|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **logoМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **Кафедра информационной безопасности** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | |
| о прохождении учебной практики (учебно-лабораторного практикума)  на тему: «Защита бизнес-данных предприятия» | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнили студенты  гр. С8117-10.05.01ммзи  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ К.В. Клишин  (подпись) | | | | | | | | |
|  |  |  | | | | | | Д.С. Левчук | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | |  | |
|  | | | | | | | | | |  |  | Заведующий лабораторией кафедры информационной безопасности ДВФУ | | | | | | | | |
|  | | | |  | С.С. Зотов | | | | |  |  |  | | | | |  | С.С. Зотов | | |
| (подпись) | | | |  | (И.О. Фамилия) | | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | |
| « | 22 | » | февраля | | | | | | 2021 г. |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  | с | « | 22 | » | февраля | | | | 2020 г. |
|  | | | | | | | | | |  |  | по | « | 26 | » | июня | | | | 2021 г. |
|  | | | | | |  | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | |
| (подпись) | | | | | |  | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | ФГАОУ ВО «Дальневосточный | | | | | | | | |
|  | | | | | | | | | |  |  | Федеральный Университет» | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | |
| 2021 г. | | | | | | | | | | | | | | | | | | | | |

Оглавление

[Введение 2](#_Toc75158386)

[1. Теоретические основы 2](#_Toc75158387)

[1.1 Рассмотрение нормативной базы в области построения комплексной системы защиты информации 2](#_Toc75158388)

[1.2 Информация, подлежащая защите, определение источников информации 2](#_Toc75158389)

[2. Анализ защиты информационных ресурсов организации ИП Корчев Василий Васильевич 2](#_Toc75158390)

[2.1 Организационная структура организации ИП Корчев Василий Васильевич 2](#_Toc75158391)

[2.2 Анализ информационных потоков 2](#_Toc75158392)

[2.3 Анализ информационных ресурсов 2](#_Toc75158393)

[2.4 Анализ защищаемого помещения и каналов утечки 2](#_Toc75158394)

[2.5 Модель угроз нарушителя 2](#_Toc75158395)

[2.6 Анализ программно-технически средств, используемых в организации «ИП Корчев Василий Васильевич» 2](#_Toc75158396)

[Заключение 2](#_Toc75158397)

[Список используемых источников 2](#_Toc75158398)

[ПРИЛОЖЕНИЕ 1 2](#_Toc75158399)

# Введение

Прохождение учебно-лабораторного практикума имеет большое значение в процессе подготовки будущих специалистов. Необходимость ее для студента заключается в том, что это отличная возможность объединить знания, полученные в процессе обучения, с практическими навыками, полученными на предприятии, и хорошая возможность получить первоначальный опыт, так необходимый начинающему специалисту при трудоустройстве.

Из этого можем сделать вывод, что главная цель практики заключается в закреплении и углублении практических знаний, полученных при изучении специальных дисциплин, приобретении практических навыков и умений.

Объектом прохождения учебно-лабораторного практикума является система защиты информации организации «Индивидуальный предприниматель Корчев Василий Васильевич», которая была создана в 2009 году. Компания работает в сфере фитнеса. Управляющий офис Компании находится во Владивостоке. Филиалы Компании открыты аналогично в пределах Владивостока.

Предприятие «Индивидуальный предприниматель Корчев Василий Васильевич» охватывает всю территорию Владивостока - от Второй Речки до Тихой. Компания постоянно расширяет свою географию. В Компании «ИП Корчев В.В.» работают только профессиональные сотрудники. Компания «ИП Корчев В.В.» регулярно расширяет область присутствия, открывая новые филиалы.

Основные предоставляемые услуги ИП Корчев В.В. являются:

* предоставление услуг в сфере фитнеса;
* предоставление услуг солярия;
* предоставление услуг фитнес-бара;
* предоставление непосредственных спортивных услуг;
* предоставление услуг спортивного ведения подготовки к соревнованиям профессиональных спортсменов и любителей;
* предоставление консультаций в сферах нутрициологии и диетологии.

Целью прохождения практики является исследование процессов защиты информации в ИП Корчев В.В. и предложение путей улучшения способов её защиты.

В соответствии с целью были выявлены основные задачи:

* рассмотрение нормативно-методической базы в области построения КСЗИ;
* исследование организационной структуры предприятия, выявление видов конфиденциальной информации и ресурсов, подлежащие защите;
* анализ системы обработки данных, классификация активов, подлежащих защите;
* обоснование актуальных угроз и определение нарушителей информационных процессов в информационной системе организации;
* исследование способов защиты информационных ресурсов;
* анализ каналов утечки информации;
* формулировка выводов о состоянии КСЗИ в организации.

# Теоретические основы

## 1.1 Рассмотрение нормативной базы в области построения комплексной системы защиты информации

При прохождении практики и для написания данной отчётности была отобрана нормативная база, состоящая из следующих документов:

* Устав организации ИП Корчев Василий Васильевич;
* Правила внутреннего распорядка и работы организации ИП Корчев Василий Васильевич;
* ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России;
* ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Госстандарт России;
* ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России;
* ГОСТ Р 51624–2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;
* ГОСТ Р 52069–2003. Защита информации. Система стандартов. Основные положения;
* ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью;
* ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности;
* ГОСТ Р ИСО/МЭК ТО 19791–2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем;
* ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;
* Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Постановление Правительства Российской Федерации от 15.09. 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Проектирование защищенных информационных систем процесс довольно сложный, который предполагает наличие соответствующих знаний и опыта, у ее создателей.

Потребитель может не вникать в разработку такого проекта и подробности его развития, однако он обязан контролировать каждый его этап на предмет соответствия техническому заданию и требованиям нормативных документов. В свою очередь, персональный опыт проектировщиков требует использования существующих нормативных документов в данной области для получения наиболее качественного результата.

Таким образом, процесс проектирования защищенных информационных систем должен основываться на знании и строгом выполнении требований существующих нормативных документов, как со стороны ее разработчиков, так и со стороны заказчиков. В организации ИП Корчев Василий Васильевич соблюдены не все требования из представленной нормативной базы, но общее состояние защиты информации на предприятии можно охарактеризовать оценкой «хорошо».

## 1.2 Информация, подлежащая защите, определение источников информации

Защита информации - это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Существует 4 уровня защиты информации:

* предотвращение - только авторизованный персонал имеет доступ к информации и технологии;
* обнаружение - обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены;
* ограничение - уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению;
* восстановление - обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Существует два источника информации, на которых базируется оценка компании: внутренний и внешний. Под внутренними источниками понимаются официальные каналы распространения информации в фирме, предоставление информации руководству компаний, ее структурных подразделений, филиалов и представительств. Под внешними - любая другая информация, полученная из внешней среды организации: СМИ, партнеров, конкурентов, клиентов, властей и т.п. (информирование акционеров, а также государственных финансовых органов, налоговых инспекций, кредитных организаций, страховых компаний, государственных органов статистики, инвестиционных фондов, органов государственной власти и управления, органов местного самоуправления, предприятий-поставщиков).

Анализируя источники информации на предприятии, можно выделить следующие:

* документы;
* представительство на ярмарках, салонах, конференциях;
* производимая продукция или оказываемые услуги;
* технические средства обеспечения производственной деятельности;
* косвенные источники (мусор, реклама, публикации в печати);
* информация на технических носителях.

Источники конфиденциальной информации дают полные сведения о составе, содержании и направлении деятельности предприятия (организации). Поэтому грамотная система защиты, разработанная с учетом всех особенностей, позволит предотвратить многие проблемы.

Всю информацию, движущуюся в организации ИП Корчев Василий Васильевич, можно разделить на три вида:

* конфиденциальная информация, с ограничением допуска посторонних лиц (вопросы, касающиеся внутреннего распорядка, устав);
* персональные данные (база данных клиентов и сотрудников);
* открытая информация, не подлежащая защите, утечка которой не нанесет вреда организации.

# Анализ защиты информационных ресурсов организации ИП Корчев Василий Васильевич

## 2.1 Организационная структура организации ИП Корчев Василий Васильевич

Генеральный директор предприятия управляет шестью основными департаментами (ПРИЛОЖЕНИЕ 1):

1. Департамент построения;
2. Департамент распространения;
3. Департамент финансов;
4. Технический департамент:
5. Секция обеспечения и сервиса;
6. Секция предоставления фитнеса;
7. Департамент связи с общественностью;
8. Административный департамент.

Департамент построения компании ИП Корчев Василий Васильевич является самостоятельным структурным подразделением предприятия и подчиняется административному директору. Отдел обеспечивает компанию персоналом, поддержанием грамотной внутренней коммуникации и своевременным информированием сотрудников обо всех изменениях и обновлениях внутри компании. Задачи первого департамента:

* разработка должностных инструкций и обучающих материалов компании;
* найм сотрудников и введение их в должность;
* ведение кадрового учета;
* организация рабочих мест;
* санкции и поощрение сотрудников;
* поддержание стандартов компании и требования их выполнения.

Департамент распространения отвечает за продвижение, выработку рекомендаций по формированию и проведению производственно-сбытовой политики предприятия, а также координацию деятельности в этой области всех подразделений предприятия. Второй департамент не подменяет другие подразделения, а ориентирует деятельность других подразделений на рынок и коррелирует их работу с общими для всего предприятия целями рыночной деятельности Отдел подчиняется непосредственно административному директору предприятия. Департамент распространения занимается:

* созданием и ведением маркетинговых кампаний;
* продвижением компании на рынке;
* продвижением SEO и SMM;
* анализом конкурентной среды;
* созданием OFF-LINE рекламы;
* ведением аналитики компании;
* описанием услуг компании;
* взаимодействием с СМИ;
* взаимодействием с корпоративными клиентами;
* продажей продуктов компании (в том числе и онлайн);
* ведением актуальной базы данных.

Департамент финансов обеспечивает компетентное и эффективное управление финансами и их контролем для достижения целей компании. Третий департамент:

* занимается решением широкого ряда организационных и финансовых вопросов;
* разрабатывает в установленные сроки проекты финансовых планов предприятия со всеми необходимыми расчетами;
* определяет потребности собственных оборотных средств по элементам и расчет нормативов оборотных средств;
* распределяет квартальные финансовые показатели по месяцам.

Технический департамент возглавляет технический директор. В своей деятельности технический отдел руководствуется уставом предприятия и положением. Данный департамент подразделяется на две секции: секция обеспечения и сервиса и секция предоставления фитнеса.

Задачи первой секции:

* планирование амортизации оборудования и своевременная его амортизация;
* ведение технологической документации;
* ведение пожарной безопасности;
* обеспечение комфорта клиентов;
* обеспечение поставок товаров (снабжения);
* клининг предприятия;
* обеспечение работоспособности IT-сервиса (в том числе и защиты данных);
* IT-обслуживание компании.

Задачи второй секции:

* планирование расписания;
* техническое обеспечение фитнес-производства;
* планирование доп. услуг;
* непосредственное оказание фитнес-услуг;
* планирование и ведение ON-LINE тренировок.

Департамент связей с общественностью подчиняется непосредственно директору по развитию. Задачи департамента заключаются в следующем:

* ведение работы с представителями других компаний;
* ведение внутренней связи с общественностью;
* контроль персонала по выполнению должностных инструкций;
* организация мероприятий;
* продвижение пробников;
* ведение семинаров и интервью.

Шестой департамент (административный) – главный среди всех вышеперечисленных. Кратко говоря, здесь обеспечивается контроль и управление всеми вышеперечисленными отделами.

## 2.2 Анализ информационных потоков

Рассмотрим внутренние информационные потоки. В административный отдел поступают приказы и распоряжения от генерального директора компании. Ответом на приказы директора, из административного отдела предоставляется отчетная документация по решенным вопросам и отчетная документация по исполненным обращениям клиентов. Из бухгалтерии предоставляются сметы по расходам компании, данным по фонду оплаты труда на заверение директору организации «ИП Корчев Василий Васильевич». Бухгалтерия получает приказы и распоряжения от руководителя организации. Осуществляемое взаимодействие между клиентами компании и техническим департаментом и департаментом распространения включает непосредственное предоставление фитнес-услуг и их приобретение.

Рассмотрим внешние информационные потоки организации «ИП Корчев Василий Васильевич». Внешнее взаимодействие компании намного обширнее. Департамент распространения занимается рекламированием компании и увеличением числа постоянных клиентов. Компания продает услуги фитнеса, а также предоставляет отчетность по продажам и осваемости денежного потока. Так же департамент распространения вместе с департаментом связи с общественностью предоставляет отчётную документацию своим партнёрам. Департамент финансов, в свою очередь, осуществляет выдачу и получение денежных средств департаменту распространения, техническому департаменту для закупки оборудования, арендодателю, финансовым и деловым партнёрам.

## 2.3 Анализ информационных ресурсов

Информационные ресурсы — это совокупность данных, организованных для получения достоверной информации; документы и массивы документов, отдельные и в информационных системах. Информационные ресурсы предприятия представлены в документах массивов информации на машинных носителях, архивах, фондах, библиотеках. Информационные ресурсы, частью которых является и информационные технологии, имеют в данном определении четкую структуру в соответствии с методикой их создания, оценки и инвентаризации. Более подробный анализ информационных ресурсов в организации «ИП Корчев Василий Васильевич» представлен в таблице 1.



## 2.4 Анализ защищаемого помещения и каналов утечки

Организация «ИП Корчев В.В.» имеет три филиала. Мы же будем рассматривать основной филиал по адресу г. Владивосток, ул. Карла Жигура 26. Организация расположена на цокольном этаже 15-этажного здания. Вблизи сооружения находятся и другие постройки, такие как продовольственный магазин, жилой многоэтажный дом, сельскохозяйственные корпуса. Почти весь цокольный этаж сооружения занят организацией «ИП Корчев В.В.». Двери кабинетов открываются наружу (в холл). Всего на этаже расположены 15 камер видеонаблюдения, физического контроля компания не имеет, камеры пишут на регистратор с защищённым жёстким диском объёмом 2 Тбайта. Дверь от лестницы в прихожую постоянно открыта в рабочее время.

Персональные компьютеры расположены в каждом кабинете, все они имеют выход в Интернет и объединены локальной сетью. Принтеры установлены в кабинете генерального директора, в кабинете департамента распространения, финансовом отделе и техническом отделах.

Существуют следующие виды утечки информации:

1. Радиоизлучение монитора. Перехват изображения монитора достаточно распространенный способ хищения информации. Это становится возможным в связи с его паразитным излучением, прием которого возможен до 50 м. В организации «ИП Корчев Василий Васильевич» нет необходимой защиты от данной угрозы.
2. Микрофонный эффект, закладки в телефонном аппарате. Акустические колебания микрофона или обмоток звонка возникают при положенной трубке и могут быть сняты с телефонного кабеля, например, на АТС. Также нет защиты;
3. Видеонаблюдение. Это возможно как через окно, так и с помощью вмонтированных камер в предметы помещения, либо в вещи постороннего человека, попавшего в закрытое помещение. На окне помещения имеются поворотные жалюзи, защищающие от съема видовой информации через окно. Посторонние лица имеют возможность разглядеть информацию на мониторе;
4. Вибрация стен, перекрытий, систем отопления, вентиляции, дверей. Такое удаленное действие возможно с помощью лазера. В помещении стоят двойные стеклопакеты, следовательно эта угроза нейтрализована;
5. Анализ передаваемых данных (электромагнитное излучение, использование атак по сети, паразитное радиоизлучение, вирусы);
6. Прослушивание телефонного и факс-модемного трафика. Организация «ИП Корчев Василий Васильевич» не имеет факсимильного аппарата, таким образом, исключён перехват трафика;
7. Жучки, направленные микрофоны;
8. Доступ посторонних лиц;
9. Человеческий фактор.

## 2.5 Модель угроз нарушителя

Модель угроз нарушителя представляет собой его комплексную характеристику, отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения.

В рассматриваемом случае учитываются только угрозы объекту, включающие несанкционированное проникновение. Но следует иметь в виду, что конечная цель проникновения может быть различной, она зависит от категории объекта, облика возможного нарушителя и может варьироваться от простой кражи до террористического акта. В таблице 2 рассмотрена модель угроз нарушителя для организации «ИП Корчев Василий Васильевич».





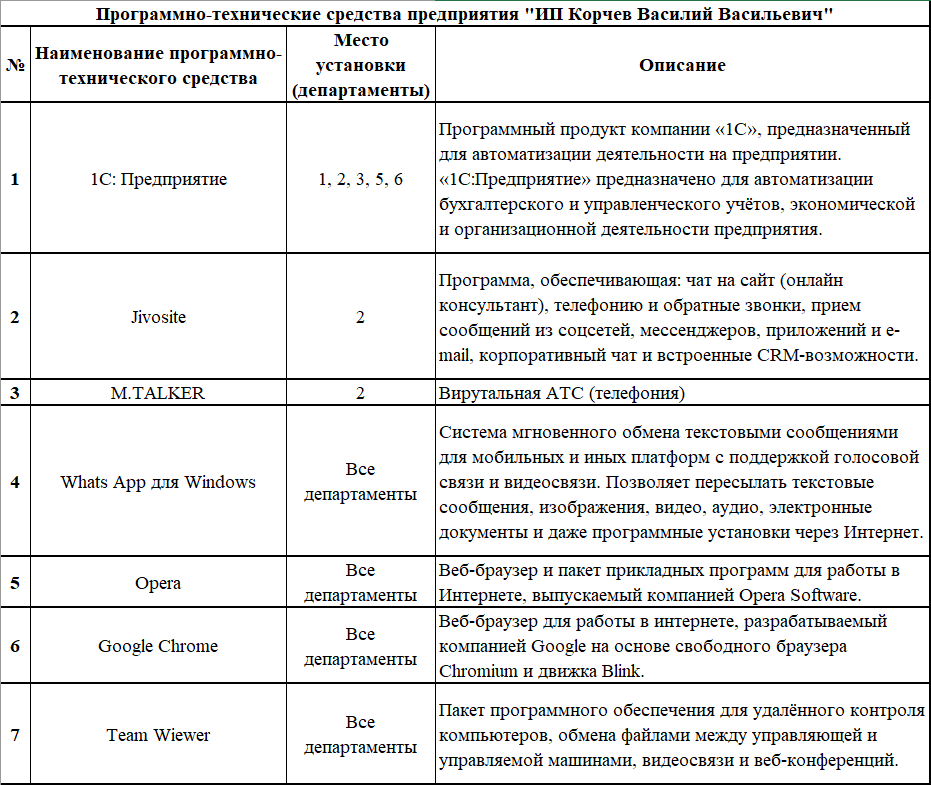
## 2.6 Анализ программно-технически средств, используемых в организации «ИП Корчев Василий Васильевич»

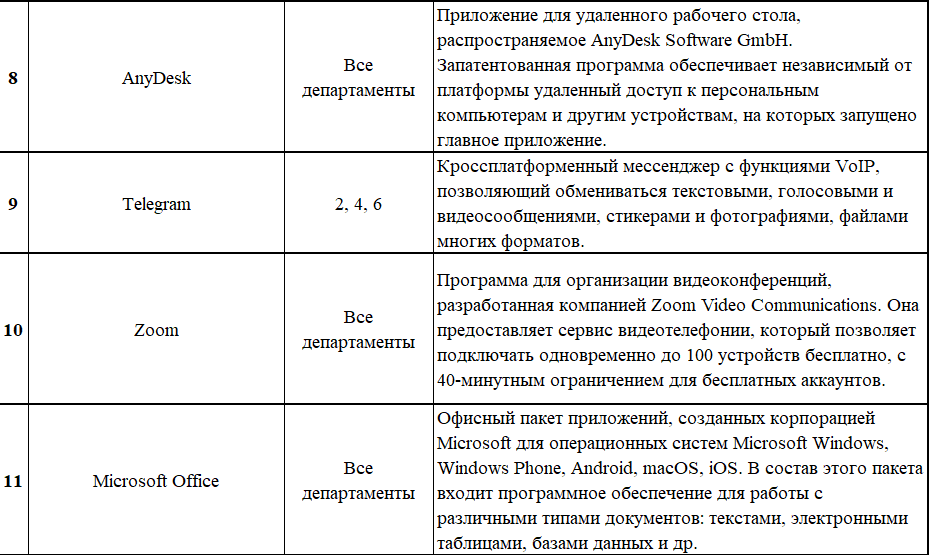
С помощью программно-технических средств можно в определенной мере решать как основные задачи защиты в вычислительных системах (от хищения, от потери, от сбоев и отказов оборудования), так и защиту от ошибок в программах.

Решение этих задач в системах защиты обеспечивается следующими способами:

* защитой от несанкционированного доступа к ресурсам со стороны пользователей и программ;
* защитой от несанкционированного использования ресурсов при наличии доступа;
* защитой от некорректного использования ресурсов;
* внесением структурной, функциональной и информационной избыточности;
* высоким качеством разработки программно-аппаратных средств.

Рассмотрим программно-технические средства, используемые на предприятии «ИП Корчев Василий Васильевич»:





Конечно же, нас интересуют не все программные средства, используемые на предприятии. Из вышесказанных мы рассмотрим следующие:

1. 1С: Предприятие (т.к. основная техническая работа организации ведется в ней);
2. ViPNet;
3. USB Flash Security;
4. Folder Lock;
5. Kaspersky Endpoint Security.

О данных ПО важно сказать, каким образом они обеспечивают информационную безопасность предприятия и какую роль они играют в системе информационной безопасности организации.

В «1С: Предприятие» защита информации строится на принципе, когда пользователей не имеет прямого доступа к базам данных – он их получает при помощи запросов процесса rphost от имени своей учетной записи. Но одного этого принципа мало – в большинстве случае без индивидуальной настройки не обойтись.

Для начала каждый пользователей базы получает логин и пароль. При загрузке программы он их указывает, если в системе существует учетная запись с соответствующими параметрами, доступ разрешается. Учетная запись создается для каждой информационной базы, используемой пользователем. Передаваемая информация шифруется полностью или частично при помощи сертификатов.

Обобщая, пользователь, проходя аутентификацию, получает доступ к базе данных. Соответственно, пользователи не имеющих учетных записей в системе доступ к ней получить не могут.

USB Flash Security. Данная программа включает в себя набор самых необходимых функций. Здесь можно полностью блокировать доступ к съемному носителю, чтобы полностью предотвратить попадание вирусов на компьютер. В последней версии USB Disk Security существует возможность проверять на вирусы определенные сайты. Эта функция очень полезна, ведь на пространстве интернета содержится бесконечное множество вирусных и шпионских программ, которые способны нанести вред не только электронному устройству, но и секретной информации. Чтобы полностью обеспечить защиту системы, необходимо вместе с антивирусом устанавливать USB Disk Security.

Folder Lock — это относительно недорогая программа шифрования, которая предлагает множество хороших и полезных функций. Есть несколько способов резервного копирования данных. В дополнение к классическому шифрованию программа также позволяет вам защитить данные с помощью простого пароля, которого должно хватить для большинства пользователей в повседневной жизни и который намного проще и быстрее, чем шифрование. Как следует из названия, Folder Lock даже специализируется не на шифровании файлов, а только на их защите в папках, защищенных паролем. Folder Lock также предлагает возможность безопасного и безвозвратного удаления данных. 256-битный алгоритм шифрования AES считается безопасным и не должен вызывать никаких проблем.

VipNet Client — многофункциональный программный комплекс для защиты локальных и удалённых рабочих мест сотрудников, сертифицированный ФСБ России. Решение разработано отечественной компанией «ИнфоТеКС» на базе технологии ViPNet. На сегодняшний день это одна из самых масштабируемых технологий построения защищённых сетей на отечественном рынке. Программный комплекс «ВипНет Клиент» выпускается в модификациях для трёх операционных систем: Microsoft Windows, Linux и OS X. Версия ViPNet Client 4 for Linux включена в Единый реестр российского программного обеспечения и полностью соответствует требованиям государственной программы импортозамещения.

«ВипНет Клиент» обеспечивает защиту корпоративных рабочих станций от внешних и внутрисетевых угроз путём фильтрации трафика. В дополнение к этому программный комплекс обеспечивает безопасную работу удалённых сотрудников в корпоративных системах и сервисах. Защищённый мобильный и веб-доступ к ресурсам компании организуется с помощью зашифрованного канала связи. Возможностей обычной виртуальной частной сети (VPN) в подобных ситуациях недостаточно, поскольку в технологии VPN не предусмотрены функции обнаружения и блокировки атак. ViPNet же отлично справляется с задачей обеспечения информационной безопасности при обмене данными между географически распределёнными сетями.

Сертификат соответствия требованиям Федеральной службы безопасности России подтверждает, что «ВипНет Клиент» может использоваться для криптографической защиты конфиденциальной информации, за исключением данных, составляющих гостайну. Приведённый в сертификате обзор возможностей ViPNet Client включает:

* создание и управление ключевой информацией;
* шифрование файлов и данных в оперативной памяти;
* шифрование IP-трафика;
* вычисление значения хэш-функции для файлов и данных в оперативной памяти;
* защиту TLS-соединений;
* реализацию функционала электронной подписи в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

Программный комплекс может использоваться в различных назначениях.

1. В качестве VPN-клиента с функциями шифрования трафика и имитозащиты IP-пакетов. Решение обеспечивает безопасность конфиденциальных данных, обмен которыми осуществляется через каналы связи общего пользования внутри корпоративной VPN-сети.
2. В роли персонального сетевого экрана (данный сценарий применения актуален только для версий ПК для Windows и Linux). Путём фильтрации трафика программный комплекс надёжно защищает компьютеры локальной сети от всех типов внешних угроз.
3. Как инструмент контроля сетевой активности приложений и компонентов ОС (данный сценарий применения актуален исключительно для версии ПК для Windows). ViPNet Client снимет со штатного специалиста по информационной безопасности значительную часть рутинной нагрузки, позволит всегда быть в курсе текущих сетевых активностей и оперативно реагировать на выявленные аномальные процессы.
4. Для защиты сети от внутренних угроз. Соединение пользователей между собой, связь с корпоративными системами и сервисами осуществляется через защищённые каналы по схеме «точка – точка». Такой подход позволяет оградить информацию от постороннего доступа внутри локальной сети компании.
5. Для защиты коммуникации пользователей. «ВипНет Клиент» легко интегрируется со всеми решениями линейки ViPNet Network Security. Его совместное использование с приложениями «ВипНет Коннект» и «ВипНет Деловая почта» позволяет создать всестороннюю и надёжную защиту для общения пользователей. Предусмотрена возможность интеграции программного комплекса с корпоративными системами IP-телефонии и видеоконференцсвязи.
6. Для защиты виртуальных машин. «ВипНет Клиент» подходит для запуска на виртуальных серверах. Предусмотрена возможность использования средств защиты ViPNet в VDI-средах.
7. Для организации повсеместного стабильного доступа. Программный комплекс обеспечивает одинаково качественный доступ к корпоративным системам и сервисам с мобильных и десктопных устройств, независимо от местоположения пользователей (при использовании решения ViPNet Network Security).

Завершая обзор ViPNet Client, следует отметить, что использование данного средства защиты информации не влияет на работу сторонних приложений на ПК пользователей.

Kaspersky Endpoint Security

Он отслеживает и анализирует различные виды активности с помощью статического набора эвристик — моделей или шаблонов подозрительной активности приложений. Как и сигнатуры, такие шаблоны регулярно обновляются: эта технология позволяет при обнаружении нового вируса или новой модификации уже известного вредоносного ПО обновлять не весь модуль проактивной защиты, а добавлять новую сигнатуру в базу эвристик и обновлять ее вместе с антивирусными базами продукта. Таким образом, какая-либо новая вредоносная программа может «внешне» значительно отличаться от уже известных, но, если она ведёт себя так же, антивирусные модули наших решений её заблокируют.

За проактивную защиту в Kaspersky Internet Security для Windows отвечает компонент System Watcher. В его состав ходит набор шаблонов (Behavior Stream Signatures, BSS) — моделей вредоносного поведения, по которым можно вычислить неизвестное вредоносное программное обеспечение ещё до того, как информация о нём заносится в базы сигнатур. System Watcher обменивается информацией с другими компонентами антивирусного ПО и, запоминая цепочки событий, формирует целостную картину поведения и регистрирует следы каждой отдельной программы и групп программ. Это значительно повышает точность обнаружения вредоносного ПО. Стоит также иметь в виду, что System Watcher отслеживает действия программ не только в текущей сессии, а на протяжении всего жизненного цикла программы.

Для дополнительного ускорения работы компонентов антивирусной защиты Kaspersky Endpoint Security для Windows с файлами на компьютере ещё в восьмой версии были реализованы две функции под названием iSwift и iChecker. Принцип работы iChecker основан на подсчете и запоминании контрольной суммы (цифровой подписи) проверяемого объекта. При любой модификации объекта меняется его контрольная сумма. iChecker сохраняет информацию об изменении контрольной суммы в специальную таблицу и при последующей проверке сравнивает предыдущую и текущую контрольные суммы, и если изменений не обнаруживается, то файл исключается из проверки. iChecker работает не только с файлами, но и с объектами автозагрузки, вложенными почтовыми сообщениями и так далее.

iSwift — это вариант iChecker, написанный для файловой системы NTFS. Преимущество этой файловой системы заключается в том, что каждому объекту в ней присваивается свой NTFS-идентификатор. iSwift сравнивает NTFS — идентификатор cо значениями, которые она хранит в специальной базе данных. И в случае, если значения в базе данных не совпадают с NTFS-идентификаторами, то объект проверяется.

Необходимость высчитывать контрольную сумму при этом отсутствует, благодаря чему iSwift может работать с файлами любых размеров (в отличие от iChecker). Файл, однако, заново проверяется при копировании, так как технология привязана к конкретному местоположению. К тому же iSwift можно использовать только в файловой системе NTFS.

Помимо описанных сигнатурного и проактивного методов защиты, в наших корпоративных продуктах применяется ещё один способ оперативного выявления новых угроз: речь идёт об интеграции System Watcher с Kaspersky Security Network.

KSN — это облачный сервис, к которому на сегодняшний день подключены более 60 млн пользователей по всему миру. С согласия каждого пользователя антивирусного приложения в KSN отправляются данные о попытках заражения компьютера и о подозрительной активности программ. Полученные данные распределённо обрабатывает экспертная система, и информация о только что появившихся угрозах и источниках их распространения становится доступной всем пользователям продукта в течение 40 секунд. Для сравнения, по данным исследования, проведенного во втором квартале 2010 года компанией NSS Labs, на «ручную» работу по блокированию веб-угроз у антивирусных компаний уходит от 4,62 до 92,48 часа.

Дальнейшее принципиальное повышение скорости реакции на угрозы с помощью обычных антивирусных обновлений невозможно, так как затраты времени на обнаружение зловредов, их последующий анализ и тестирование формируемых антивирусных обновлений уже сведены к минимуму. В свою очередь, уровень детектирования эвристических методов, даже самых продвинутых, составляет в среднем 50–70%, соответственно, 30–50% вновь появляющихся угроз эвристики не детектируют.

Kaspersky Security Network вбирает в себя и анализирует огромные объёмы данных о новых угрозах и позволяет реагировать практически мгновенно: «облачным» технологиям на выявление и детектирование новых угроз необходимы минуты, а то и секунды. Если в той или иной программе выявлена вредоносная составляющая, информация о ней передаётся в Систему мгновенного детектирования, откуда распространяется клиентам.

В целом использование Kaspersky Security Network позволяет, во-первых, сократить до минимума время реагирования на угрозы, во-вторых, существенно сократить трафик, расходуемый на обновления антивирусных баз, и в-третьих, минимизировать количество ложных срабатываний защитного решения. KSN также активно применяется для борьбы с вредоносными ссылками и спамом.

Как мы видим, организация надёжно защищена программными средствами. Все версии программ регулярно обновляются специалистами. Так же организация хранит все важные данные в облачном сервисе для исключения непреднамеренного удаления информации.

# Заключение

Цель учебно-лабораторного практикума, которая заключалась в исследовании процессов защиты информации, была достигнута. В процессе прохождения были изучены информационные системы, меры и средства для их защиты, официальные документы предприятия, нормативная и методическая документация, которые позволили решить многие поставленные задачи. В ходе прохождения учебно-лабораторного практикума я ознакомился с организационной структурой, рассмотрел информационную систему обработки персональных данных, построил для неё модель угроз и модель нарушителя, определил класс и тип и рассчитал актуальные угрозы ИСПДн. Также ознакомился с новыми программными средствами обеспечения безопасности информации. Осмотрел различное оборудование и получил краткую характеристику по каждому из них. В процессе прохождения практики я влился в рабочий коллектив, почувствовал весь рабочий процесс предприятия.

Немаловажным является тот факт, что в процессе прохождения учебно-лабораторного практикума были получены новые теоретические и практические знания в области информационной безопасности:

* рассмотрение нормативно-методической базы в области построения комплексной системы защиты информации;
* анализ системы обработки данных;
* исследование организационной структуры предприятия, выявление видов конфиденциальной информации и ресурсов;
* обоснование актуальных угроз и определение нарушителей информационных процессов в системе организации;
* исследование способов защиты информационных ресурсов в системе;
* анализ каналов утечки информации на предприятии;
* формулировка выводов о состоянии комплексной системы защиты информации в организации.

Во время прохождения практики я сделал вывод, что состояние защищенности предприятия «ИП Корчев Василий Васильевич» является удовлетворительным. С целью совершенствования системы защиты в организации «ИП Корчев Василий Васильевич» следует провести следующие мероприятия:

* осуществлять более тщательный контроль соблюдения правил хранения рабочей документации сотрудников предприятия;
* регулярно проверять и обслуживать все информационные системы и информационные инфраструктуры на работоспособность;
* разграничить доступ к файлам, каталогам, дискам;
* установить программы защиты от спама;
* установить источники бесперебойного питания.

Исходя из всего вышеизложенного, можно сделать выводы, что все поставленные на учебно-лабораторный практикум цели и задачи были выполнены.

# Список используемых источников

1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
2. ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России;
3. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Госстандарт России;
4. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России;
5. ГОСТ Р 51624–2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;
6. ГОСТ Р 52069–2003. Защита информации. Система стандартов. Основные положения;
7. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью;
8. ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности;
9. Галатенко, В.А. Стандарты информационной безопасности: справ. пособие / В. А. Галатенко - М.: Интернет-университет информационных технологий, 2006. - 328 c.
10. Грибунин, В.Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В. Г. Грибунин, В.В. Чудовский. - М.: Издательский центр «Академия», 2009. - 416 с.
11. Куприянов, А. И. Основы защиты информации: учеб. Пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В. А. Шевцов - М.: Издательский центр «Академия», 2006. - 256 с.
12. Петраков, А.В. Основы практической защиты информации: учебное пособие / А.В. Петраков - М.: Радио и связь, 2004.-368с.
13. Попов, Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации. «Альтпресс», 2009. -512c.
14. Семкин, С. Н. Защита информации. Основы информационной безопасности объектов: курс лекций / С. Н. Семкин - Орел.: ВИПС, 2000. - 269 с.

# ПРИЛОЖЕНИЕ 1

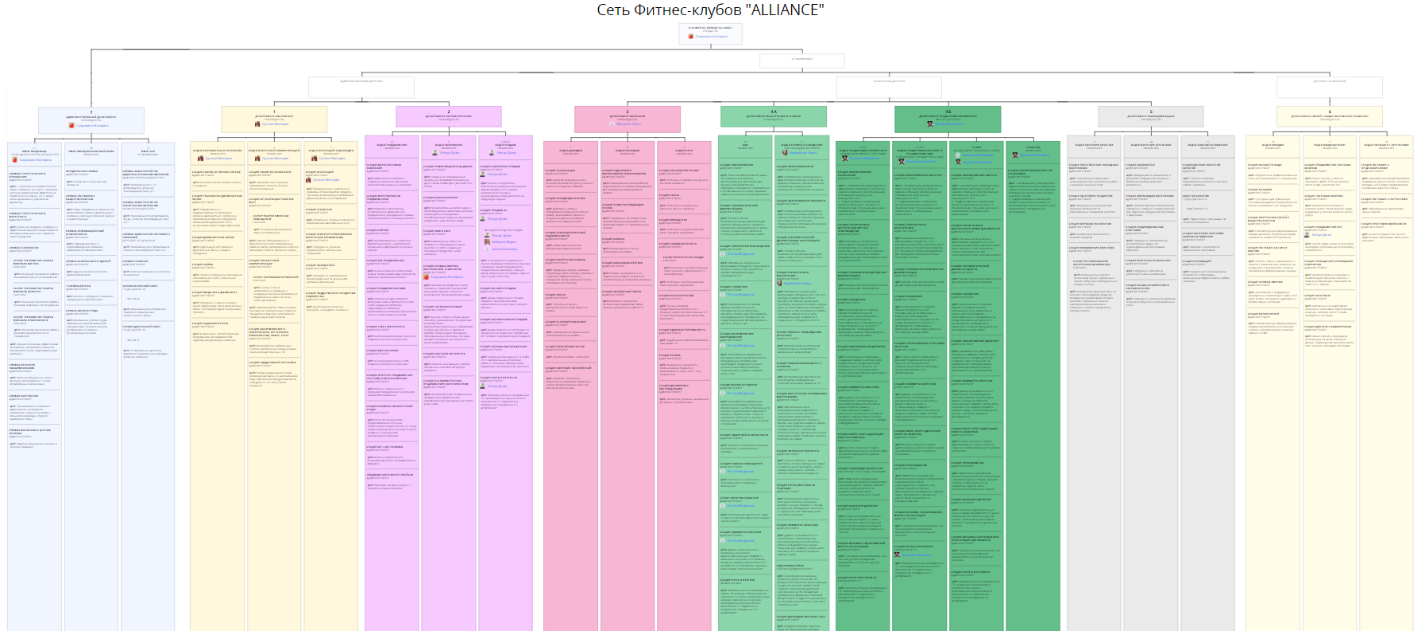


Рисунок 1 - Организационная схема предприятия «ИП Корчев Василий Васильевич»