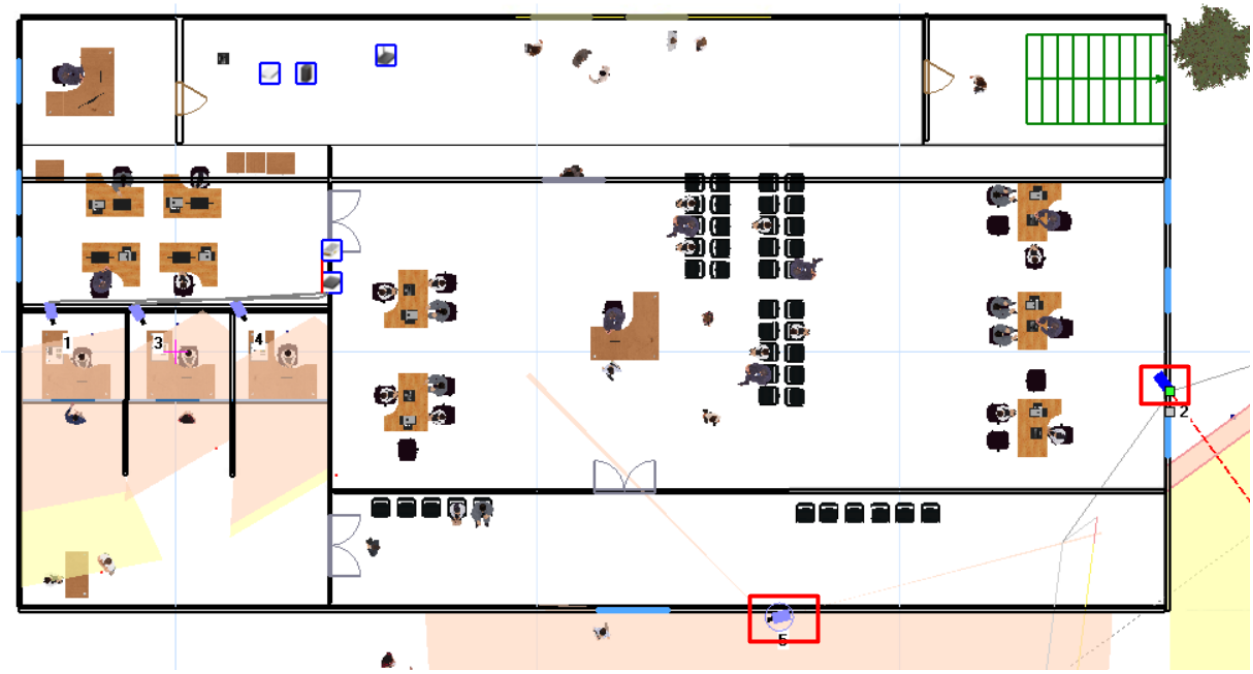

Рисунок 2.17 – Установка внешних камер

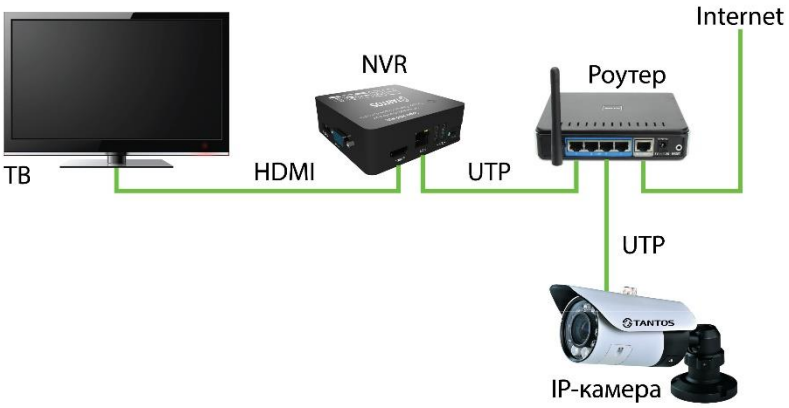

Рисунок 2.18 – Схема подключения камеры

Для начала необходимо произвести замену монитора видеооператора. Для более комфортного видеонаблюдения в системе видеонаблюдения следует заменить старый монитор. Выбирая тип монитора следует отдать предпочтение ЖК-монитору.

Затем производится замена соединительного кабеля. Состояние кабеля соединяющего элементы системы видеонаблюдения можно оценить, как неудовлетворительное. Поэтому высок риск искажений и потерь в качестве

изображения. Принято решение использовать для передачи стандартный коаксиальный кабель с волновым сопротивлением.

В зависимости от качества кабеля (вносимого им затухания), как правило, приемлемое качество изображения может быть достигнуто, если видеокамера удалена от поста наблюдения на расстояние не более 200…400 м. При больших расстояниях для компенсации потерь в кабеле рекомендуется использовать магистральные видеоусилители. Будучи вспомогательными приборами, они могут быть размещены в отдалении от оператора, причем, для повышения отношения сигнал/шум магистральные видеоусилители желательно располагать как можно ближе к видеокамере.

Кроме размещения видеокамер будет выполнен перенос видеосервера в специальное помещение на втором этаже, там же будет заменен монитор. Кроме того, будет установлен монитор видеонаблюдения в проходной компании. Для получения записей с камеры настраивается проброс портов. Если интернет-подключение имеет статический (белый) IP адрес, то доступ осуществляется введением этого адреса непосредственно в адресную строку браузера. В противном случае придется использовать динамические сервисы (DynDNS). Прокладка кабеля на рисунке 2.19.

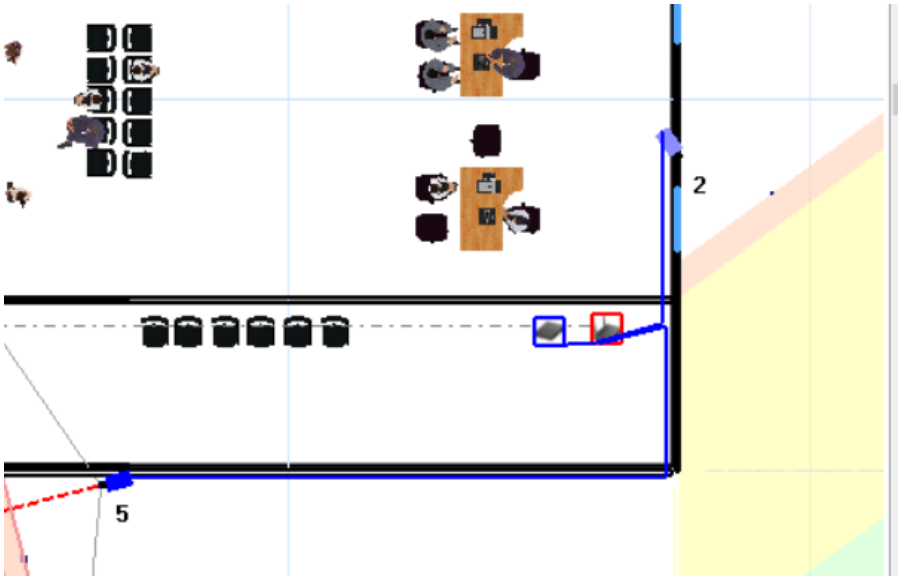

Рисунок 2.19 – Прокладка кабеля

Внешние камеры соединены витой парой. Обычно мы прибегаем к использованию витой пары в тех случаях, когда дальность предполагаемой линии от камеры до устройства приема сигнала составляет от 300 до 1000 м (расстояние возможной прокладки рабочей линии видеонаблюдения при помощи витой пары может составлять до 3 км.).

UTP кабель самый простой, он не имеет защитных экранирующих оболочек, и представляет собой 8 изолированных, попарно скрученных проводников, помещенных в общую защитную оболочку. К недостаткам UTP кабелей можно отнести их низкую устойчивость к помехам, поэтому в

случаях прокладки коммуникаций для видеонаблюдения рядом с электропроводкой, и другими источниками помех, лучше использовать кабели с дополнительной защитой.

Для подключения цифровых IP камер используется UTP кабель с обжатыми коннекторами RJ-45 на обоих концах. Его преимущество заключается в возможности прокладки одной общей линии витой пары для целой системы IP камер видеонаблюдения, с использованием коммутатора (свитч). Питание камер при этом можно реализовать тремя способами:

- прокладка отдельного кабеля питания к каждой камере;
- монтаж блоков питания в местах установки каждой камеры;
- электропитание камер при помощи свободных проводов в витой паре.

Третий вариант подходит только для тех случаев, когда камера и коммутатор поддерживают технологию PoE (Power of Ethernet), позволяющую осуществлять питание посредством Ethernet кабеля для IP видеонаблюдения, в других случаях необходимо применение инжекторов Passive, которые позволяют объединить передачу сигнала и питания с обеих сторон одного кабеля. Общий трафик и объем диска, а также список и общая длина кабелей показана на рисунках 2.20; 2.21; 2.22; 2.23; 2.24; 2.25. Таблица 2.11, 2.12, 2.13.

Разрешение	Видеосжатие	Сложность ...	% Движ...	Размер кадр...	FPS (кадров в секунду)	Суток	Камер	% Записи	Трафик,Мб/с	Объем,Гб	Битре...	Примечания
2600x1950 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	619	10	30	1	62	50,71	10186,3	50708	
2600x1950 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	619	10	30	1	62	50,71	10186,3	50708	
2600x1950 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	619	10	30	1	25	50,71	4107,4	50708	
2600x1950 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	619	10	30	1	31	50,71	5093,2	50708	
2600x1950 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	619	10	30	1	100	50,71	16429,5	50708	

Рисунок 2.20 – Трафик и объем диска

Разрешение	Видеосжатие	Сложность ...	% Движ...	Размер кадр...	FPS...	Сут...	Камер	% Записи	Трафик,Мб/с	Объем,Гб	Битре...	Примечания
2560x1920 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	600	10	30	1	62	49,15	9873,7	49152	
2560x1920 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	600	10	30	1	62	49,15	9873,7	49152	
2560x1920 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	600	10	30	1	62	49,15	9873,7	49152	
2560x1920 (5 MP)	MJPG-20 (Хорош	50 - Средняя	50 - Средн	600	10	30	1	62	49,15	9873,7	49152	

Рисунок 2.21 – Трафик и объем диска

Таблица 2.11 – Список кабелей

ID кабеля	Тип	От	До	Длина, м
2	Кабель питания	1	PoE инжектор 2	1,8
1	Кабель питания	4	PoE инжектор 1	0,92
3	Кабель питания	6	PoE инжектор 3	1,02
6	Витая пара	5	Беспроводная точка доступа 1	1,32
7	Витая пара	Беспроводная точка доступа 1	PoE инжектор 1	6
8	Витая пара	Беспроводная точка доступа 1	PoE инжектор 2	3,7

9	Витая пара	PoE инжектор 3	Беспроводная точка доступа 1	20,41
10	Кабель питания	Источник питания 1	Беспроводная точка доступа 1	0,92
11	Витая пара	Беспроводная точка доступа 1	Видеорегистратор 1	0,78

Таблица 2.12 – Общая длина кабелей

Тип кабеля	Длина, м
Витая пара	32,21
Кабель питания	4,67

Таблица 2.13 – Трафик и объем диска

Разрешение	Видеосжатие	Сложность кадра	% Движения	Размер кадра, Кб	FPS	Суток	Камер	% Записи	Трафик, Мб/с	Объем, Гб	Битрейт, Кбит/с
2600x1950 (5MP)	MJPG-20 (Хорошее качество)	50 – средняя	50 – средняе	619	10	30	1	100	50,71	16429,5	50708
2600x1950 (5MP)	MJPG-20 (Хорошее качество)	50 – средняя	50 – средне е	619	10	30	1	100	50,71	16429,5	50708
2600x1950 (5MP)	MJPG-20 (Хорошее качество)	50 – средняя	50 – средне е	619	10	30	1	100	50,71	16429,5	50708
2600x1950 (5MP)	MJPG-20 (Хорошее качество)	50 – средняя	50 – средне е	619	10	30	1	100	50,71	16429,5	50708

Таблица 2.14 – Общая сумма

Сум. FPS	Трафик, Мбит/с	Сум.объем, Гб
40	202,84	65718

Необходимо также учитывать правовые аспекты установки камер видеонаблюдения. Согласно п. 2 ст. 3 Закона «О персональных данных» под персональными данными понимается любая информация, позволяющая, прямо или косвенно идентифицировать конкретное лицо. Статья 85 Трудового кодекса РК под обработкой персональных данных понимает их получение, хранение, комбинирование или передачу, или любое иное использование персональных данных работника.

Соответственно, в том случае, если система видеонаблюдения позволяет отслеживать деятельность сотрудников на рабочем месте или иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.

Таким образом, при осуществлении видеонаблюдения за объектами, имеющими режим ограниченного доступа, работодателю необходимо руководствоваться не только соображениями обеспечения законности получения доказательств, но и дополнительно соблюдать ограничения, связанные с регулированием процесса обработки персональных данных. В данном случае, предполагая, что круг лиц, имеющих доступ в помещение, где осуществляется видеонаблюдение, ограничен, то есть заранее определен, справедливо будет сделать вывод, что видеонаблюдение имеет своей целью только строго установленный круг лиц. Следовательно, осуществление такого видеонаблюдения изначально будет рассматриваться как получение и обработка персональных данных.

В отсутствие иных нарушений запись, полученную с соблюдением законодательства о персональных данных, можно использовать в качестве доказательства. Исключение, пожалуй, составляют лишь случаи несанкционированного проникновения в помещения, имеющие режим ограниченного доступа.

Основываясь на системном толковании норм закона «О персональных данных», можно установить, что для обработки персональных данных работника, работодателю необходимо:

- заключить с работниками соглашение о сборе и обработке персональных данных (или включить соответствующие положения в трудовой договор) с указанием целей обработки, предполагаемыми источниками получения персональных данных, способами ее получения, последствиями отказа работников от дачи согласия на ее получение;
- принять локальный нормативный акт, устанавливающий порядок обработки персональных данных работников и связанные с этим права работников;
- осуществлять надлежащую охрану полученных данных;
- указать работников, ответственных за обработку персональных данных в данном локальном нормативном акте.

Следовательно, если на предприятии впервые вводится система видеонаблюдения, потребуется внесение соответствующих изменений в

положение о персональных данных. Указанное справедливо и в случае осуществления видеонаблюдения силами частной охранной организации.

Отдельно следует рассмотреть вопрос организации скрытого видеонаблюдения. Данный вид наблюдения представляет собой форму получения информации с помощью устройств, предназначенных для ее негласного получения. Осуществление такого наблюдения в принципе запрещено физическим и юридическим лицам в соответствии с ч. 6 ст. 6 закона «Об оперативной и розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ.

Кроме того, ст. 138.1 Уголовного кодекса РК воспрещает приобретение и использование устройств, предназначенных для негласного получения информации под страхом лишения свободы сроком до 4 лет.

Таким образом, даже неофициальное использование скрытого видеонаблюдения несет в себе риск применения достаточно жестких санкций.

Установка видеокамер на рабочем месте должна иметь законное основание и обоснованную цель. Видеосъемка должна проводиться открыто, а работники должны быть надлежащим образом уведомлены о том, что ведется видеонаблюдение. Первое, на что стоит обратить внимание — это то, что рабочее место не находится в стороне от личной жизни определенного лица (решение Конституционного суда РК № 2-рп/2012, согласно которому личной жизнью физического лица является его поведение в сфере личностных, семейных, бытовых, интимных, товарищеских, профессиональных, деловых и иных отношений вне общественной деятельности, осуществляемой, в частности, при выполнении лицом функций государства или органов местного самоуправления).

Таким образом поведение лица в профессиональных и деловых отношениях можно рассматривать как его личную жизнь. Из упомянутого решения Конституционного суда следует, что информация о личной жизни человека — это любые сведения или совокупность сведений о физическом лице, которое идентифицировано или может быть конкретно идентифицировано.

Закон. РК «О защите персональных данных», регулирует отношения, связанные с защитой и обработкой персональных данных и направлен на защиту права человека на личную жизнь. Видеосъемку можно рассматривать как способ обработки определенных персональных данных работника на которую распространяются нормы указанного Закона.

Факт видеосъемки работника на рабочем месте уже есть обработкой персональных данных такого работника, то есть сведений или совокупности сведений о работнике, который идентифицирован или может быть конкретно идентифицирован. Такие персональные данные работника априори являются конфиденциальной информацией, поскольку это информация о физическом лице, и их обработка без согласия соответствующего лица не допускается, кроме случаев, четко определенных законом.

Согласно ст. 2 Закон. РК «О защите персональных данных» согласие субъекта персональных данных — это добровольное волеизъявление физического лица о предоставлении разрешения на обработку его персональных данных в соответствии с сформулированной целью их обработки, высказанное в письменной форме или в форме, что позволяет сделать вывод о предоставлении согласия.

Виды согласия:

- ясно выраженное согласие. Письменный формат является наилучшим вариантом получения согласия. У вас всегда будет железное доказательство;
- устное согласие. Однако доказать наличие такого вида весьма проблематично при возникновении проблем, как вариант — можно на камеру проговорить сотруднику о видеонаблюдении, что будет являться подтверждением, предупреждения со стороны работодателя, но суды не всегда берут во внимание;
- молчаливое согласие. Это когда человек знает и видит, что за ним ведется видеонаблюдение, но не высказывает своих возражений относительно его проведения. Молчаливое согласие — это и обычный кивок перед камерой после предупреждения о видеонаблюдении на рабочем месте либо на видном месте размещены таблички о видеонаблюдении.

Одной из систем решения задачи обеспечения информационной безопасности была выбрана система SpiceWorks, SpiceWorks — это уникальная система и решение для ИТ инфраструктурой малого и среднего бизнеса, а также управления доступом к информационным ресурсам организации, соблюдения политики безопасности.

Ряд ее преимуществ:

- она совершенно бесплатна;
- имеет русский интерфейс.

При этом бесплатность достигается абсолютно законным путём. Также один небольшой интересный факт – в систему внедрено сообщество ИТ-специалистов, которое позволяет администратору решать многие проблемы с помощью краудсорсинга. В сообществе есть форум, где можно спросить совета, закрытые группы для общения или совместной работы, вики с полезными статьями и рейтинги железа и программного обеспечения с отзывами коллег. И конечно же, такое сообщество стало прекрасной причиной для создания Marketplace, где ИТ-специалисти могут продвигать свои продукты (размещать горячие предложения, новости, статьи) и общаться со своей целевой аудиторией - ИТ-специалистами

Spiceworks обладает функциями мониторинга различных систем и оборудования, инвентаризации, бэкапа конфигураций сетевого оборудования, у неё есть встроенная система HelpDesk для сотрудников организации и еще целый спектр других возможностей. Новая версия Spiceworks 5.1, обзавелась модулем мониторинга источников бесперебойного питания.

Данная програма, Spiceworks, адаптирована в два режима, первый это режим службы, а второй это режим приложения, можно по желанию

провести селекцию по завершению установки. Система запускает собственный HTTP-сервер и всё управление осуществляется непосредственно через WEB-интерфейс. На время установки нужно выпустить ПК с системой в интернет для регистрации аккаунта, под которым вы будете работать и проводить мониторинг системы в Spiceworks. Этот же аккаунт будет работать на форуме поддержки и в сообществе этой системы.

После установки перед нами появляется следующее окно, рисунок 2.22.

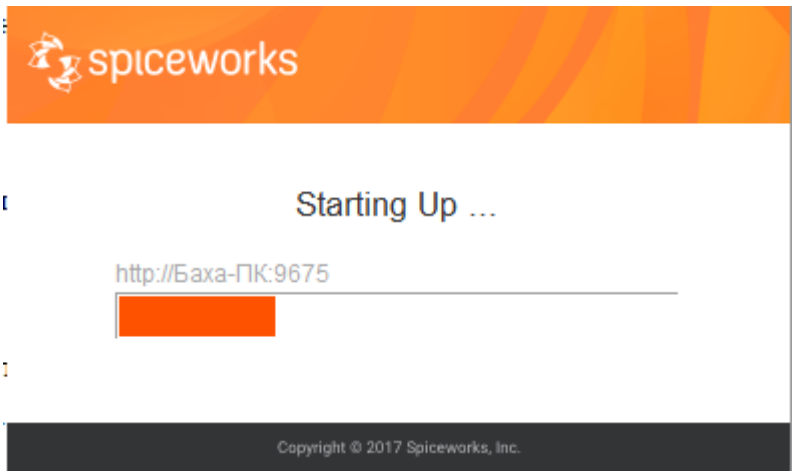

Рисунок 2.22 – Сбор данных о рабочих станциях

В панельном меню производятся все необходимые нам настройки.

По умолчанию здесь отображается сводная диаграмма событий, которые регистрируются в журналах событий Windows просканированных машин. Количество предупреждений и ошибок. Снизу представлена вкладка «устройства», рисунок 2.23.

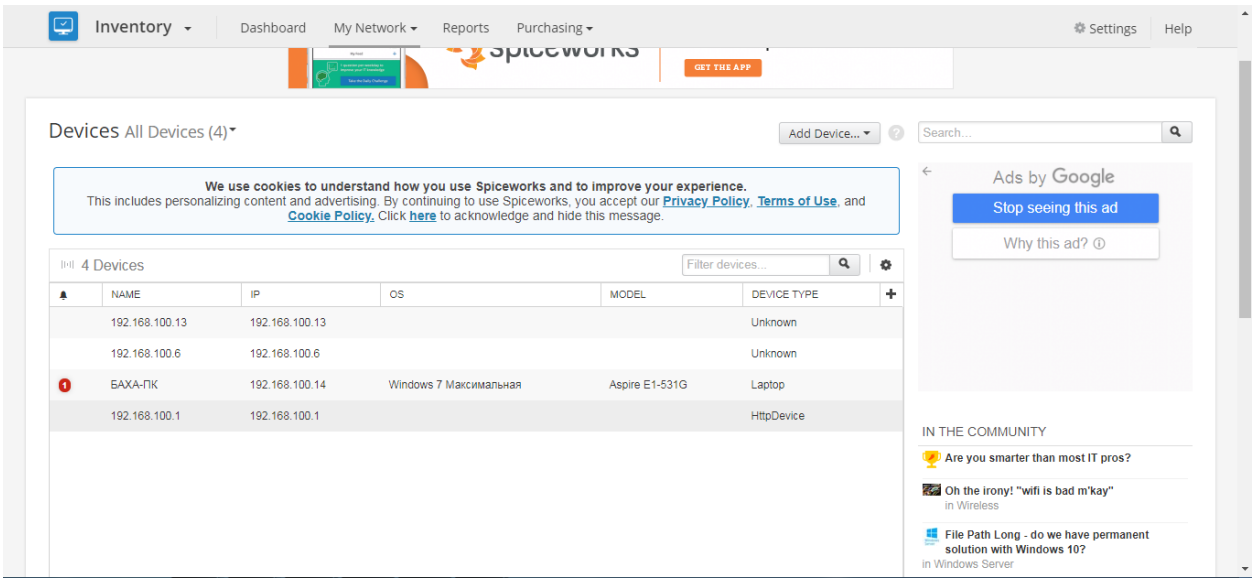

Рисунок 2.23 – Вкладка «устройства»

По умолчанию здесь дополнительная информация об антивирусной защите на просканированных компьютерах. Под диаграммой расположена

легенда и информация о том, каких антивирусы, в каком количестве и на каких компах установлены.

Хронология событий. В процессе сканирования все изменения, которые фиксирует Spiceworks отображаются. Аппаратные средства, разбитые по группам. Диаграмма производителей аппаратных средств. Тревоги. Здесь Spiceworks показывает всё, на что следует обратить внимание. Например, картридж в принтере заканчивается или свободное место на каком-нибудь ПК. Также можно просмотреть характеристики каждой рабочий станции, находящейся в сети. Кликнув по диаграмме журнала событий, мы сможем увидеть на каких компьютерах какие ошибки возникают.

Кликая по компьютеру, мы можем увидеть всю информацию о нем: модель, серийный номер, характеристики железа, ОС, список установленных программ, кто сейчас работает за этим ПК, какой IP адрес назначен, в какой коммутатор и в какой порт воткнут, рисунок 2.24.

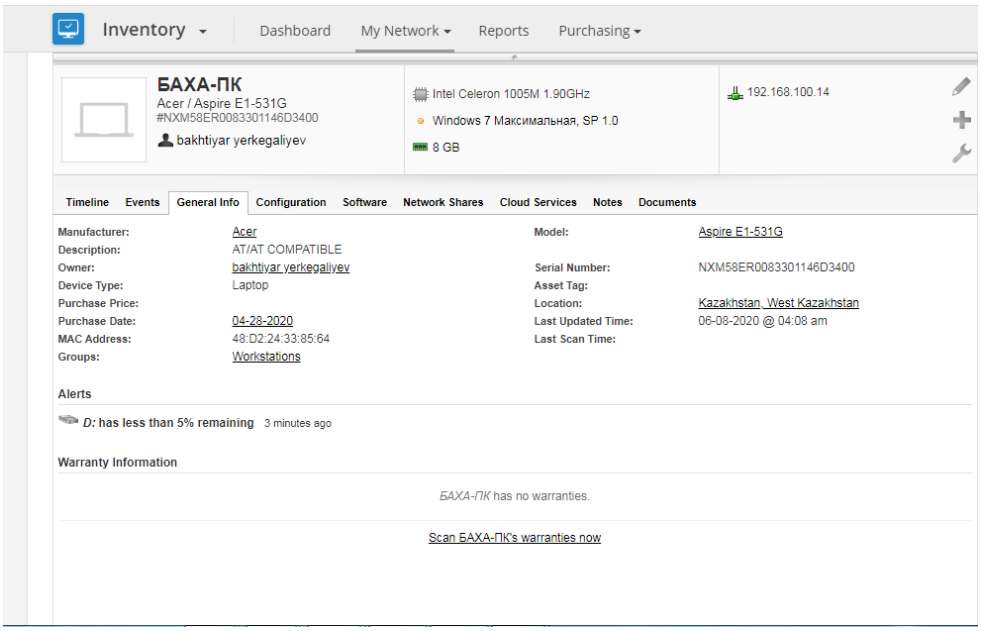

Рисунок 2.24– Полная информация и характеристика о рабочей станции

Помимо вышеперечисленных функций, SpiceWorks может отслеживать за состоянием памяти на рабочих станциях, рисунок 2.25.

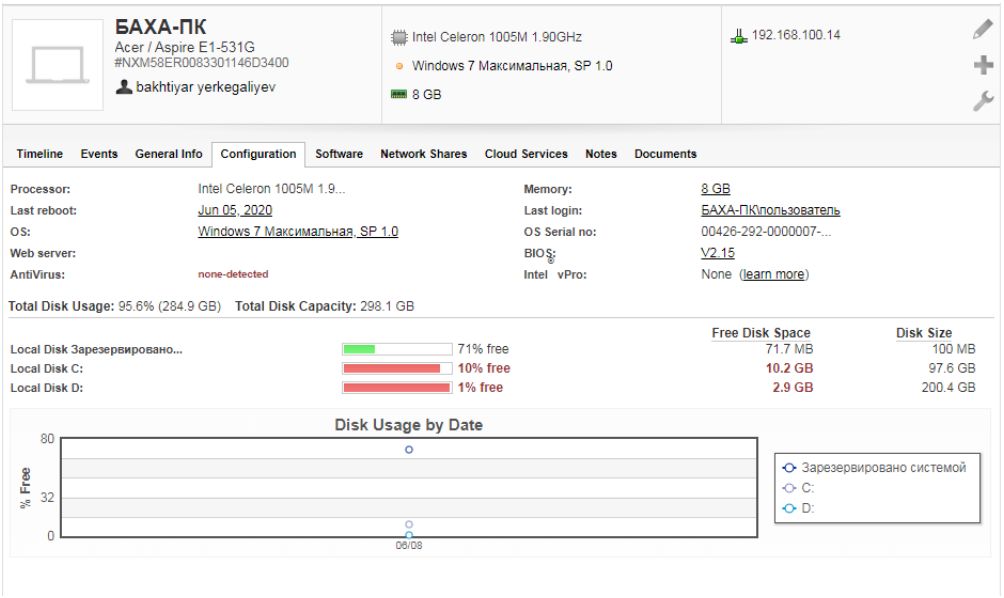

Рисунок 2.25 – Состояние памяти на дисках

Также информация о беспроводном соединении, с полной информацией об IP адресе, маске, mac-адресе, dhsp/dns серверах , рисунок 2.26. Ну и об отдельных рабочих станциях, в данном случае это виртуальные машины, представленные на рисунках 2.26, 2.27.

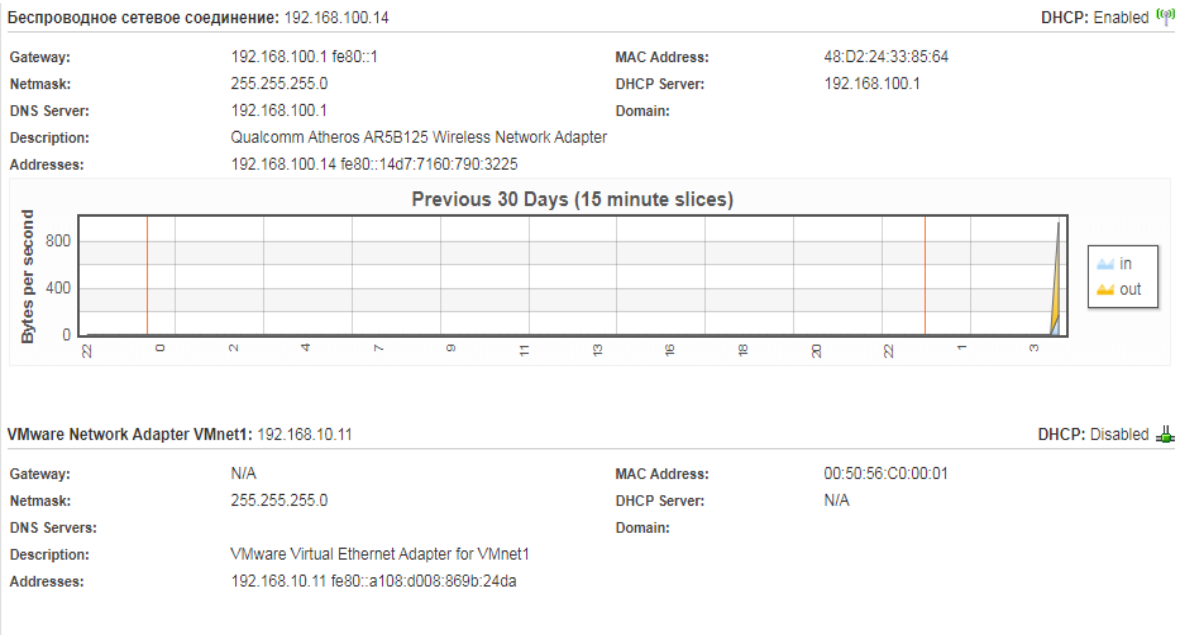

Рисунок 2.26 – Информация о соединении

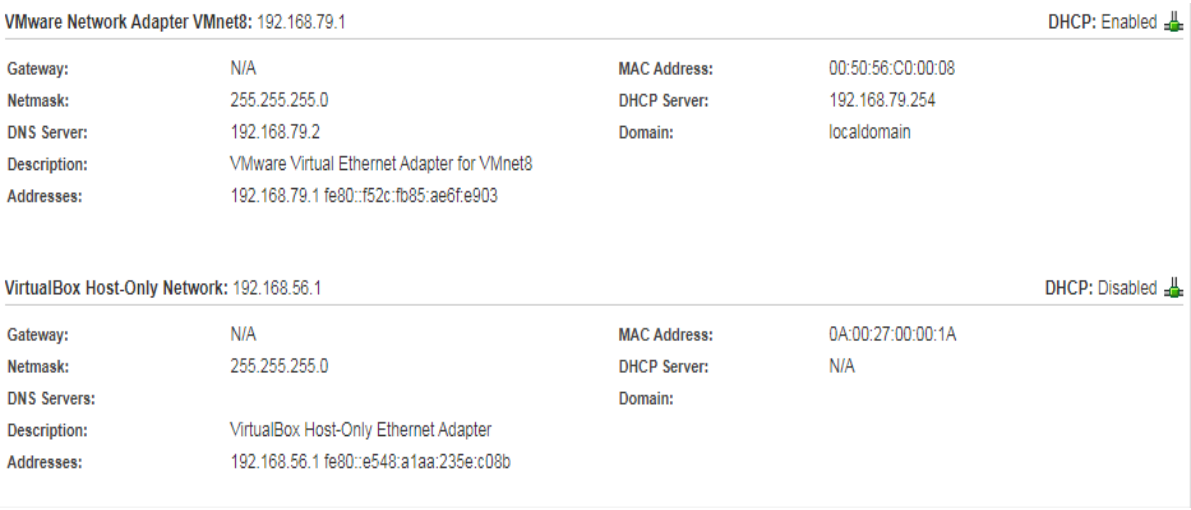

Рисунок 2.27 – Информация о рабочих станциях

Имеется удобная функция просмотра всех установленных приложений, утилит, а также информация об установленном программном обеспечении, полная информация включает в себя: последнюю активность в программе, какой пользователь именно был в последней сессии, ну и ее лицензия, в случае если программа была установлена без ключа авторизации, то можно его добавить, рисунок 2.28.

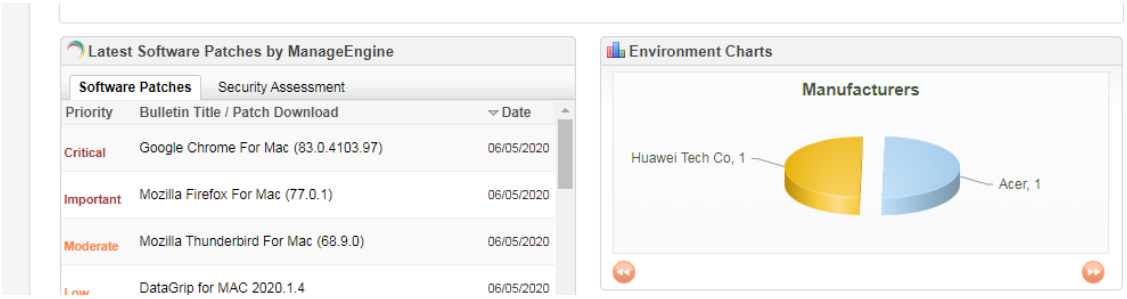

Рисунок 2.28 – Информация о производителе

Отчет о состоянии сети:

- просмотр ПО на машинах в сети, использование ими дискового пространства, устранение неисправностей и многое другое;
- создание пользовательских отчетов посредством простого интерфейса;
- публикация статей для сотрудников компании;
- экспорт отчетов в PDF и Excel;
- обмен полезными шаблонами отчетов с другими пользователями.

Исправление неисправностей сети:

- контроль ПО, замедляющего работу ПК;
- запуск средств удаленного управления из Spiceworks;
- сравнение параметров двух машин для проверки и понимания различающихся параметров;
- проверка присутствия машин в сети утилитой пингования (ping);

- запуск traceroute для проверки потока данных;
- тестирование наличия свободного места на диске сервера.

10-Страйк: Инвентаризация Компьютеров Pro	8.9	11-18-2019	All users	Enter License
10-Страйк: Схема Сети	3.5	10-11-2019	All users	Enter License
@RISK	7.6.01018.0	11-03-2019	All users	Enter License
Adobe Acrobat Reader DC - Russian	20.009.20065	05-22-2020	All users	Enter License
Adobe Refresh Manager	1.8.0	03-25-2020	All users	Enter License
AdRem NetCrunch 10 Server	10.7.1.4789	11-19-2019	All users	Enter License
AIDA64	6.20.5300		All users	Enter License
Arena	16.00.00002	10-28-2019	All users	Enter License
CA ERwin Process Modeler	7.003.1773	11-25-2019	All users	Enter License
ChildWebGuardian PRO, версия	5.16.0.0	04-01-2019	All users	Enter License
Cisco Packet Tracer	7.1.0.0222	10-18-2019	All users	Enter License
CPN Tools	4.0.1		All users	Enter License
Definition Update for Microsoft Office 2010 (KB3115475) 32-Bit Edition			All users	Enter License
Entity Framework Designer for Visual Studio 2012 - enu	11.1.20810.00	12-12-2019	All users	Enter License
Google Chrome	83.0.4103.97	06-05-2020	All users	Enter License
Google Update Helper	1.3.35.451	03-25-2020	All users	Enter License
Icecream Screen Recorder, версия	5.92	04-18-2019	All users	Enter License
Intel(R) Processor Graphics	10.18.10.3910		All users	Enter License
Internet Lock	6.0		All users	Enter License
IP Video System Design Tool 10	v.10.0.0.1821	09-02-2019	All users	Enter License
Java 8 Update	8.0.1210.13	10-10-2019	All users	Enter License
Java Auto Updater	2.8.121.13	10-10-2019	All users	Enter License
K-Lite Codec Pack Standard	10.6.5	03-21-2019	All users	Enter License
Kaspersky Free	20.0.14.1085	05-13-2020	All users	Enter License
Kaspersky Secure Connection	20.0.14.1085	04-12-2020	All users	Enter License
Lightshot	5.4.0.35	03-22-2019	All users	Enter License

Рисунок 2.29 – Список программ одной из рабочих станций

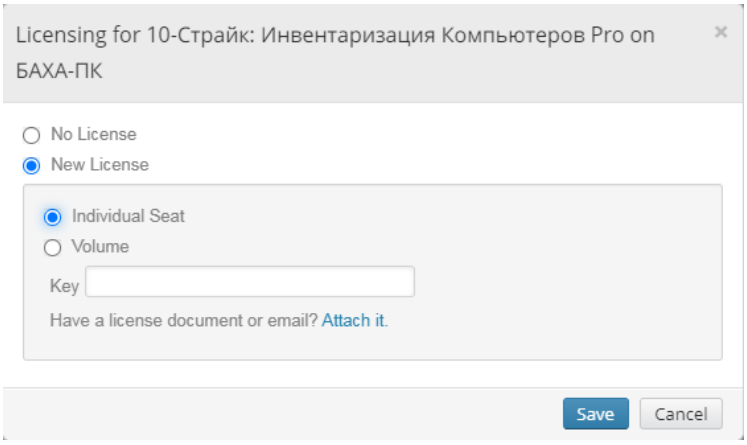

Рисунок 2.30 – Введение ключа лицензии программного обеспечения

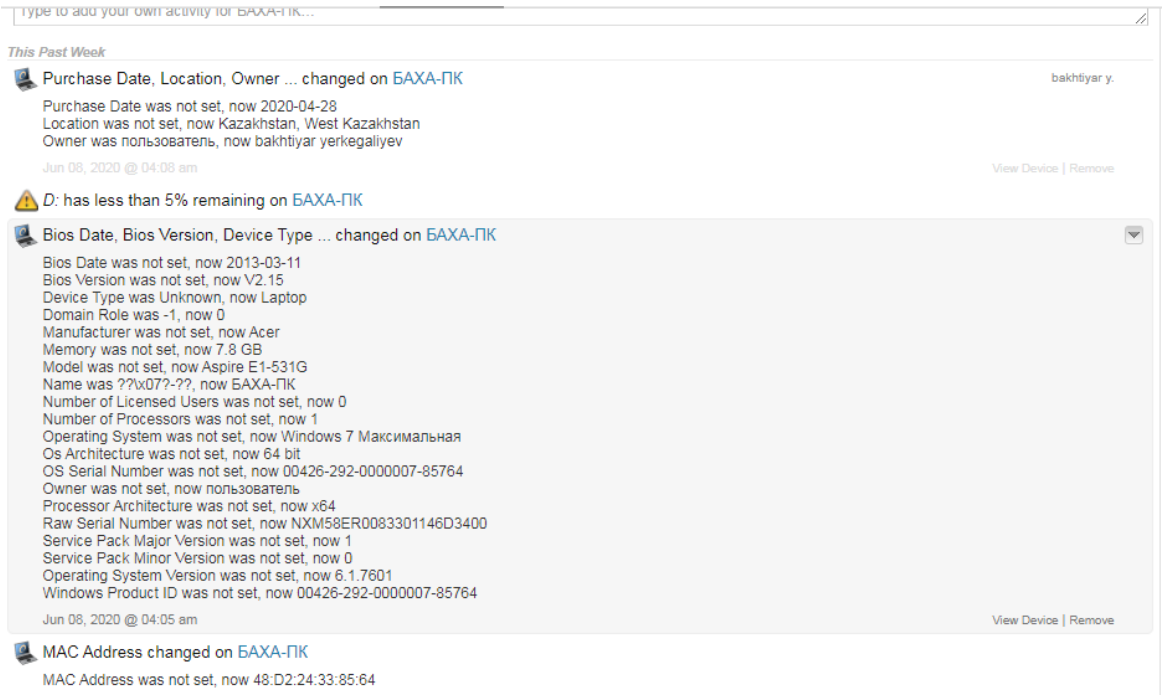

Рисунок 2.31– Информация о Bios рабочей станции

В «Микрофинансовой организация» также есть потребность в развертывании антивирусной защиты, поэтому необходимо определиться с селектом антивирусного ПО.

Для объективного выбора следует провести сравнительный анализ нескольких видов антивирусных предложений, которые будут доступны для организации, это: Kaspersky Endpoint Security (версия 12.0.0.7734), McAfee VSE (8.8 Scan Engine Hotfix 116778), Symantec Endpoint Protection (версия 14.2.2.1 build 5569), ESETNOD 32.

Результаты проведенного сравнительного анализа были отображены в виде таблицы для максимально удобного понимания разницы между тестируемыми программными обеспечениями. Сравнительный анализ антивирусного ПО представлен в приложении А.

Просматривая и сравнивая полученные данные, можно быть уверенным, что со всеми поставленными нами задачами, такими как постоянный мониторинг и контроль программ, интернет-ресурсов и дополнительных устройств, справился только один программный продукт - Касперский. Конкурентный антивирус McAfee показал себя довольно хорошо и получил хорошие результаты а также был номинирован за лучший “контроль устройств”, получив максимальную оценку, но, к сожалению, для веб-контроля и контроля программ этого недостаточно.

Еще одним существенным анализом антивирусных продуктов стало их практическое исследование для выявления уровня защиты персональных рабочих станций сотрудников. Для проведения этого анализа были внедрены еще три антивирусных средства: Dr. Web, AVG, TrustPort, таким образом общая картина сравнения программ данного класса стала еще полнее. Для

тестирования были задействованы 280 зараженных файлов с различными классами угроз, и то, как справились с ними тестируемые антивирусные программы, отображено в таблице 2.15.

Таблица 2.15 – Подробный анализ быстродействия антивирусного ПО

Антивирус	Найдено угроз	% определения	Время на поиск	Загрузка ЦП, %	Цена, тенге.
Касперский	251	96,3	23 мин	80-95	164.000
McAfee	249	90,1	12 мин	60-80	52.400
Dr. Web	215	77,3	1 мин 10 сек	50-60	155.000
AVG	208	74	5 мин 32 сек	15-30	70.000
Symantec	190	65	6 мин 10 сек	40-50	62.000
TrustPort	148	54,9	45 сек	40-50	45.000
ESET NOD32	140	50,8	1 мин 10 сек	40-50	88.000

По такому необходимому показателю как процентность определения угроз антивирус Касперского демонстрирует значение более 96%. Но, тем не менее время, которое было потрачено на уличение зараженных файлов и потребляемые ресурсы рабочей станции, оказались самыми большими среди всех тестируемых его конкурентов.

Исходя из результатов проведенных тестов, антивирус Касперского можно с уверенностью считать наилучшим вариантом для защиты информации в компании, к тому же цена на продукт лаборатории Касперского не является самой высокой.

В компании необходимо разработать стратегию антивирусной защиты. Стратегия антивирусной защиты предприятия направлена на осуществление многоуровневой защиты всех потенциально уязвимых мест в экосистеме организации, рисунок 2.32.

Рисунок 2.32 – стратегия антивирусной защиты

Более детально рассмотрим стратегию антивирусной защиты:

- инфраструктурный уровень. Данная структура сети, обеспечивающая должную защиту от несанкционированных вторжений для самых слабых и критично важных элементов сети. Она включает в работу защиту сети от атак всплывающих через инсталяцию сетевого шлюза с файерволом организации, фильтрация внешнего веб-трафика сети (в том числе входящих электронных писем), загружаемых интернет-страниц и служб мгновенных сообщений, которые чаще всего становятся источниками заражения;

- уровень программного обеспечения. Проводится работа по выявлению потенциально уязвимых приложений, регулярное своевременное обновление ПО с целью закрытия обнаруженных уязвимостей. Внедряется нужное ПО, в зависимости от целей конкретной организации;

- уровень оборудования. Прослеживается возможность и порядок применения внешних запоминающих устройств (Flash-накопители, оптические носители и прочее) с целью сокращения числа возможных источников заражения вирусами;

- уровень прав доступа. Регламентируются права пользователей системы, сводя к минимуму возможность проникновения вредоносных программ. Организовывается регулярное резервное копирование всей критичной информации для быстрого восстановления при необходимости. Проводится планомерный контроль состояния антивирусных программ, аудит безопасности сети и полные антивирусные проверки.

Комплексная защита сети от вирусов организации выполняет следующие задачи:

- защита рабочих станций сотрудников, предотвращает проникновение вредоносных программ из разных источников. Так обеспечивается активная защита от неизвестных в базе вирусов;

- защита шлюзов и сервера электронной почты, системы обмена электронной почтой и обеспечивает безопасную коллективную доступность к документам предприятия. Антивирус на почтовом сервере проводит ежедневный мониторинг и проверяет электронную почту, лечит или уничтожает поврежденные файлы. Система защиты не пропускает фишинг на

персональные компьютеры, куда попав вредоносный файл, начинает заражать и портить целостность документов;

- защита веб-трафика. Антивирус проверяет весь входящий и исходящий трафик, поступающий из Интернета, и удаляет вирусы. Данный этап существенно повышает общую защищенность персональных компьютеров в сети и является важнейшим дополнением к антивирусной защите рабочих мест и серверов, но не гарантирует полную безопасность;

- защита файлового сервера. В этом случае антивирус проверяет открываемые или редактируемые файлы. Проводится распределение системой серверных ресурсов между антивирусом и прочими серверными приложениями, предоставляя возможность минимального влияния на ключевые серверные службы;

- систематическое автообновление ПО позволяет устранять уязвимости в программных продуктах, предотвращая заражение, а не пытаясь бороться уже с действующим вирусом;

- обеспечение централизованного доступа к управлению элементами антивирусной защиты. Этот этап является ключевым в обеспечении безопасности корпоративной системы. Систематичное отслеживание всех элементов защиты дает возможность администратору максимально быстро реагировать и выявить проблему на одном компьютере, исключая ее распространение на следующие устройства. Отличие персональных антивирусных программ от корпоративных решений заключается именно в возможности централизованного мониторинга и администрирования. Даже в самых небольших сетях такая возможность крайне необходима для обеспечения безопасности.

Ранее было обосновано использование средств антивирусной защиты Kaspersky Internet Security. Однако существуют другие версии и комплектации программного обеспечения Kaspersky не ограничивается этой серией. Обоснуем выбор конкретного продукта. Для этого проведем сравнительный анализ. Результаты сравнения приведены в таблице 2.16.

Таблица 2.16 –Сравнительный анализ продуктов KIS

Тип защищаемого узла сети	KasperskySecurity для предприятия	Защита отдельных узлов сети

	Стартовый	Стандартный	Расширенный	Total	KIS для почтовых серверов	Kaspersky Systems Managament	KIS для интернет шлюзов	KIS для виртуальных сред
Рабочие станции	+	+	+	+				
Файловые серверы		+	+	+				
Мобильные гаджеты/планшеты		+	+	+				
Системное Администрирование			+	+		+		
Серверы совм. работы				+				
Почтовые серверы				+	+			
Интернет-шлюзы				+			+	
Виртуальная инфраструктура								+

На основе проделанного детального сравнительного анализа было принято решение остановиться на выборе пакета «Kaspersky Endpoint Security» в версии для малого и среднего бизнеса, но с приставкой «расширенный». «Kaspersky Endpoint Security для бизнеса расширенный» предоставляет возможность высокоэффективной технологии и инструментов системы обеспечения информационный безопасности IT-структуры для построения многоуровневой защиты. Технологии сканирования сети на наличие рисков и управления установкой исправлений устраняют уязвимости в операционных системах и приложениях, а технология шифрования данных обеспечивает защиту конфиденциальной информации в случае утери нетбука или попытки злоумышленником несанкционированного доступа к коммерческим данным организации.

Качественная инсталляция и настройка системы защиты локальной сети от вирусов на предприятии является задачей не из легких, требующей привлечения профессионального IT-специалиста. Ведь услуга комплексной антивирусной защиты может обеспечить предприятию надежность и высокую уровень безопасности функционирования ИС, гарантированно снижая риски вирусного заражения компьютерных систем предприятия.

3 Программный комплекс DeviceLock DLP Suite 8

Корпоративные данные имеющие коммерческую ценность для организации, которые вы пытаетесь защитить от внутренних и внешних нарушителей с помощью межсетевых экранов и сложный паролей, буквально утекают сквозь руки злоумышленников.

Программный комплекс DeviceLock DLP Suite включает в себя базовый компонент DeviceLock Base и взаимодополняющие его компоненты — NetworkLock, ContentLock, DeviceLock Discovery и DeviceLock Search Server (DLSS). Они лицензируются отдельно, в любых комбинациях. Агент DeviceLock выполняет весь спектр функций контроля внешних устройств и сетевого трафика на компьютере, где он установлен. То есть архитектурно анализ событий осуществляется непосредственно на рабочих станциях. Агент DeviceLock, содержащий в себе все три основных компонента комплекса (устанавливается на каждый компьютер, функционирует, начиная с уровня ядра Microsoft Windows, запускается автоматически и обеспечивает защиту от утечек данных, оставаясь в то же время невидимым для локального пользователя, рисунок 3.1, 3.2.

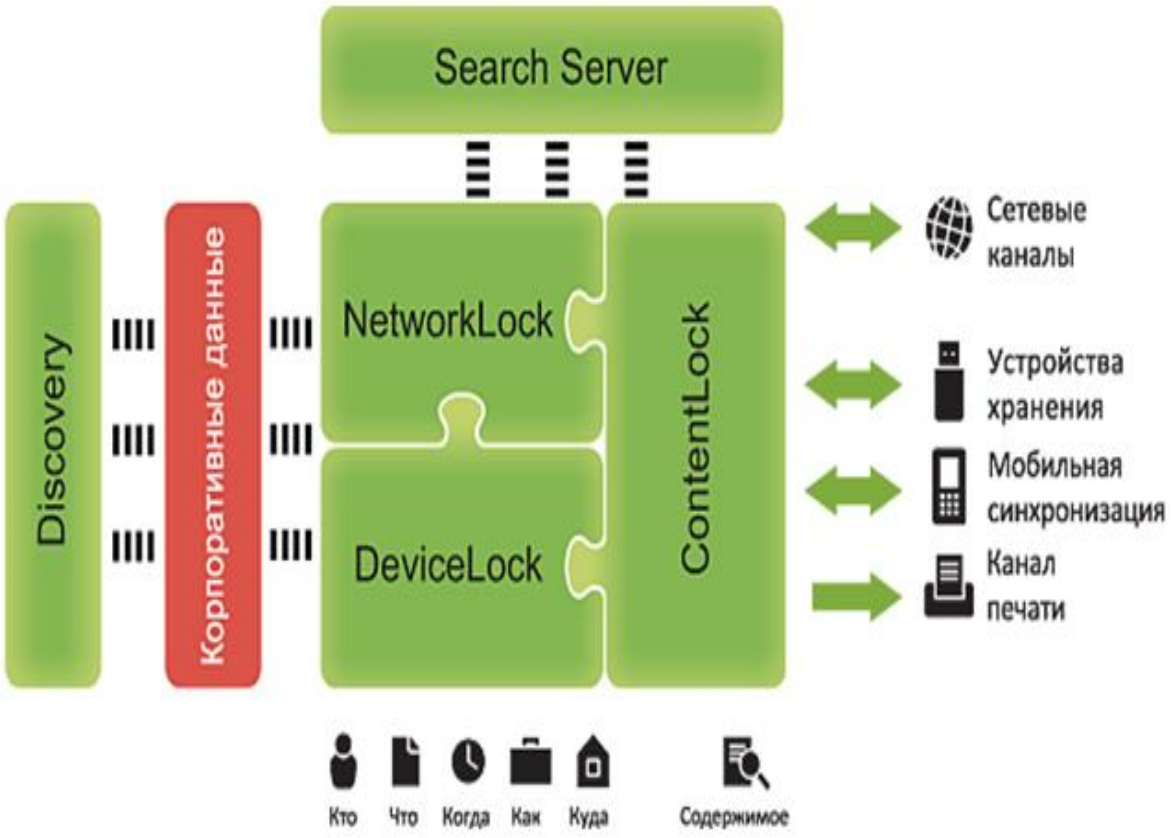

Рисунок 3.1 – Покомпонентный состав DeviceLock DLP

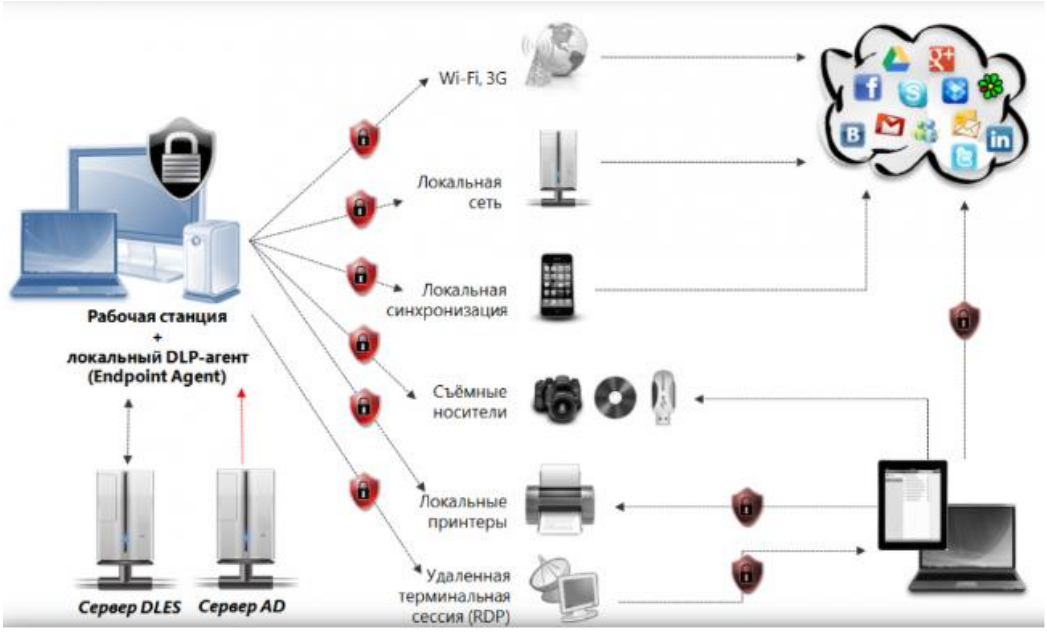

Рисунок 3.2 – Контроль каналов утечки данных в Агенте DeviceLock

DeviceLock DLP решает данную проблему и предотвращает утечки конфиденциальных данных, используя в своей работе огромный набор механизмов контекстного контроля операций с данными. Помимо всего прочего реализовывает контроль доступа к портам, интерфейсам, устройствам, сетевым протоколам и сервисам, журналирование доступа и событий передачи, а также сохранения данных, с применением контентной фильтрации непосредственно на контролируемых рабочих станциях при попытках передачи или сохранения. Является полноценной endpoint DLP-системой, рисунок 3.3.

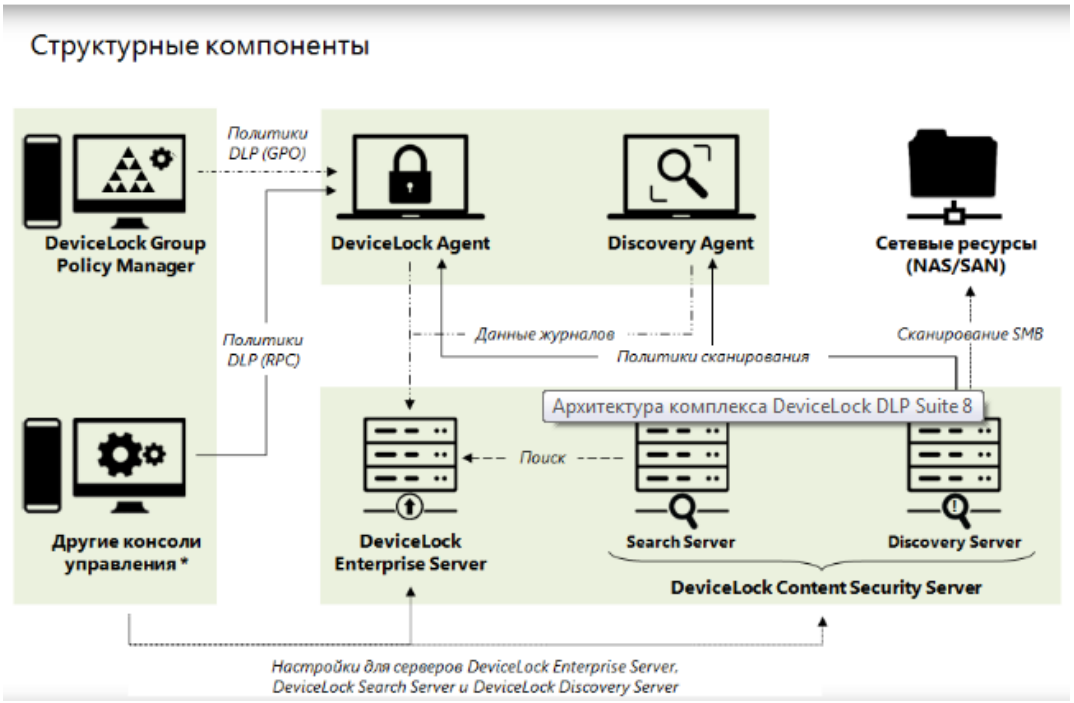

Рисунок 3.3 – Архитектура комплекса DeviceLock DLP

Также осуществляет весь спектр потенциально опасных устройств и сетевых коммуникаций: USB-порты, CD- и DVD-приводов, сменных накопителей, смартфонов на базе iOS, Windows Mobile, Palm и Blackberry, любых внешних и внутренних накопителей и жёстких дисков, локальных и сетевых принтеров, а также портов, буфер обмена Windows, простые и SSL-защищенные SMTP-сессии электронной почты, HTTP и HTTPS-сессии, MAPI и IMB/Lotus Notes, веб-почту (webmail) и социальные сети, службы мгновенных сообщений (Instant Messaging), файловый обмен по протоколам FTP, общие сетевые ресурсы (SMB), файлообменные сервисы (такие, как DropBox, SkyDrive), Telnet-сессии, Torrent. Процесс установки DeviceLock DLP представлена на рисунке 3.4, 3.5.

Рисунок 3.4 – Процесс установки системы

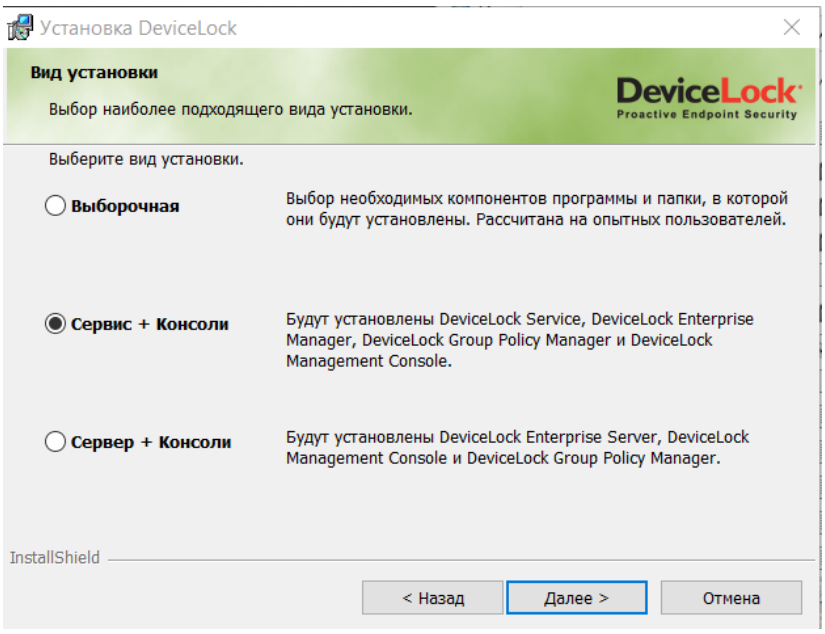

Рисунок 3.5 – Процесс установки DeviceLock DLP

DeviceLock поддерживает формирование политик безопасности на основании белых списков. Белый список USB-устройств — по производителю, модели устройства или уникальному серийному номеру. Белый список носителей CD/DVD-дисков на основе записанных на них данных с разрешением их использования, даже если сам CD/DVD-привод заблокирован. Запретим полноценный доступ USB – портов, рисунках 3.6, 3.7, 3.8, 3.9.

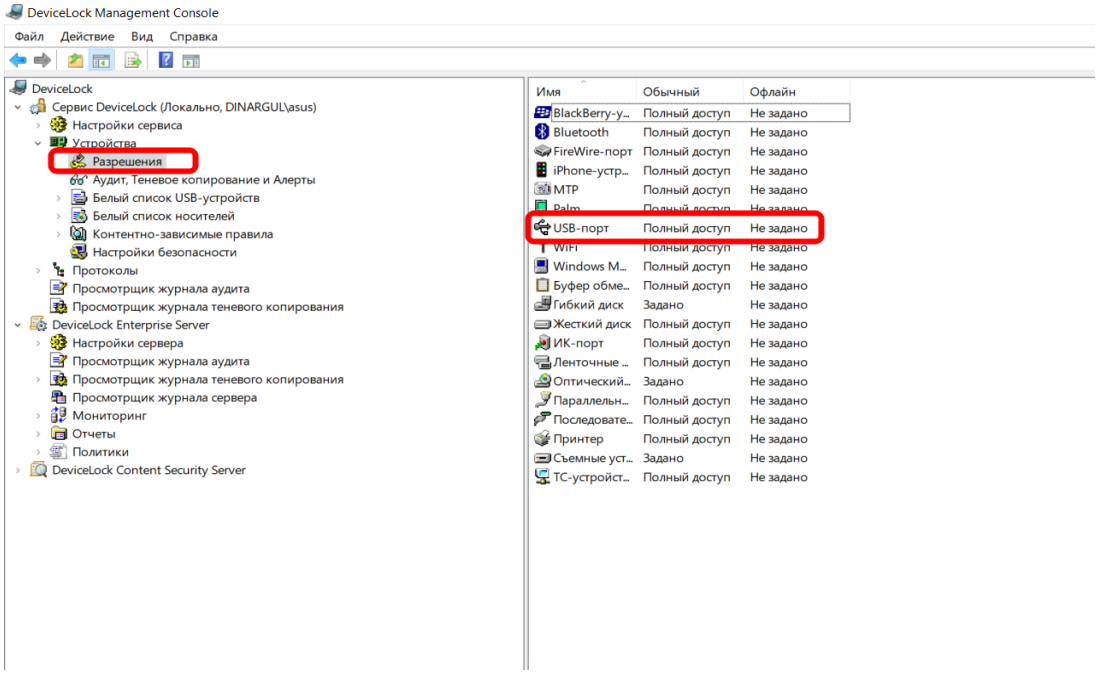

Рисунок 3.6 – Запрет на доступ USB – портов

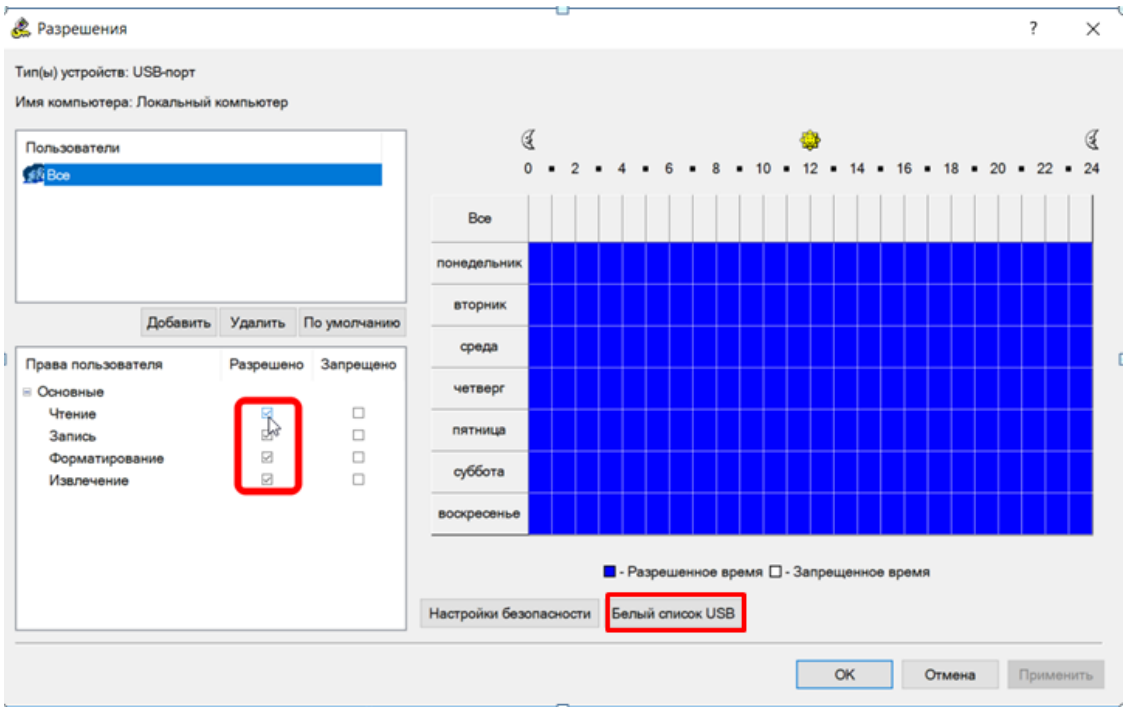

Рисунок 3.7 – Процесс запрета USB – портов

После подтверждения нажатием на кнопку ОК, можем проверить запрещен ли доступ к компьютеру USB – портов.

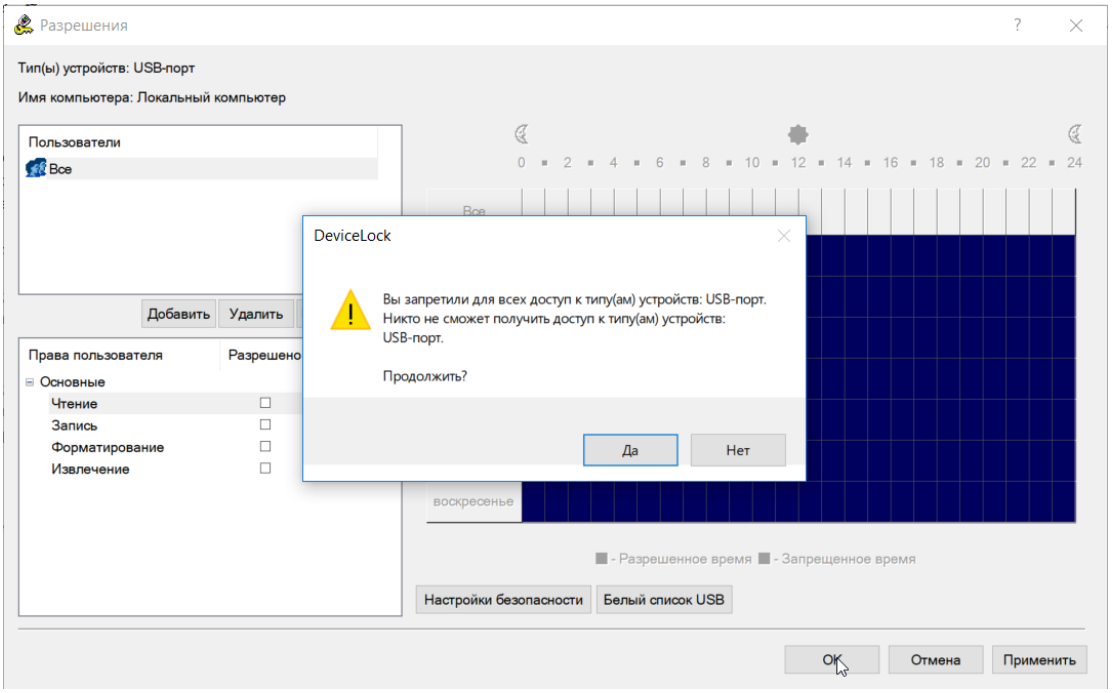

Рисунок 3.8 – Процесс запрета на использование USB – портов

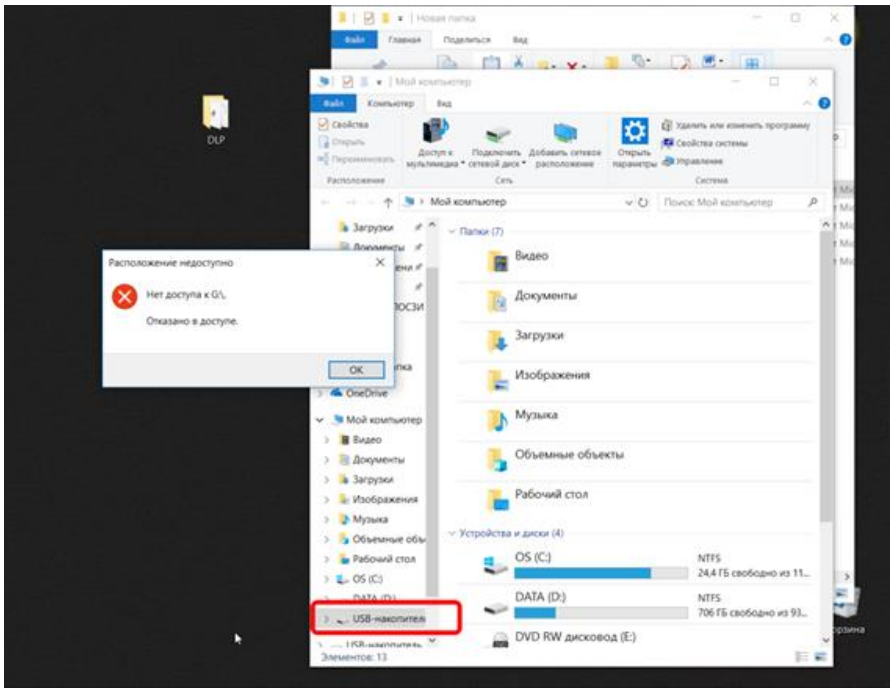

Рисунок 3.9 – Результат запрета на использование USB – портов

Вторым примером послужило запрет на копирование файлов, текста, изображения. На рисунке 3.10 представлены клюючевые возможности программного продукта DeviceLock.

Рисунок 3.10 – Возможности NetworkLock в составе DeviceLock

Компонент NetworkLock обеспечивает контекстный контроль каналов сетевого обмена данными на рабочих компьютерах, включая распознавание сетевых протоколов и используемых портов, детектирование приложений, инициирующих соединение и их селективную блокировку, реконструкцию сообщений и сессий с восстановлением файлов, данных и параметров, а также протоколирование и теневое копирование передаваемых файлов рисунок 3.11, 3.12.

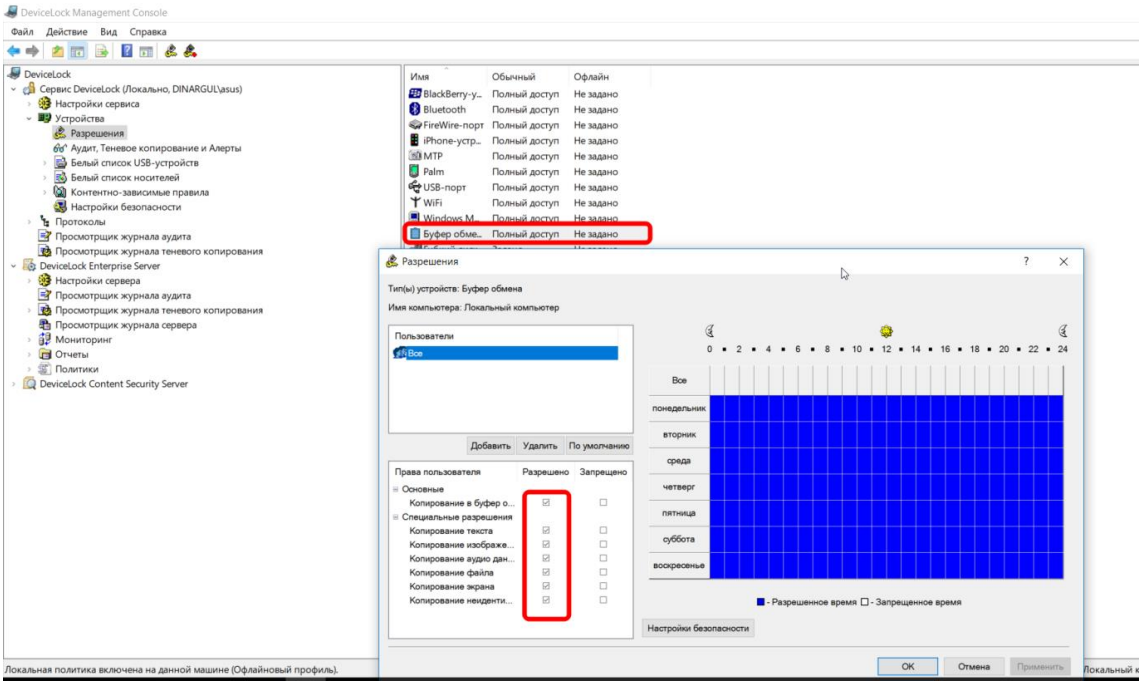

Рисунок 3.11 – Запрет на несанкционированное копирование данных на рабочей станции

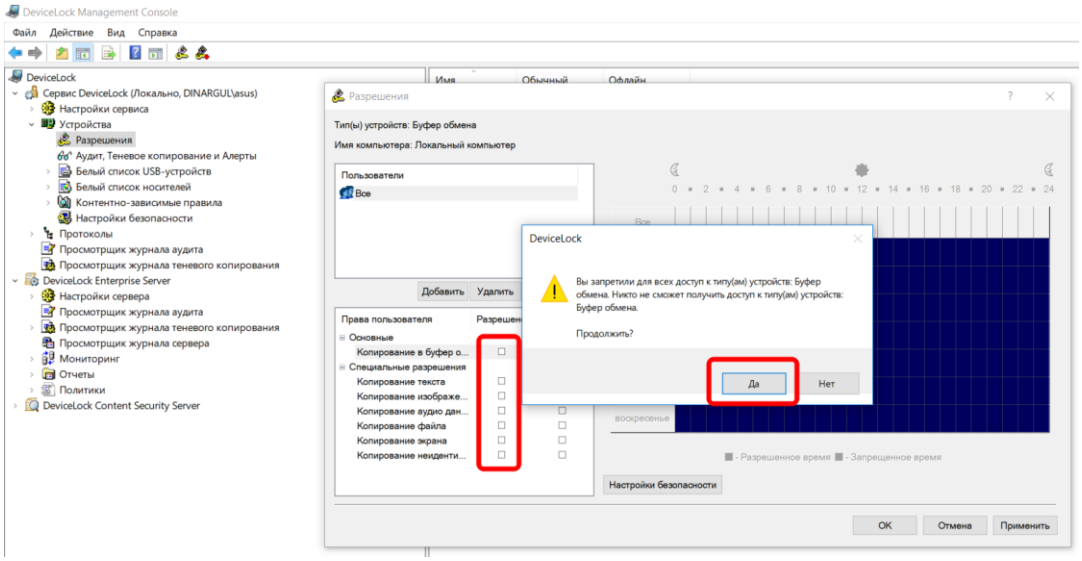

Рисунок 3.12 – Результат запрета на копирование данных

Также есть политики автономного и оперативного режима DeviceLock может применять один набор политик для ситуации, когда компьютер подключен к сети, доступен контроллер. Применение различных политик для двух режимов полезно, например, для запрета использования адаптеров Wi-Fi, когда компьютер подключен к офисной сети компании, и разрешения, когда находится за ее пределами. На рисунке 3.13 продемонстрирован запрет на запрет на доступ к сети Wi-Fi.

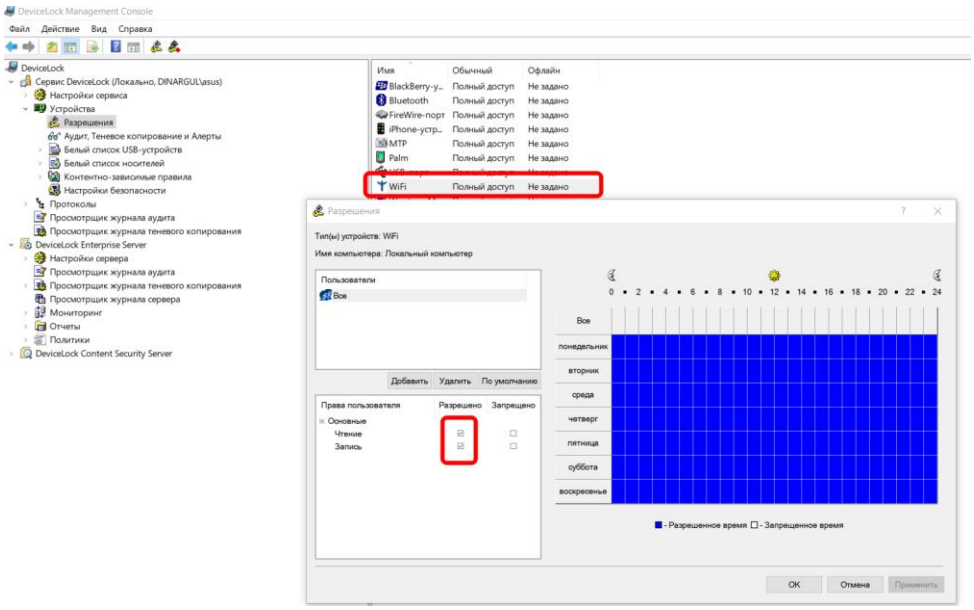

Рисунок 3.13 – Запрет на доступ к Wi-Fi

Аудит действий пользователей DeviceLock позволяет протоколировать все действия пользователей с устройствами и файлами (копирование, чтение, удаление и т. п.). Также можно настроить протоколирование изменений в настройках DeviceLock, время старта и остановки сервиса. DeviceLock использует стандартную подсистему протоколирования событий в Windows, а также автоматически собирает данные событийного протоколирования с удаленных компьютеров в локальной сети и хранит их в центральной базе данных SQL-сервера. Даже пользователи с административными правами (если они не входят в список авторизованных администраторов DeviceLock) не могут изменить, удалить или иным образом исказить теневые копии и данные журналов, как еще хранимые в локальном кэше на контролируемой рабочей станции, так и уже переданные на DeviceLock Enterprise Server.

Но также данный программный продукт даёт возможность просмотреть журнал аудита. В данном журнале показаны какие действия были успешно выполнены. Все запреты, которые оказались работоспособными приведены на рисунке 3.14.

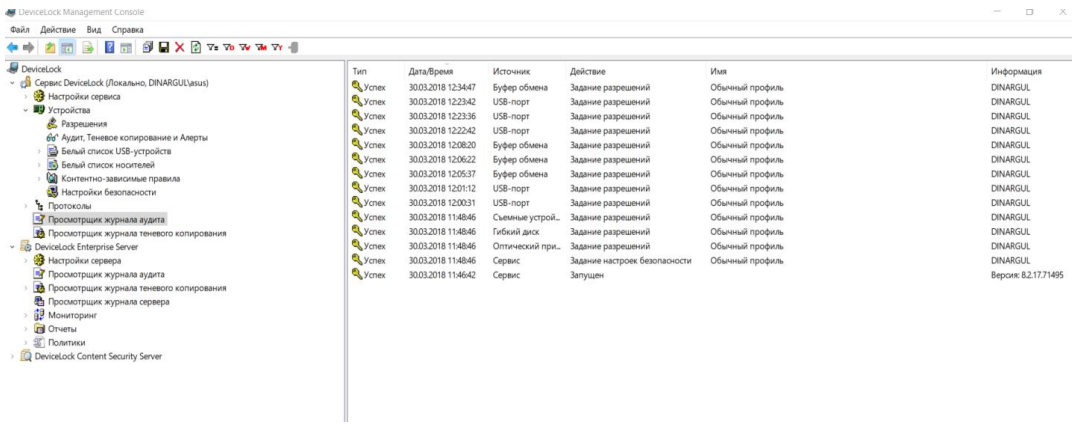

Рисунок 3.14 – Журнал аудита проделанных действий

4 Рекомендации по СОИБ для сотрудников

4.1 Ответственность

Ответственность, возлагаемая на сотрудников:

- все сотрудники «Микрофинансовой организации» взаимодействующие непосредственно с информацией несут ответственность за выполнение требований настоящей политики;
- сотрудники «Микрофинансовой организации», нарушающие требования информационной безопасности и руководители подразделений, не обеспечивающие их выполнение, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Республики Казахстан;
- контроль за выполнением требований настоящей политики возлагается на руководство «Микрофинансовой организации», руководство ИТ-управления, руководителей всех структурных подразделений «Микрофинансовой организации».

4.2 Основные принципы обеспечения ИБ организации

«Микрофинансовая организация» определяет следующие основные принципы обеспечения информационной безопасности:

- осведомленность о риске информационной безопасности. Процессы обеспечения информационной безопасности затрагивают каждого сотрудника «Микрофинансовой организации», использующего его информационные ресурсы, и накладывают на него соответствующие обязанности и ограничения. Персональная ответственность. Ответственность за нарушения требований информационной безопасности возлагается непосредственно на сотрудников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены;
- минимальность полномочий. Любому сотруднику «Микрофинансовой организации» доступ к информационным ресурсам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами;
- комплексность защиты. Меры по обеспечению безопасности информационных ресурсов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков информационной безопасности;
- адекватность защиты. Принимаемые меры обеспечения информационной безопасности эффективны и соразмерны имеющим место рискам информационной безопасности;
- эргономичность защиты. Средства защиты должны быть максимально “прозрачными” и удобными для пользователей и администраторов автоматизированных систем;

- документированность. Документирование обеспечивает закрепление достигнутого текущего состояния системы обеспечения информационной безопасности. Любые изменения этого состояния оформляются документально;

- непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности. В «Микрофинансовой организации» осуществляется постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых осуществляется анализ эффективности принятых мер обеспечения информационной безопасности с учетом изменений IT-среды, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты;

- контроль со стороны руководства. Руководство на регулярной основе рассматривают отчеты о состоянии информационной безопасности в подразделениях «Микрофинансовой организации» и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы. Политика информационной безопасности и предложения по ее актуализации рассматриваются Руководством на периодической основе;

- целевое финансирование мероприятий по обеспечению информационной безопасности. Ежегодный бюджет «Микрофинансовой организации» предусматривает специальные статьи расходов на обеспечение информационной безопасности.

4.3 Назначение и распределение ролей, обеспечение доверия к персоналу

«Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.

Роли формируются с учетом принципа минимальности полномочий. Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

В критичных системах по решению владельца информационного ресурса может вводиться роль администратора информационной безопасности автоматизированной системы, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности.

Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников «Микрофинансовой организации» под роспись.

4.4 Управление доступом к информационным ресурсам и регистрация

Все информационные ресурсы «Микрофинансовой организации» идентифицируются, категорируются и имеют своих владельцев. Доступ к информационным ресурсам всем сотрудникам «Микрофинансовой организации» предоставляется только на основании документально оформленных заявок, согласованных с их владельцами. По умолчанию определяется отсутствие доступа. Доступ к информационным ресурсам не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения сотрудника. Проводится периодический формальный контроль соответствия согласованных и реальных прав доступа к информационным ресурсам текущему статусу пользователя. Прямой доступ пользователей к базам данных не предоставляется. Доступ ко всем информационным ресурсам «Микрофинансовой организации» осуществляется только после авторизации пользователя. Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны, защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.

4.5 Безопасное использование ресурсов Интернет

Использование ресурсов Интернет в подразделениях «Микрофинансовой организации» разрешается исключительно в производственных целях. Взаимодействие с контрагентами по сети Интернет осуществляется с использованием специализированных систем и средств защиты, аттестованных на соответствие требованиям информационной безопасности.

Использование рабочих станций с доступом к ресурсам Интернет для обработки критичной информации запрещается.

Порядок публикации информации в сети Интернет определяется отдельными регламентами. Обсуждение сотрудниками «Микрофинансовой организации» на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний руководства. Доступ сотрудников к ресурсам сети Интернет санкционируется руководством и согласовывается службой

информационной безопасности, которая осуществляет контроль за соблюдением сотрудниками требований информационной безопасности, включая контентный анализ сообщений.

На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия хакерским атакам и распространению спама.

5 Безопасность Жизнедеятельности

5.1 Анализ потенциально опасных и вредных факторов в офисе, воздействующих на персонал

Опасные и вредные производственные факторы (ГОСТ 12.0.003-74) подразделяются на четыре группы: физические, химические, биологические и психофизиологические.

Физические опасные и вредные производственные факторы подразделяются на:

- движущиеся машины и механизмы, подвижные части производственного оборудования, передвигающиеся изделия, заготовки, материалы, разрушающиеся конструкции, обрушивающиеся горные породы;
- повышенная запыленность и загазованность воздуха рабочей зоны;
- повышенная или пониженная температура поверхностей оборудования, материалов;
- повышенное или пониженное барометрическое давление в рабочей зоне и его резкое изменение;
- повышенная или пониженная влажность воздуха;
- ионизация воздуха;
- ионизирующее излучение;
- повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека;
- повышенный уровень статического электричества, электромагнитных излучений и др.

Химические опасные и вредные производственные факторы подразделяются на: токсические, раздражающие, канцерогенные, мутагенные, влияющие на репродуктивную функцию.

Биологические опасные и вредные производственные факторы включают биологические объекты: микроорганизмы (бактерии, вирусы, грибы, простейшие и др.) и продукты из жизнедеятельности.

Психофизиологические опасные и вредные производственные факторы по характеру действия подразделяются на: физические перегрузки, нервно-психические перегрузки. Нервно-психические перегрузки это - умственное перенапряжение, перенапряженность анализаторов, монотонность труда, эмоциональные перегрузки.

Между вредными и опасными производственными факторами наблюдается определенная взаимосвязь. Во многих случаях наличие вредных факторов способствует проявлению травмоопасных факторов. Например, чрезмерная влажность в производственном помещении и наличие токопроводящей пыли (вредные факторы) повышают опасность поражения человека электрическим током (опасный фактор). Уровни воздействия на работающих вредных производственных факторов нормированы предельно-допустимыми уровнями, значения которых указаны в соответствующих

стандартах системы стандартов безопасности труда и санитарно-гигиенических правилах.

Предельно допустимое значение вредного производственного фактора (по ГОСТ 12.0.002-80) - это предельное значение величины вредного производственного фактора, воздействие которого при ежедневной регламентированной продолжительности в течение всего трудового стажа не приводит к снижению работоспособности и заболеванию как в период трудовой деятельности, так и к заболеванию в последующий период жизни, а также не оказывает неблагоприятного влияния на здоровье потомства. [1]

Условия труда подразделяются на 4 класса:

- 1-й класс – оптимальные условия труда;

- 2-й класс – допустимые условия труда, которые могут вызывать функциональные отклонения, но после регламентированного отдыха организм человека приходит в нормальное состояние (оптимальный и допустимый классы соответствуют нормальным условиям труда);

- 3-й класс – вредные условия труда, характеризующиеся наличием вредных производственных факторов, превышающих гигиенические нормы. Они оказывают неблагоприятное воздействие на работающего и могут негативно влиять на его потомство. Вредные условия труда по степени превышения гигиенических норм и выраженности изменений в организме работающих, в свою очередь, подразделяются на четыре степени вредности и опасности;

- 4-й класс – опасные (экстремальные) условия труда, при которых в течение рабочей смены, небольшого промежутка времени создается угроза для жизни, высокий риск возникновения тяжелых и острых профессиональных поражений. Работа в экстремальных условиях труда не допускается за исключением ликвидации аварийных ситуаций, проведения ремонтных работ.

В соответствии с правилами электробезопасности в служебном помещении должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Электрические установки, к которым относится практически все оборудование ЭВМ, представляют для человека большую потенциальную опасность, так как в процессе эксплуатации или проведении профилактических работ человек может коснуться частей, находящихся под напряжением. Специфическая опасность электроустановок – токоведущие проводники, корпуса стоек ЭВМ и прочего оборудования, оказавшегося под напряжением в результате повреждения (пробоя) изоляции, не подают каких-либо сигналов, которые предупреждают человека об опасности. Реакция человека на электрический ток возникает лишь при протекании последнего через тело человека. Исключительно важное значение для предотвращения электротравмотизма имеет правильная организация обслуживания

действующих электроустановок, проведения ремонтных, монтажных и профилактических работ.

В зависимости от категории помещения необходимо принять определенные меры, обеспечивающие достаточную электробезопасность при эксплуатации и ремонте электрооборудования.

Другим методом защиты является нейтрализация заряда статического электричества ионизированным газом. В промышленности широко применяются радиоактивные нитрализаторы. К общим мерам защиты от статического электричества можно отнести общие и местное увлажнение воздуха.

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. Во всех служебных помещениях обязательно должен быть “План эвакуации людей при пожаре”, регламентирующий действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

Пожары в вычислительных центрах представляют особую опасность, так как сопряжены с большими материальными потерями. Характерная особенность ВЦ – небольшие площади помещений. Как известно пожар может возникнуть при взаимодействии горючих веществ, окисления и источников зажигания. В помещениях ВЦ присутствуют все три основные фактора, необходимые для возникновения пожара. [2]

На работников могут оказывать неблагоприятное воздействие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень ионизирующих излучений;
- повышенный уровень статического электричества;
- повышенная напряженность электростатического поля;
- повышенная или пониженная ионизация воздуха;
- повышенная яркость света;
- прямая и отраженная блесткость;
- повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека;
- статические перегрузки костно-мышеч-ного аппарата и динамические локальные перегрузки мышц кистей рук;
- перенапряжение зрительного анализатора;
- умственное перенапряжение;
- эмоциональные перегрузки;
- монотонность труда.

В зависимости от условий труда, в которых применяются ПК, и характера работы на работников могут воздействовать также другие опасные и вредные производственные факторы.

Количество опасных и вредных производственных факторов у электромонтера меньше, чем у офисного работника. Конечно, вероятность

получить производственную травму, а также степень тяжести травмы у электромонтера выше, чем у сотрудника, работающего в офисе.

Однако основной сложностью трудового процесса (при условии использования хорошей оргтехники), связанного с работой на компьютере, является тяжесть трудового процесса (а именно стереотипные рабочие движения, рабочая поза), а также напряженность трудового процесса:

- интеллектуальная нагрузка (восприятие сигналов и их оценка);
- сенсорная нагрузка (длительность сосредо-точенного наблюдения, плотность сигналов, наблюдение за экранами видеотерминалов);
- эмоциональная нагрузка (степень ответственности за результат своей деятельности);
- монотонность нагрузок (продолжительность выполнения повторяющихся операций).

Пользователь ПЭВМ и его руководитель должны знать о вредном воздействии факторов и об эффективных способах зашиты от них, что уменьшает вероятность получения ими различных профессиональных заболеваний, а также снижает количество сбоев и ошибок в работе операторов.

Необходимо более подробно остановиться именно на анализе вредных и опасных производственных факторов, воздействующих на персонал, работающий в офисе.

Перечислим основные нарушения, допускаемые со стороны администрации:

- практически нигде не проводится аттестация рабочих мест по условиям труда, а это значит, что существующие нарушения требований безопасно не выявляются и не устраняются;
- большинство операторов и пользователей ПК не знают, какие опасные и вредные производственные факторы действуют на них на компьютеризированном рабочем месте;
- работающие на ПЭВМ не знают фактических величин параметров опасных и вредных производственных факторов, действующих на рабочем месте;
- операторы (и другие пользователи) не знакомы с основами трудового законодательства об охране труда, со своими правами, с обязанностями администрации по обеспечению нормальных условий труда;
- на предприятиях отсутствуют нормативные документы по охране труда и безопасности ПК;
- практически повсеместно не проводится обучение безопасным приемам и методам труда на ПК, а также инструктирования операторов, программистов, техников и других пользователей, тогда как работы на ПК нередко относятся к категории работ с опасными и вредными условиями труда (на основании документа Р 2.2.755-99);
- находящиеся в эксплуатации и приобретаемые вновь мониторы практически нигде не имеют сертификатов безопасности и гигиенических

сертификатов (согласно требованиям СанПиН 2.2.2.542-96), причем торгующие организации зачастую вручают малограмотным покупателям фальсифицированные гигиенические сертификаты и сертификаты безопасности;

- операторы и пользователи не проходят периодических медосмотров как работающие во вредных условиях труда на основании приказа Минздрава РК и департамента Госкомсанэпиднадзора РК от 05.10.1995 № 280/88, а именно: п.п. 5.2.2 (электромагнитные поля радиочастот); п.п. 6.1.5 (работы, связанные с локальными мышечными напряжениями преимущественно мышц кисти и предплечья); п.п. 6.2 (зрительно-напряженные работы и наблюдение за экраном);

- далеко не всем операторам и пользователям выдаются положенные им средства индивидуальной защиты на основании п. 3.8 СанПиН 2.2.2.542-96;

- большинство работодателей не затрачивают достаточных средств на оборудование рабочих мест в соответствии с требованиями норм (в частности, по обеспечению освещенности, необходимого воздухообмена, аэроионного состава и микробиологической чистоты воздуха; по обеспечению эргономичной мебелью и т. п.);

- во многих офисных и производственных помещениях и мест место несоответствие санитарным нормам по площади и объему на одного работающего (нередко эти параметры оказывались меньше нормы в 2-2,5 раза).

На работающего на ПЭВМ постоянно или периодически действуют следующие опасные и вредные факторы:

- загрязнение воздуха вредными веществами, пылью, микроорганизмами и положительными аэроионами;

- несоответствие нормам параметров микроклимата;

- возникновение на экране монитора статистических зарядов, заставляющих частички пыли двигаться к ближайшему заземлённому предмету, часто им оказывается лицо оператора;

- повышенный уровень шума на рабочем месте;

- повышенный уровень статистического электричества при неправильно запроектированной рабочей зоне;

- опасный уровень напряжения в электрической цепи, замыкание которой может пройти через тело человека;

- широкий спектр излучения от дисплея, который включает рентгенов скую, ультрафиолетовую и инфракрасную области, а также широкий диапазон электромагнитных излучений других частот;

- повышенный уровень электромагнитных излучений;

- повышенный уровень ионизирующих излучений (мягкое рентгеновское, гамма-излучение);

- отсутствие или недостаток естественного света;

- недостаточная освещенность рабочей зоны;

- повышенная яркость света;

- пониженная контрастность;
- прямая и обратная блёсткость;
- повышенная пульсация светового потока (мерцание изображения);
- длительное пребывание в одном и том же положении и повторение одних и тех же движений приводит к синдрому длительных статических нагрузок (СДСН);
- нерациональная организация рабочего места;
- несоответствие эргономических характеристик оборудования нормируемым величинам;
- умственное перенапряжение, которое обусловлено характером решаемых задач приводит к синдрому длительных психологических нагрузок (СДПН);
- большой объем перерабатываемой информации приводит к значительным нагрузкам на органы зрения;
- монотонность труда;
- нервно-психические нагрузки;
- нервно-эмоциональные стрессовые нагрузки;
- опасность возникновения пожара.

Остановимся подробнее на недостаточной освещенности рабочей зоны помещения, где установлены ПЭВМ, а также на влиянии повышенной яркости света, пониженной контрастности, прямой и обратной блёсткости и повышенной пульсации светового потока.

Нарушение функционального состояния зрительного анализатора проявляется в снижении остроты зрения, устойчивости ясного видения, аккомодации, электрической чувствительности и лабильности.

Причинами нарушения функционального состояния зрительного анализатора являются:

- постоянная переадаптация органов зрения в условиях наличия в поле зрения объекта различения и фона различной яркости;
- недостаточная четкость и контрастность изображения на экране;
- срочность воспринимаемой информации;
- постоянные яркостные мелькания;
- наличие ярких пятен на клавиатуре и экране за счет отражения светового потока;
- большая разница между яркостью рабочей поверхности и яркостью окружающих предметов, наличие равноудаленных предметов;
- невысокое качество исходной информации на бумаге;
- неравномерная и недостаточная освещенность на рабочем месте. Наряду с перечисленными общепринятыми особенностями работы пользователя на рабочем месте ПЭВМ существуют особенности восприятия информации с экрана монитора.

Особенностями восприятия информации с экрана монитора органами зрения пользователя ПЭВМ являются следующие:

- экран монитора является источником света, на который в процессе работы непосредственно обращены органы зрения пользователя, что вводит оператора в другое психофизиологическое состояние;

- привязанность внимания пользователя к экрану монитора является причиной длительности неподвижности глазных и внутриглазных мышц, что приводит к их ослаблению;

- длительная и повышенная сосредоточенность органон зрения приводит к большим нагрузкам, а следовательно, к утомлению органов зрения, способствует возникновению близорукости, головной боли и раздраженности, нервного напряжения и стресса;

- длительная привязанность внимания пользователя к экрану монитора создает дискомфортное восприятие информации, в отличие от чтения обычной печатной информации;

- экран монитора является источником падающего светового потока на органы зрения пользователя, в отличие от обычной печатной информации, которая считывается за счет отраженного светового потока;

- информация на экране монитора периодически обновляется в процессе сканирования электронного луча по поверхности экрана и при низкой частоте происходит мерцание изображения, в отличие от неизменной ин формации на бумаге. [3]

Для снижения нагрузки на органы зрения пользователя при работе на ПЭВМ необходимо соблюдать следующие условия зрительной работы.

При работе на ПЭВМ пользователь выполняет работу высокой точности, при минимальном размере объекта различения 0,3-0,5мм (толщина символа на экране), разряда работы III, подразряда работы Г (экран - фон светлый, символ - объект различения - темный или наоборот).

Естественное боковое освещение должно составлять 2%, комбинированное искусственное освещение – 400 лк, при общем освещении - 200 лк.

К системам производственного освещения предъявляются следующие основные требования:

- соответствие уровня освещенности рабочих мест характеру выполняемой работы, достаточно равномерное распределение яркости на рабочих поверхностях и в окружающем пространстве, отсутствие резких теней, пря мой и отраженной блескости (блескость - повышенная яркость светящихся поверхностей, вызывающая ослепленность);

- оптимальная направленность излучаемого осветительными приборами светового потока.

Искусственное освещение в помещении и на рабочем месте создает хорошую видимость информации, машинописного и рукописного текста, при этом должна быть исключена отраженная блескость.

В связи с этим предусматриваются мероприятия по ограничению слепящего воздействия оконных проемов и прямое попадание солнечных лучей, а также исключение на рабочих поверхностях ярких и темных пятен.

Площадь оконных проемов должна составлять не менее 25% площади пола. В помещении рекомендуется комбинированная система освещения с использованием люминесцентных ламп. Для проектирования местного освещения рекомендуются люминесцентные лампы, светильники которых установлены на столе или его вертикальной панели.

Светильники местного освещения должны иметь приспособления для ориентации в разных направлениях, устройства для регулирования яркости и защитные решетки от ослепления и отраженного света.

Для создания равномерной освещенности рабочих мест при общем освещении светильники с люминесцентными лампами встраиваются непосредственно потолок помещения и располагаются в равномерно-прямоугольном порядке. Наиболее желательное расположение светильников - в непрерывный сплошной ряд вдоль длинной стороны помещения

5.2 Расчет защитного зануления

В офисном помещении находится серверная стойка, электропитание которой производится с помощью четырехпроходной линии и трансформатора с обмотками низшего напряжения 400/230 В. В целях обеспечения электробезопасности для серверной стойки было решено использовать защитное зануление. Необходимо рассчитать параметры зануления и определить отключающую способность зануления.

Для данной задачи:

- длина четырехпроходной линии – 400 м;
- номинальное напряжение обмоток низшего напряжения трансформатора – 400/230 В;
- номинальное напряжение обмоток высшего напряжения трансформатора – 10 кВ;
- мощность трансформатора - 160кВА;
- схема соединения обмоток трансформатора – D/Y_H;
- провода линии – медные, сечение проводов – 25 $мм^2$;
- плотность тока в нулевом защитном проводнике – 1 $А/мм^2$;
- сечение нулевого защитного проводника – 20 $мм^2$;
- характеристики двигателя: двигатель серии 4АС номинальной мощностью 12кВт, коэффициент мощности cos f =0,85, КПД=82,5;
- номинальный ток вставки двигателя - 50А.

Для начала необходимо определить приближенное полное расчетное сопротивление трансформатора. Значение берется из таблицы 5.1.

Таблица 5.1 – Приближенные полные расчетные сопротивления трансформаторов Z_t (Ом) для схемы соединения D/Y_H

Мощность трансформатора, кВА	Номинальное напряжение обмоток высшего напряжения, кВ	Схема соединения обмоток
		D/Y_H
25	6-10	0,906
40	6-10	0,562
63	6-10	0,360
	20-35	0,407
100	6-10	0,226
	20-35	0,327
160	6-10	0,141
	20-35	0,203
250	6-10	0,090
	20-35	0,130
400	6-10	0,056
	20-35	-
630	6-10	0,042
	20-35	-
1000	6-10	0,027
	20-35	0,032
1600	6-10	0,017
	20-35	0,020

По таблице 5.1 видно, что трансформатор мощностью 160 кВА с номинальным напряжением обмоток высшего напряжения 10 кВ и схемой соединения обмоток D/Y_H, имеет приближенное полное расчетное сопротивление трансформатора, равное 0,141 Ом.

Таким образом, $Z_t = 0,141$ Ом.

Следующий шаг – определение допустимого значения тока короткого замыкания. Определятся по формуле (5.1):

$$J^{Д}_{к.з.} \geq 3 * J^{ПВ}_{н}, \quad (5.1)$$

где $J^{ПВ}_{н}$ – номинальный ток вставки двигателя.

Расчет:

$J^{Д}_{к.з.} \geq 3 * 50$.

$J^{Д}_{к.з.} \geq 150$ А.

Далее необходимо определить активное сопротивление нулевого защитного провода. Расчет производится по формуле (5.2):

$$R_H = 1,2 * ((\rho_н * l_н)/S_н), \quad (5.2)$$

где $\rho_н$ – удельное сопротивление нулевого защитного провода (для меди – 0,018 Ом*мм^2/м);

$l_н$ – длина нулевого защитного провода, м;

$S_н$ – сечение нулевого проводника, мм^2.

Расчет активного сопротивления фазного тока:

$R_Н$ = (1,2 * 0,018 * 400) / 20 = 8,64 / 20 = 0,432 Ом.

Расчет активного сопротивления нулевого защитного провода:

$R_Н$ = (1,2 * 0,018 * 400) / 20 = 8,64 / 20 = 0,432 Ом.

Заключительный этап – расчет тока короткого замыкания. Определяется по формуле (5.3):

$$J_{к.з.} = U_Ф / ((Z_t/3) + (R_Ф+R_Н)^2) \quad (5.3)$$

Отключающая способность средств защиты от тока замыкания обеспечена, если соблюдается следующее условие (5.4):

$$J_{к.з.} \geq J^Д_{к.з.} \quad (5.4)$$

Расчет:

$J_{к.з.}$ = 220 / ((0,141/3) + (0,17 +0,432)^2 = 220 / (0,047+0,602^2) = 220 / 0,409 = 538 А.

538 А > 150 А – верно.

Ответ: да, отключающая способность средств защиты от тока короткого замыкания обеспечивается.

5.3 Расчет микроклиматических условий в офисе: норма воздухообмена

Необходимо рассчитать один из параметров микроклиматических условий (для офисного помещения), а именно – норма воздухообмен в офисном помещении (при этом было принято решение использовать вытяжную вентиляцию).

Для расчета были приняты следующие входные данные:

- длина помещения: 25 м;
- ширина помещения: 18 м;
- высота помещения: 4,5 м;
- число человек, постоянно находящихся в помещении офиса: 10;
- число временных посетителей офисного помещения (в расчете на один день): 30.

Расчет воздухообмена будет производиться на основании двух алгоритмов:

- по кратности воздухообмена;
- на основании количества человек, находящихся в помещении.

Приступим к расчету нормы воздухообмена по кратности воздухообмена. Кратность берется из СНиП № 2.09.04.87 (значения представлены в таблице 5.2).

Таблица 5.2 – Кратность воздухообмена

Наименование помещений	Кратность воздухообмена к, $ч^{-1}$	
	по притоку	по вытяжке
Курительные	—	10
Помещения для отдыха	5	4
Помещения для обогрева работающих	5	5

Рассчитать количество воздуха, которое должно быть обновлено в течение часа, следует по формуле (5.5):

$$L=N*V, \quad (5.5)$$

где N – кратность воздухообмена за час, взятая из таблицы 2;

V – объём помещения, куб.м.

Производим расчет по формуле (5.5):

$V = 25*18*4,5$ ($м^3$) = 2025 $м^3$.

N = 4 (кратность воздухообмена по вытяжке).

$L = 2025\ м^3 * 4 = 8100\ м^3$.

Воздухообмен: 8100 $м^3$.

Произведем расчет нормы воздухообмена на основании количества человек, находящихся в помещении.

Норма воздухообмена в расчете на 1 человека для рабочего помещения берется на основании СНиП № 2.09.04.87, таблицы 5.3.

Таблица 5.3 - Нормы воздухообмена в помещениях общественных зданий

Наименование помещения	Плотность, $м^2$/чел.	Норма воздухообмена по ASHRAE 62–1–2004		Норма воздухообмена по ASHRAE 62–1–1999	
		$м^3$/(ч •чел.)	$м^3$/(ч • $м^2$)	$м^3$/(ч • чел.)	$м^3$/(ч • $м^2$)
1	2	3	4	5	6
Административные здания Офисные помещения	20	30	1,5	36	2,6*
Офисные помещения при плотности 10 $м^2$/чел., кабинет	10 18	30	3,0	36	3,6

Рассчитаем плотность постоянно находящихся в офисе людей.

Площадь помещения S = 25*18 = 450 $м^2$.

Количество постоянно находящихся в офисе: 10 человек.

Плотность > 10 $м^2$/чел. Следовательно, при расчетах ориентируемся на вторую строку в таблице 3.

Норма воздухообмена по ASHRAE 62–1–2004: 30 $м^3$/чел.

Для временных посетителей примем норму воздухообмена = 15 $м^3$/чел.

Расчет воздухообмена:

L = 30 $м^3$/чел * 10 + 15 $м^3$/чел * 30 = 750 $м^3$.

6. Расчёт рисков информационной безопасности

6.1 Анализ и расчет рисков информационной безопасности

Дипломный проект посвящен созданию системы информационной безопасности предприятия. Сама тема охватывает достаточно обширную область: защита физического доступа, система видеонаблюдения, программные средства защиты информации и т.д.

Целью выполнения дипломной работы является построение системы защиты для некой организации, следовательно, риски будут проанализированы и рассчитаны для объектов этой организации (незащищенных, например, серверная комната), затем для уменьшения этих рисков будут применены меры по их обработке, некоторые из них - методы и средства, рассмотренные в ходе выполнения данной работы. С учетом применения данных мер и будут рассчитаны остаточные риски.

В процессе анализа рисков информационной безопасности в первую очередь, опираясь на тему дипломного проекта, были выделены защищаемые активы. Это серверная комната, рабочие станции, локальная сеть.

Как и упоминалось ранее, тема, рассматриваемая в данной работе достаточно обширна, поэтому активы были подобраны так, чтобы можно было рассмотреть различные виды мер обеспечения информационной безопасности, это организационные и технические (как программные, так и аппаратные средства):

- серверная комната – рассматриваются технические аппаратные средства защиты информации. Для защиты данного актива будут применяться такие средства, как ключ-карты (контроль физического доступа), видеонаблюдение и т.д. Комната представляет собой помещение, в котором находятся все важные серверы компании: бэкап-сервер, веб-сервер, файловый сервер и т.д.;
- рабочие станции – рассматриваются программные средства (к примеру, антивирус, парольная защита) и организационные меры (например, инструктаж сотрудников);
- локальная сеть - рассматриваются как организационные (например, тщательное планирование топологии сети), так и технические программные, и технические аппаратные средства обеспечения информационной безопасности.

Для анализа рисков был выбран алгоритм, представленный в стандарте ISO-27005. Расчет по данному алгоритму производится на основе оценки степени вероятности возникновения угрозы, простоты использования уязвимости и ценности актива. Алгоритм представлен в таблице 6.1.

Таблица 6.1 - Ценность активов, уровни угроз и уязвимостей

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Простой общий рейтинг рисков:

- низкий риск (приемлемый): 0-2;
- средний риск: 3-5;
- высокий риск (неприемлемый): 6-8.

Анализ рисков (угроз и уязвимостей) информационной безопасности для вышеперечисленных активов представлен в таблице 6.2.

Таблица 6.2 – Анализ рисков информационной безопасности

Угрозы	**Уязвимости**	**Максимальный уровень риска**	**Меры по обработке риска**	**Остаточный уровень риска**	**Комментарии, ресурсы, ответственный**
Актив1. Серверная комната					
1 Несанкцио-нированный доступ на территорию помещения	Отсутствие контрольно-пропускных механизмов	8	Система контроля управления доступом: ключ-карты для аутентификации легитимных пользователей. Видеонаблюдение	2	Начальник физической безопасности
2 Возникновение пожара. Может повлечь порчу оборудования	Нахождение помещения рядом с пожароопасным объектом в связи с изначально неправильной планировкой здания	7	Достаточно оперативная газовая система пожаротушения	2	Начальник пожарной безопасности
3 Сбои в электросети, что может повлечь за собой выход из строя аппаратуры в серверной комнате	Несоблюдение норм электрической безопасности в помещении серверной комнаты	6	Источник бесперебойного питания и независимые питающие центры	1	Начальник электробезопас ности
Актив 2. Рабочие станции					
4 Заражение вредоносным вирусным ПО, направленным на повреждение данных	Отсутствие антивируса или неосторожность пользователя	6	Антивирус. Инструктаж сотрудников	1	Системный администратор

компьютера					

Продолжение таблицы 6.2

5 Использование уволенным сотрудником своих учетных данных для авторизации и получения ресурсов, которые были ему доступны	Учетные записи уволенных сотрудников не удаляются	5	Автоматизированное удаление учетных данных уволенных сотрудников	1	Системный администратор
6 Нарушение функционирования ПО компьютера в результате неосторожных действий пользователя. Например, заражение вирусом после вставки в компьютер сотрудником личной флешки	Отсутствие автоматизированного контроля действий пользователей. Недостаточный инструктаж сотрудников	5	Системы управления действиями пользователей: DLP-система. Инструктаж сотрудников	1	Системный администратор
Актив 3. Локальная сеть					
7 Некорректная фильтрация трафика	Неправильное расположение межсетевых экранов в топологии сети	6	Тщательное планирование и переосмысление топологии сети	1	Сетевой администратор
8 Поломка и выход из строя ключевых элементов сети. Нарушение функционирования сетевой инфраструктуры	Недостаточное техническое обслуживание оборудования + отсутствие резервного копирования конфигурации сетевого оборудования	6	Резервное копирование конфигурации сетевого оборудования. Планирование и организация регулярного техобслуживания	1	Сетевой администратор
9 Перехват незащищенного трафика с конфиденциальной информацией	Отсутствие защиты передачи трафика	7	Шифрование. Туннелирование. VPN	2	Сетевой администратор
10 Взлом пароля и получение несанкционированного доступа к управлению важными элементами сети: межсетевой экран, маршрутизатор и т.д.	Отсутствие многофакторной аутентификации: доступ осуществляется только по паролю	8	Многофакторная аутентификация. Использование биометрической аутентификаци	2	Сетевой администратор

В таблице 6.2 были проанализированы и оценены различные рисковые ситуации для трех активов (серверная комната, рабочие станции и локальная сеть). Риски были перерассчитаны с учетом указанных защитных мер, и в результате этого риски уменьшились в среднем в 3-4 раза.

Далее будут показаны диаграммы взаимосвязи элементов анализа вышеперечисленных рисков (угроз и уязвимостей), реализованные в программе CORAS.

На рисунке 6.1 представлена диаграмма, на которой показаны защищаемые активы, для удобства разделенные на категории. Диаграмма читается слева направо. Первая часть данной диаграммы – категории защищаемых активов: «помещение», «оборудование», «программное обеспечение», «среда передачи данных». Следующая часть диаграммы – это сами активы. Так, актив «серверная комната» принадлежит категории «помещение», актив «рабочие станции» принадлежит одновременно двум категориям – «оборудование» и «программное обеспечение», актив «локальная сеть организации» принадлежит категории «среда передачи данных».

На рисунке 6.2 представлена диаграмма, на которой показана модель угроз. Диаграмма читается слева направо. Данная схема иллюстрирует модель реализации угрозы со всеми ее компонентами: источник угрозы, эксплуатируемые уязвимости, сами угрозы, результаты реализации угрозы (атака), целевые активы. Источники угрозы: «нарушитель», «пользователь», «система», «непредвиденные обстоятельства». Эксплуатируемые уязвимости: «отсутствие контрольно-пропускных механизмов», «отсутствие защиты трафика», «слабая парольная защита» и т.д. Угрозы: «НСД на территорию серверной комнаты», «заражение рабочей станции вирусом» и т.д. Результаты реализации угрозы: «копирование информации», «кража оборудования» и т.д. Целевые активы: «серверная комната», «локальная сеть компании», «рабочие станции». Пример того, как следует читать данную диаграмму: источник угрозы «нарушитель», эксплуатируя уязвимость «отсутствие контрольно-пропускных механизмов», совершает несанкционированный доступ на территорию серверной комнаты и получает доступ к оборудованию, находящемуся в ней; далее он совершает копирование/удаление/модификацию данных на серверах или кражу/порчу оборудования; актив, на который нацелена атака – серверная комната.

На рисунке 6.3 продемонстрирована диаграмма модели угроз с вероятностью возникновения инцидентов. Читать диаграмму следует также слева направо. Элементы диаграммы: источник угрозы, эксплуатируемые уязвимости, сами угрозы, инциденты, вероятность возникновения инцидента, целевые активы. До элемента «вероятность возникновения инцидента» элементы диаграммы совпадают с элементами, представленными на рисунке 6.2, и соответственно, читается она также. Вероятность возникновения инцидента (далее - вероятность) – это величина, которая берется из таблицы 6.1 и характеризуется как «высокая», «средняя» и «низкая». Именно она использовалась при расчете рисков, результаты которых занесены в таблицу 6.2. Пример того, как читается диаграмма: «нарушитель», используя уязвимость «отсутствие контрольно-пропускных механизмов», совершает несанкционированный доступ на территорию серверной комнаты и получает

доступ к оборудованию, находящемуся в ней; далее он совершает копирование (вероятность - высокая), либо удаление (вероятность - высокая), либо модификацию (вероятность - высокая) данных на серверах или кражу (вероятность - высокая), либо порчу (вероятность - высокая) оборудования; актив, на который нацелена атака – серверная комната.

На рисунке 6.4 продемонстрирована диаграмма модели угроз с характеристиками влияния угроз. Читать диаграмму следует слева направо. Элементы диаграммы: источник угрозы, эксплуатируемые уязвимости, сами угрозы, характеристиками влияния угроз, целевые активы. Характеристика влияния угрозы – это величина, которая берется из таблицы 6.1 и характеризуется как «высокая», «средняя» и «низкая». Она использовалась при расчете рисков, результаты которых занесены в таблицу 6.2. Пример того, как читается диаграмма: «нарушитель», используя уязвимость «отсутствие контрольно-пропускных механизмов», совершает несанкционированный доступ на территорию серверной комнаты и получает доступ к оборудованию, находящемуся в ней, влияние угрозы на бизнес-процессы компании характеризуется как «высокое»; целевой актив – серверная комната.

На рисунке 6.5 продемонстрирована диаграмма модели угроз с добавлением защитных мер. Элементы диаграммы: источник угрозы, защитная мера для уменьшения риска, эксплуатируемые уязвимости, сами угрозы, характеристиками влияния угроз, целевые активы. Данная схема во многом схожа с диаграммой, представленной на рисунке 6.2, за исключением добавления защитных мер, поэтому и читать ее следует почти так же. Защитные меры, представленные на диаграмме: «контроль физического доступа; ключ-карты; контрольно-пропускные механизмы; видеонаблюдение», «антивирус; инструктаж пользователей», «шифрование трафика; туннелирование; VPN», «автоматизация удаления учетных записей» и т.д. Пример: для уменьшения риска, связанного с уязвимостью «заражение рабочей станции вирусом» принято решение внедрить 6.2 защитные меры: антивирус и инструктаж пользователей.

На рисунке 6.6 продемонстрирована диаграмма недопустимых рисков. В данной диаграмме показаны только те риски, чье максимальное значение (результаты расчета показаны в таблице 6.2 составляет от 6 до 8. За исключением этого, данная диаграмма по структуре совей – диаграмма рисунка 6.4, поэтому ее следует читать так же.

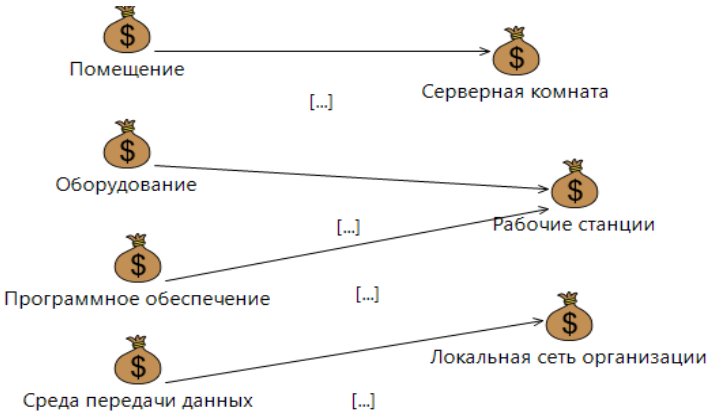

Рисунок 6.1 – Перечень активов

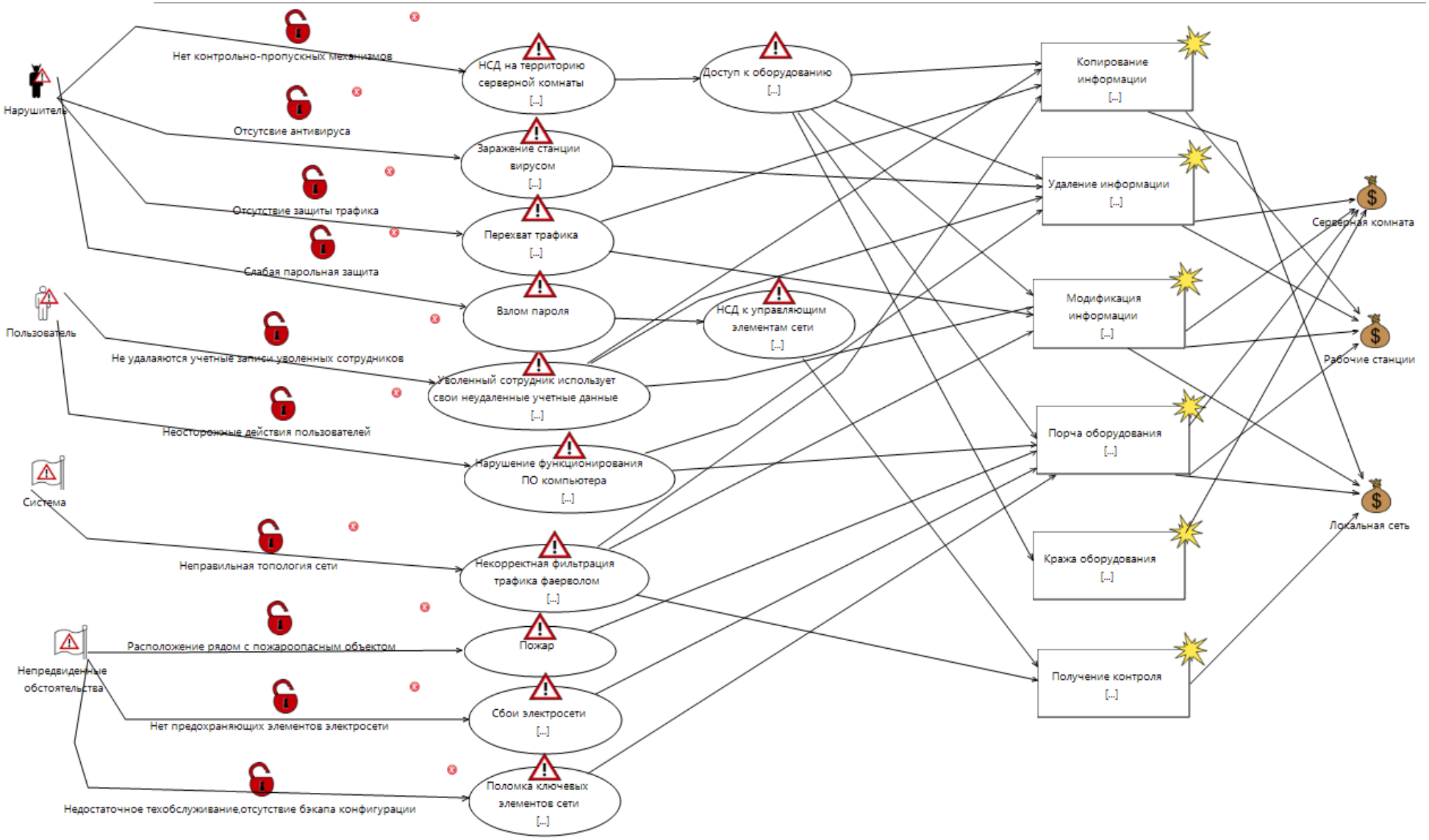

Рисунок 6.2 – Модель угроз

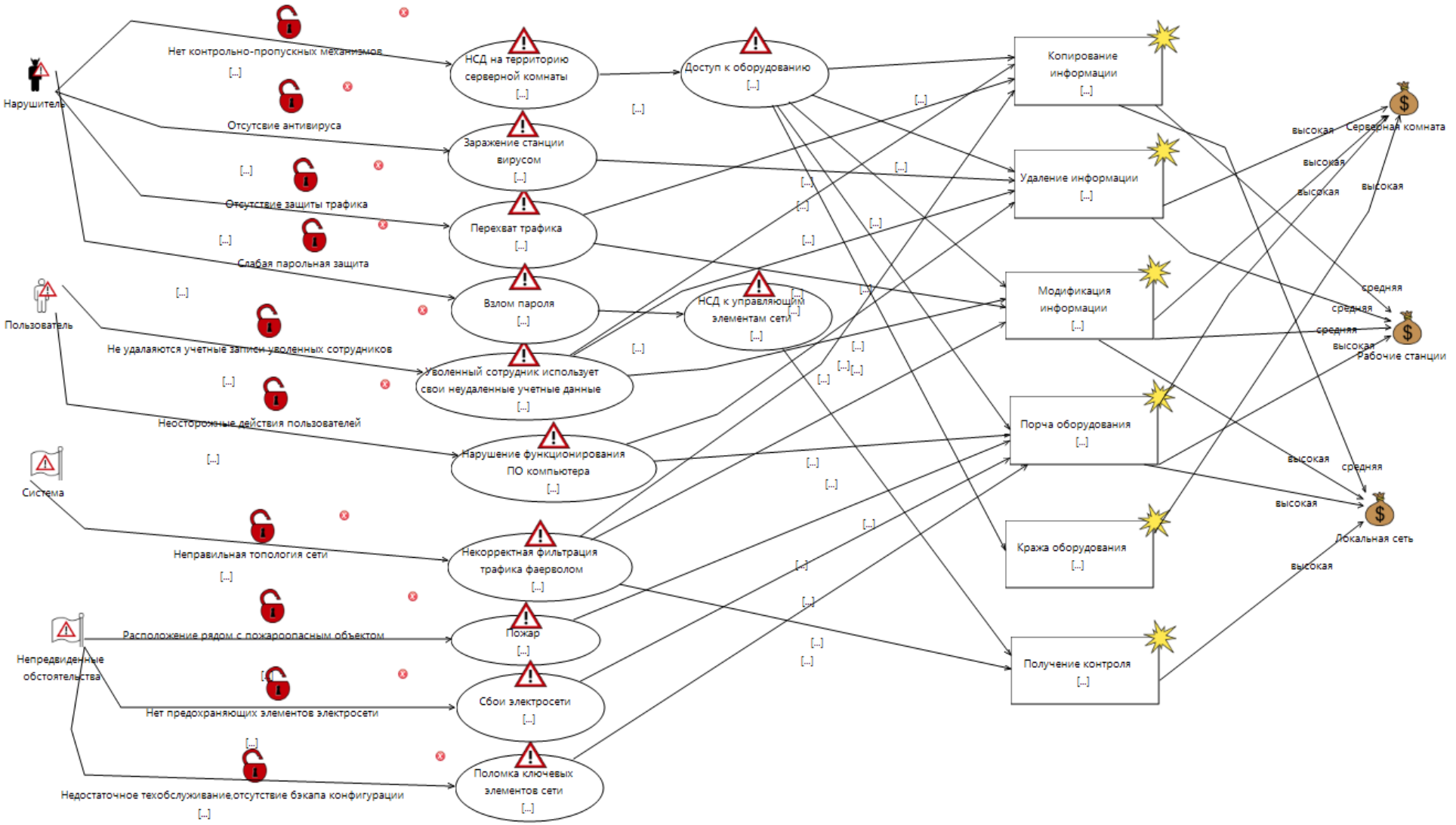

Рисунок 6.3 - Модель угроз с учетом вероятности возникновения инцидентов

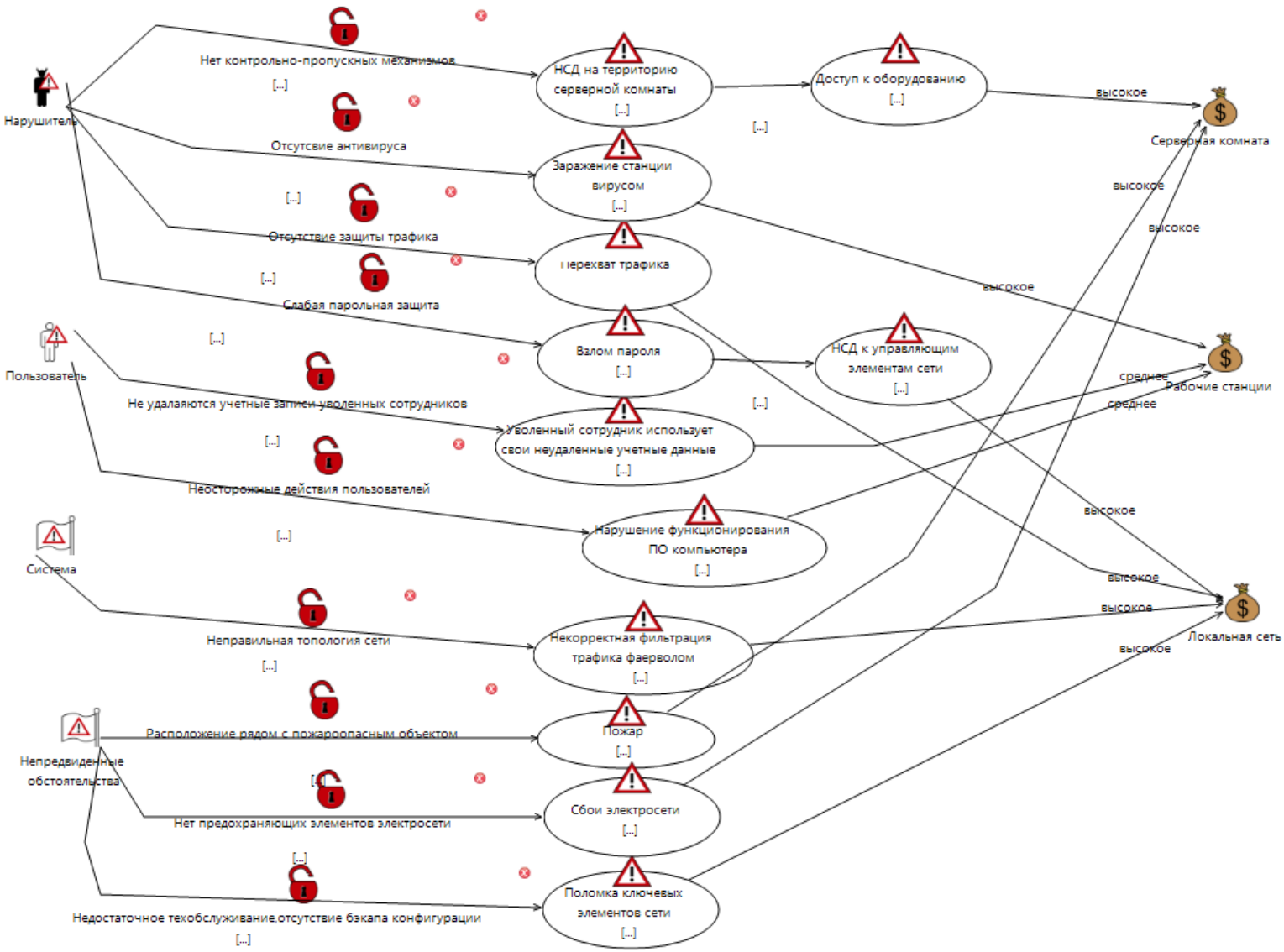

Рисунок 6.4 – Диаграмма рисков с характеристиками влияния угроз

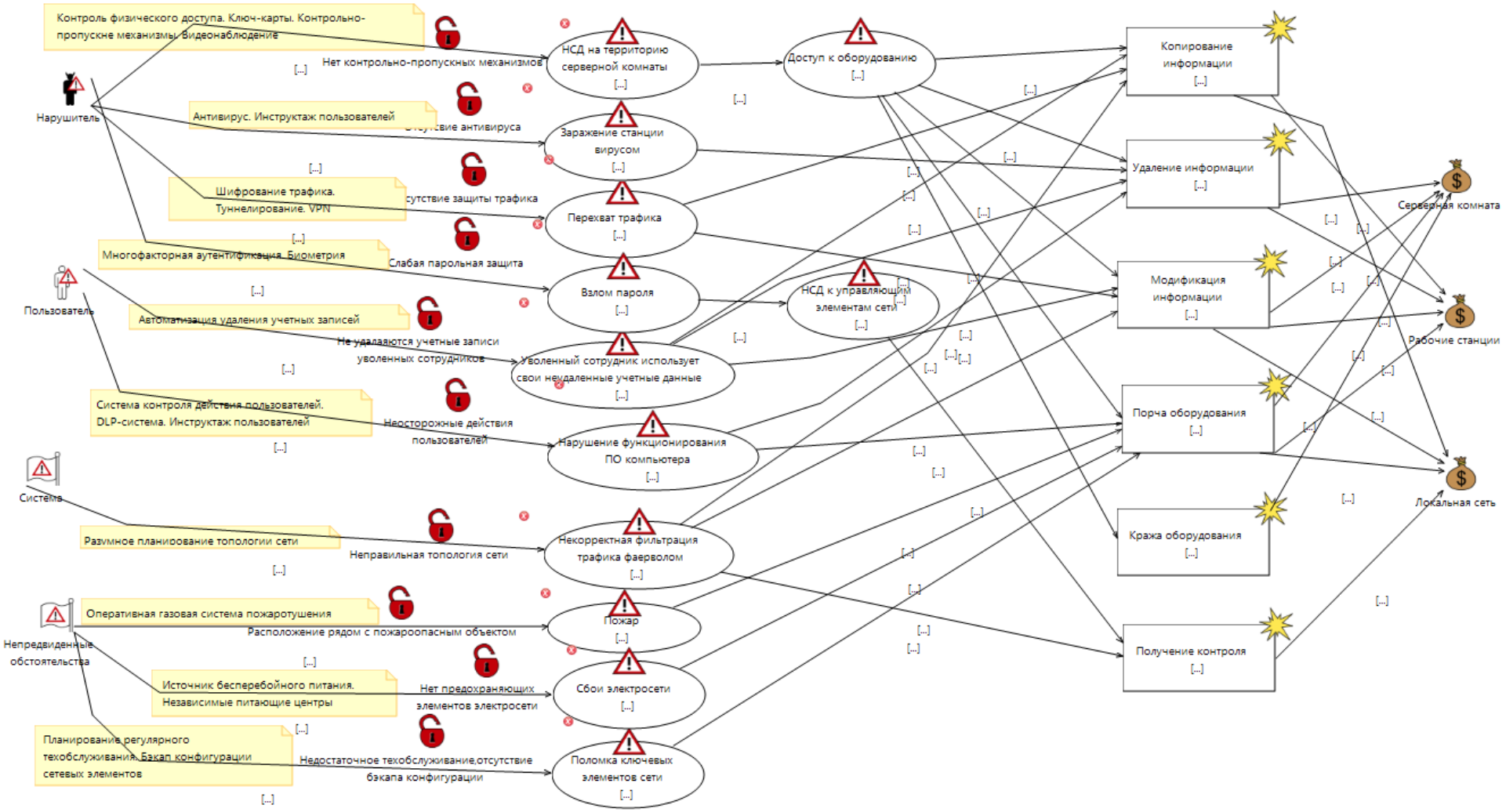

Рисунок 6.5 - Модель угроз с учетом защитных мер

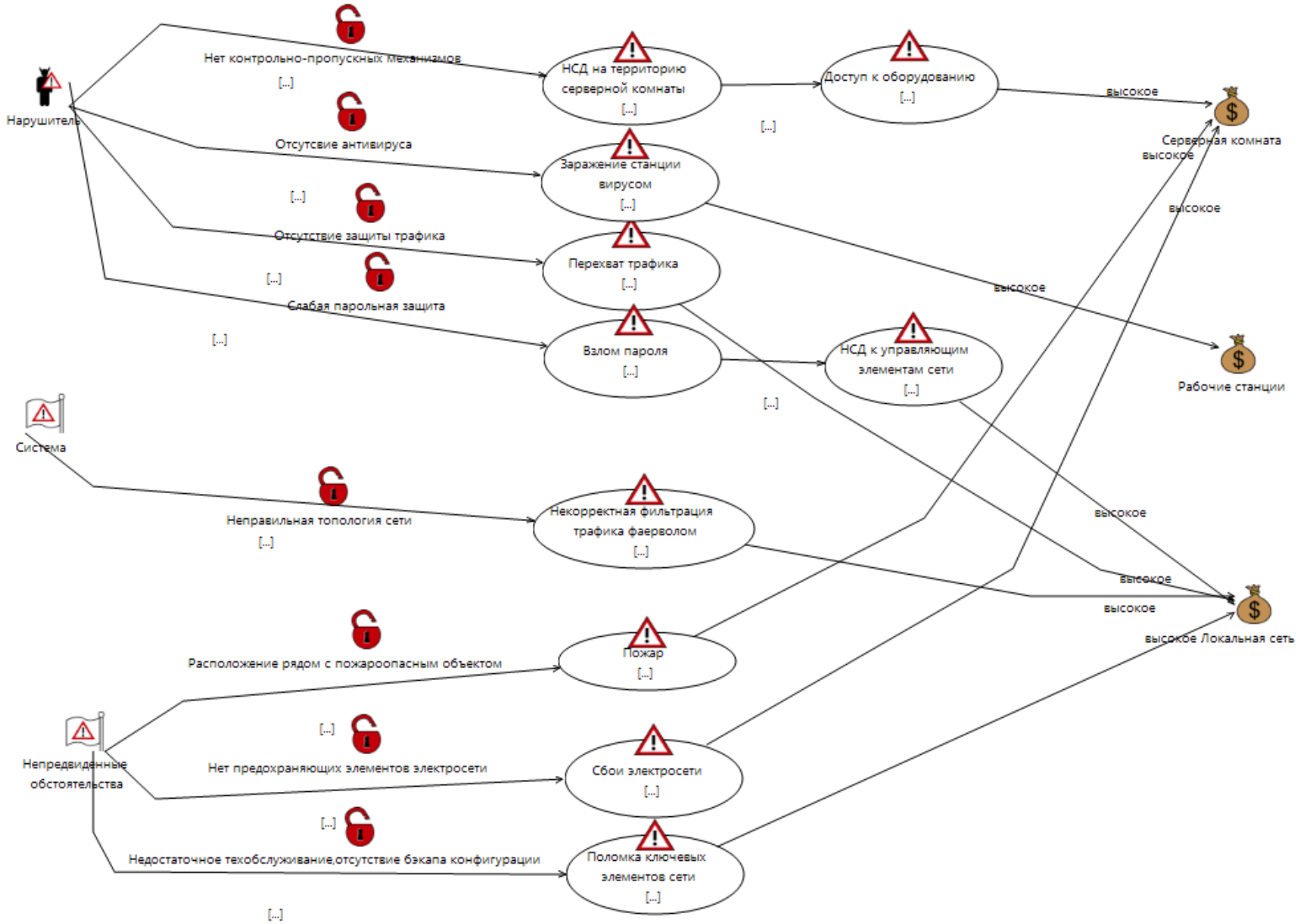

Рисунок 6.6 – Диаграмма недопустимых рисков

Вывод по разделу: задача, выполняемая в данном разделе, состояла в том, чтобы проанализировать различные рисковые ситуации (угрозы и уязвимости), ориентируясь именно на тему и специфику дипломного проекта. Так как тема посвящена организации системы информационной безопасности некого предприятия и является обширной, то были рассмотрены различные активы и разноплановые рисковые ситуации. Расчет данных рисков (по одному из алгоритмов стандарта ISO-27005) показал, что все рассматриваемые риски в численном эквиваленте составляют от пяти до восьми баллов (шкала – восемь баллов), то есть являются неприемлемыми. Это значит, что реализацию ни одного из анализируемых рисков организация не может себе позволить финансово компенсировать. С учетом этого, а также того, что после расчета остаточных рисков с учетом вышеуказанных мер обработки риски стали приемлемыми (их значение уменьшилось до 1-2 баллов), применение данных защитных мер является разумным и приемлемым.

Заключение

Внедрение системы обеспечения информационной безопасности (СИБ) будет намного эффективней, при наличии надёжной поддержки и при условии соблюдения правил политики информационной безопасности. Шаги построения политики и концепции безопасности – это внедрение в описание объекта автоматизации структуры ценности и непосредственное проведение анализа риска, а также определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим определённую степень ценности.

Организационные меры обеспечения защиты информации являются первоочередными, т.к. они призваны обеспечить эффективное функционирование остальных мер обеспечения конфиденциальности информации. С этой точки зрения организационные меры являются первичными по отношению к остальным мерам.

Все документы должны пройти согласование с юридической службой предприятия, утверждены руководством и введены в действие приказомпо предприятию. При этом необходимо также учитывать, что документы должны соответствовать законам и другим правовым документам РК в этой области, так как на работников накладываются определённые ограничения и ответственность, вплоть до уголовной, за нарушения правил работы с коммерческой тайной.

В организации предлагается внедрить комплексную систему антивирусной защиты на основе программного продукта Kasperskiy Internet Security, систему видеонаблюдения, помимо этого систему от вторжений в информационной среде организации.

По результатам анализа объекта защиты и обзора технических средств разработаны проект модернизации существующей системы видеонаблюдения. Модернизированная система обеспечивает надежную защиту объекта от несанкционированного проникновения и полностью отвечает требованиям банка в сфере видеонаблюдения.

При выборе технических средств особое внимание уделялось их функциональным характеристикам и технической совместимости устройств друг с другом. Разработанная система полностью отвечает требованиям технического задания и готова к внедрению на данном объекте.

Таким образом, в дипломной работе были предложены меры по защите информации, которые позволят избежать рисков и потерь. Затраты на реализацию мер составляют 887 255 тенге. Разработанная система принятия мер по обеспечению информационной безопасности оправдает себя уже через полгода.

Список литературы

1 Садердинов А.А. Информационная безопасность предприятия учебное пособие. —2-е изд. —М.: Дашков и К°, 2005. — 336 с.

2 Игнатьев В.А. Информационная безопасность современного коммерческого предприятия Монография. — Старый Оскол: ООО «ТНТ», 2005. — 448 с. ISBN 5-94178-070-2. 102 с.

3 Законы РК // digital.report.kz: Обзор законодательства Республики Казахстан в сфере информационной безопасности. URL: https://digital.report/zakonodatelstvo-kazahstana-v-sfere-informatsionnoi-bezopasnosti/, (дата обращения: 15.03.2020).

4 Закон о персональных данных // online.zakon.kz: Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». URL: https://online.zakon.kz/document/?doc_id=31396226, (дата обращения: 15.03.2020).

5 Закон об информатизации // online.zakon.kz: Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации». URL: https://online.zakon.kz/document/?doc_id=33885902, (дата обращения: 15.03.2020).

6 Требования и обеспечения ИБ // adilet.zan.kz: Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности. URL: http://adilet.zan.kz/rus/docs/P1600000832, (дата обращения: 15.03.2020).

7 Гришина Н.В. Организация комплексной системы защиты информации М.: Гелиос АРВ, 2007. — 256 с., ил. ISBN 978-5-85438-171-0.

8 Система ЗИ // twirpx.com: Проектирование системы защиты информации URL: https://www.twirpx.com/file/2561/, (дата обращения: 25.03.2020).

9 ИБ предприятия // kp.ru: Информационная безопасность предприятия: ключевые угрозы и средства защиты. URL: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html, (дата обращения: 17.04.2020).

10 Безопасность ИС предприятия // itdiplom.ru: Безопасность информационных систем предприятия – ВКР/НИР URL: https://itdiplom.ru/bezopasnost-informacionnyh-sistem, (дата обращения: 29.04.2020), (дата обращения: 17.04.2020).

11 Программа видеонаблюдения // jvsg.com: Проектирование видеонаблюдения в IP Video System Design Tool 10. URL: https://www.jvsg.com/проектирование-видеонаблюдения/, (дата обращения: 27.04.2020).

12 SpiceWorks // habr.com: Spiceworks. Часть 1: Инвентаризация в сети. URL: https://habr.com/ru/post/192280/, (дата обращения: 03.05.2020).

13 SpiceWorks // tadviser.ru: Spiceworks – система мониторинга систем. URL: http://www.tadviser.ru/index.php/продукт:SpiceWorks, (дата обращения: 04.05.2020).

14 Антивирусные программы // ru.safetydetectives.com: Современные антивирусные программы и их эффективность. URL: https://ru.safetydetectives.com/, (дата обращения: 08.05.2020).

15 DeviceLock DLP // anti-malware.ru: DeviceLock DLP Suite 8. Часть 1: функциональные возможности. URL: https://www.anti-malware.ru/reviews/DeviceLock_DLP_Suite_8_part_1, (дата обращения: 12.05.2020).

16 Рекомендации по ИБ // https://habr.com/ru: Рекомендации по информационной безопасности для малого и среднего бизнеса (SMB). URL: https://habr.com/ru/post/348892/, (дата обращения: 16.05.2020).

17 Охрана труда // Protrud.com: Опасные и вредные производственные факторы. URL: https://www.protrud.com/ опасные-и-вредные-производственные-факторы/ (дата обращения 05.06.2020)

18 Проведение специальной оценки условий труда // Asout.ru: Классификация опасных и вредных производственных факторов. URL: https://asout.ru/klassifikatsiya-opasnyih-i-vrednyih-proizvodstvennyih-faktorov (дата обращения 05.06.2020).

19 Учебные материалы // Works.doklad.ru: Опасные и вредные производственные факторы. URL: https://works.doklad.ru/view/xFydZ1T5NZ4.html (дата обращения: 05.06.2020).

Приложение А

Сравнительный анализ антивирусного ПО

Таблица А.1 – Сравнительный анализ антивирусного ПО

Характеристика	Kaspersky	ESET	McAfee	Symantec
1.Контроль программ и белые списки				
Поддержка сценария «запрет по умолчанию» с возможностью автоматического исключения из сценария необходимых для работы системы процессов и доверенных источников обновлений	+	-	+	-
Разрешение / блокировка программ:				
Выбор из реестра программ	+	-	-	-
Выбор из реестра исполняемых файлов	+	-	-	-
Ввод метаданных исполняемых файлов	+	-	+	-
Ввод контрольных сумм исполняемых файлов (MD5, SHA1)	+	-	+	+
Ввод пути к исполняемым файлам (локального или UNC)	+	-	+	+
Выбор предустановленных категорий приложений	+	-	-	-
Разрешение блокирование приложений для отдельных пользователей групп пользователей Active Directory	+	-	+	-
Мониторинг и ограничение активности программ	+	-	+	+
Мониторинг и приоритезация уязвимостей	+	+	+	-
2. Веб-контроль				
Разрешение/блокирование				
Фильтрация ссылок	+	+	+	+
Фильтрация содержимого по предустановленным правилам	+	-	+	-
Фильтрация содержимого по типу данных	+	-	-	-
Интеграция с Active Directory	+	-	+	-
Разрешение/блокирование доступа к веб-ресурсам по расписанию	+	-	+	+
Формирование подробных отчетов об использовании ПК для доступа к веб-ресурсам	+	-	+	-