МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.03.03 Прикладная информатика
(код и наименование направления подготовки / специальности)

Бизнес-информатика
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(БАКАЛАВРСКАЯ РАБОТА)

на тему «Проектирование системы обеспечения информационной безопасности для АНПОО «Учебно-курсовой комбинат» г. Псков»

Обучающийся А.А. Старостин
(Инициалы Фамилия) (личная подпись)

Руководитель к.т.н., Н. В. Хрипунов
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Выпускная квалификационная работа на тему «Проектирование системы обеспечения информационной безопасности для АНПОО «Учебно-курсовой комбинат» г. Псков» изложена на 76 страницах содержит 17 рисунков, 2 таблицы, 31 использованный источник литературы и 2 приложения.

Вопросы применения систем мониторинга вторжений в ЛВС любой организации всегда является актуальным, так как позволяет обеспечить грамотную защиту и работу системы обеспечения информационной безопасности.

Объект исследования – системы безопасности современного предприятия.

Предмет исследования – методы реализации системы безопасности для современной организации.

Цель исследования – осуществить разработку системы безопасности для АНПОО «Учебно-курсовой комбинат».

В результате выполнения выпускной квалификационной работы был выполнен анализ деятельности АНПОО «Учебно-курсовой комбинат», изучены реализованные мероприятия по обеспечению информационной безопасности, а также предложены собственные разработки касаемо мониторинга вторжений в каналы передачи данных и мониторинга состояния сетевого оборудования.

Содержание

Введение

Вопросы обеспечения защиты и сохранности информации были актуальны во все времена. Так, некоторая информация требует обеспечения доступа к ней только определенным кругом лиц, что не так просто реализовать. Всегда имеются люди, которые стремятся данной информацией завладеть, и применяют для этого самые различные методы и технологии.

Современное общество является информационным – информация в нем является одной из важных ценностей. Информация как покупается, так и продается, поэтому актуальность вопросов защиты информации только обострилась. Это связано не только с выделением ценности информации, но и активным развитием науки и техники, а также появлением новых классов программного обеспечения.

Поэтому не только злоумышленники, но и сотрудники, ответственные за обеспечение высокого уровня защиты данных и информационной безопасности прибегают к использованию современных программных и аппаратных средств защиты. Одним из довольно распространенных видов программного обеспечения данного рода являются системы анализа событий, обеспечивающие механизмы защиты и оповещения о нарушениях информационной безопасности за счет выполнения поведенческого анализа, считающегося одним из эффективных методов защиты. Вопрос выбора системы подобного рода всегда является актуальным, так как важно обеспечить должный уровень безопасности на предприятии, выбрав соответствующий по функционалу программный продукт.

Объект исследования – системы безопасности современного предприятия.

Предмет исследования – методы реализации системы безопасности для современной организации.

Цель исследования – осуществить разработку системы безопасности для АНПОО «Учебно-курсовой комбинат».

Для достижения поставленной цели необходимо решить следующие задачи:

– рассмотреть основные вопросы обеспечения информационной безопасности, методы и средства защиты информации;

– выполнить анализ деятельности организации;

– осуществить выбор состава оборудования для реализации системы защиты;

– разработать собственные проектные решения по модернизации инструментов защиты информации.

Планируемыми результатами исследования является выполнение функционального анализа методов обеспечения информационной безопасности, а также повышения уровня защиты целевой системы за счет внедрения системы обеспечения безопасности.

1 Анализ методических материалов по разработке системы управления информационной безопасности АНПОО «Учебно-курсовой комбинат»

1.1 Организация разработки системы управления информационной безопасностью

1.1.1 Основные процессы управления информационной безопасностью

Угроза информационной безопасности представляет собой некоторый процесс, либо явление, которые могу привести к убыткам для организации. В рамках информационной безопасности угроза принимает возможность оказать влияние на информацию, либо на системы обработки информации, в результате чего может возникнуть ущерб как для информации, так и для информационной системы.

Риском в разрезе информационной безопасности называется некоторая вероятностная оценка, на основании которой приводится численная характеристика величины возможного ущерба, который может понести владелец информационного ресурса в случае негативного воздействия на данный ресурс.

Уязвимость представляет собой потенциальный путь проникновения, либо объект, на который будет воздействовать угроза информационной безопасности [15].

Приводить полный перечень угроз информационной безопасности не имеет смысла, так как он попросту очень огромный. При осуществлении процедур установления текущего уровня защиты в организации необходимо помимо изучения существующих средств защиты провести составление исчерпывающего перечня потенциальных угроз информационной безопасности. На основании сформированного перечня будет выполняться оценка достаточного уровня защиты, а также подбор требуемых

инструментов и средств обеспечения информационной безопасности.

Для упрощения задачи анализа вероятных угроз, параллельно составлению перечня актуальных угроз информационной безопасности для предприятия, осуществляется составление перечня классифицирующих признаков угроз [23]. На основании требований к выделяемым классификационным признакам в обязательном порядке должно быть использовано одно из правил или требований к реализуемой системе защиты информации. Соответствие вероятных угроз одному из выделенных классификационных признаков позволяет выполнить детальное рассмотрение всех соответствующих данным параметрам требований [6].

Реализация обобщенной системы для выполнения классификации угроз информационной безопасности при реализации систем защиты – это необходимость, обусловленная воздействием на всю хранимую и обрабатываемую информацию набору факторов. Это приводит к тому, что становится попросту невозможно составить полный перечень угроз. Именно в связи с данным фактом наиболее объективным решением считают составление только перечня, содержащего классификационные признаки угроз информационной безопасности.

В зависимости от выделяемых классификационных параметров, все угрозы информационной безопасности можно классифицировать как несколько различных типов. В зависимости от выделенного ранга непреднамеренного напряжения угрозы выделяют следующие категории угроз информационной безопасности:

- угрозы, которые возникли в результате ошибочных действий персонала, либо небрежного выполнения должностных обязанностей, при работе или обслуживании информационной системы. Например – ввод некорректной информации, некорректное применение средств защиты и т.д.
- угрозы, возникшие в результате преднамеренно оказанных действий на информационную систему, например попытки её

взлома и т.д. [9]

На основании характера, приведшего к возникновению угрозы, выделяют:

– искусственные угрозы информационной безопасности, возникшие в результате воздействия человека или программного средства [1];
– природные угрозы, которые возникли в результате каких-либо природных бедствий.

В зависимости от того, какая причина привела к возникновению данной угрозы, для классификации могут использовать следующие причины:

– человек, который осуществляет неправомерные действия с целью получения необходимых ему данных;
– природные угрозы, такие как стихийное бедствие;
– вредоносное программное обеспечение;
– ошибки и сбои в работе программ [2].

На основании уровня активности информационной системы угрозы информационной безопасности классифицирую на:

– угрозы, которые возникли при осуществлении процедур по обработке информации;
– угрозы, которые никаким образом не зависят от уровня активности ИС [12].

На основании текущего состояния источника возникновения угрозы информационной безопасности их классифицируют как:

– угрозы, которые имеют место в самой информационной системе;
– угрозы, которые находятся в пределах рабочей зоны ИС;
– угрозы, которые имеют место за пределами работы информационной системы.

Также угрозы информационной безопасности могут быть классифицированы с использованием уровня воздействия на ИС:

– активные угрозы ИБ, которые приводят к сдвигам как в

структуре, так и сущности работы ИС;

– пассивные угрозы ИЮ, не оказывающие никакого влияния на работу ИС, и реализуются непосредственно для получения данных [7].

На основании используемых методов, которые используют с целью получения доступа к данным, выделяют:

– угрозы, реализация которых выполняется с использованием специальных каналов доступа к данным;
– угрозы, реализация которых происходит посредством обычных каналов передачи данных.

Помимо этого, существует классификация угроз информационной безопасности на случайные и преднамеренные.

1.1.2 Структурно-логическая схема действий руководства предприятия по разработке системы управления информационной безопасностью

Все методы, направленные на обеспечение информационной безопасности, подразделяются на несколько групп:

– Технические средства защиты. Сюда относятся технические и аппаратные средства, которые позволяют запретить доступ к информации самым различным образом. К числу подобных средств относятся различного рода шумовые завесы, межсетевые экраны и т.д. К основным преимуществам использования данных средств защиты следует отнести их надежность, отсутствие зависимости от различных субъективных факторов, а также высокий уровень устойчивости к различным модификациям. Недостатками данных устройств является отсутствие возможности оперативной модернизации, большие размеры и масса, а также высокая стоимость.
– Программные средства защиты. К их числу относится специализированное программное обеспечение, которое может

быть использовано с целью осуществления идентификации пользователей, проведения процедур по контролю доступа, шифрования данных и так далее. Основные преимущества программных средств защиты заключаются в их универсальности, гибкости, надежности, а также простоты инсталляции и модификации. Недостатки программных средств защиты заключаются в их ограниченной функциональности, высоком уровне чувствительности к изменениям, а также наличие некоторой зависимости от типа компьютера.

– Смешанные, программно-аппаратные средства, у которых состав функций включает в себя не только функции двух предыдущих категорий средств защиты, но и дополнительные, промежуточные функции.
– Организационные средства защиты, в состав которых относятся организационно-технические, а также организационно-правовые средства защиты данных. Преимущества данной категории средств защиты заключаются в легкости их реализации, а также возможности оперативной реакции на опасность. Однако они обладают высоким уровнем зависимости от влияния субъективных факторов [5].

Как уже было отмечено ранее, при реализации должного уровня защиты в комплексе используют три категории средств защиты – организационно-правовые, технические и программные.

Говоря о первой категории, необходимо отметить наличие специальных государственных законов, прямым образом направленные на осуществление регулирования правовых отношений в области обеспечения защиты и безопасности данных, которые хранятся в рамках информационной системы. При организации данного процесса важно соблюдать права собственности на данную информацию. Организация правовой защиты

информации происходит на законодательном уровне, и содержит в себе две категории методов защиты:

- методы, направленные на организацию и поддержку негативной реакции общества в отношении нарушителей закона;
- методы, направленные на координацию и поддержку мер, которые направленны на рост уровня образованности людей в области информационной безопасности.

Для получения защиты требуется в обязательном порядке пройти сразу несколько этапов – осуществить анализ и выбор политики информационной безопасности, произвести процедуру внедрения наиболее подходящих программных и технических средств защиты, а также разработать и внедрить организационные меры.

При реализации систем защиты масштаба предприятия важно не только обеспечить техническую и программную защиту, но и подобрать и использовать нормативно-правовые документы. После определения их состава осуществляется оценка потенциальных угроз, а также оценка возможного уровня ущерба в отношении каждой угрозы. Далее формируется специальное подразделение, либо должность, которые будут ответственными за обеспечение информационной безопасности. Данное подразделение будет осуществлять работу одновременно в нескольких направлениях – обеспечивать защиту данных, обеспечить реализацию несанкционированных проникновений, обеспечить целостность данных и т.д.

Для защиты данных возможно использование различных методов, к числу которых относится электронная подпись, криптографическое шифрование, парольный доступ, инструменты аудита и протоколирования и так далее [18]. При построении системы защиты информации обязательно важно учитывать тот факт, что не существует идеальной защиты. По данной причине к числу наиболее распространенных методик относят обеспечение физической защиты для всех съемных носителей данных, вплоть до их запирания в сейфе. Также используется одновременно и программная, и

аппаратная защита к данным и инструментам их хранения, обработки и передачи.

Для того, чтобы обеспечить грамотную работу всех перечисленных средств защиты, необходимо выполнить планирование системы управления информационной безопасностью. Все процедуры системы управления должны последовательно проходить следующие четыре этапа: планирование, внедрение, мониторинг и анализ, совершенствование [18]. Каждый этап характеризуется выполнением различных процедур. Опишем последовательно этапы разработки системы управления информационной безопасностью, начиная с создания системы.

а) Планирование процедур системы управления информационной безопасностью:
   1) решение о создании системы управления руководством компании;
   2) выбор области действия системы;
   3) инвентаризация и категорирование информационных активов;
   4) оценка уровня защищенности информационной системы (ИС) – определение уязвимостей и угроз информационной безопасности;
   5) анализ информационных рисков;
   6) разработка Положения о применимости;
   7) выбор мер по снижению информационных рисков;
   8) разработка базы нормативных документов по информационной безопасности.

б) Внедрение процедур системы управления информационной безопасностью:
   1) внедрение мер по снижению информационных рисков;
   2) определение методов оценки эффективности внедренных мер;

3) повышение квалификации сотрудников компании в области ИБ;
4) внедрение системы управления инцидентами информационной безопасности.

в) Мониторинг и анализ процедур системы управления информационной безопасностью:
1) регулярные проверки эффективности процедур системы управления;
2) регулярный пересмотр результатов анализа информационных рисков;
3) регистрация записей системы управления с целью оценки ее эффективности.

г) Совершенствование системы управления информационной безопасностью:
1) выполнение корректирующих и превентивных действий;
2) обеспечение эффективности предпринятых мер совершенствования системы управления информационной безопасностью.

1.2 Методические материалы по оценке эффективности процессов разработки и внедрения системы управления информационной безопасностью

1.2.1 Модели по управлению информационной безопасностью

Требования к информационной безопасности определяются с помощью систематической оценки рисков [9]. Решения о расходах на мероприятия по управлению информационной безопасностью должны приниматься, исходя из возможного ущерба, нанесенного бизнесу в результате нарушений информационной безопасности. Методы оценки риска могут применяться как для всей организации, так и для какой-либо ее части, отдельных

информационных систем, определенных компонентов систем или услуг, а именно там, где это практически выполнимо и целесообразно.

Оценка риска – это систематический анализ:

- вероятного ущерба, наносимого бизнесу в результате нарушений информационной безопасности с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации и других активов;
- вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью;

Может потребоваться неоднократное проведение оценки рисков и выбора мероприятий по управлению информационной безопасностью для того, чтобы охватить различные подразделения организации или отдельные информационные системы [9].

Важно периодически проводить анализ рисков в области информационной безопасности и внедренных мероприятий по управлению информационной безопасностью для того, чтобы учесть:

- изменения требований и приоритетов бизнеса;
- появление новых угроз и уязвимостей;
- снижение эффективности существующих мероприятий по управлению информационной безопасностью.

Уровень детализации такого анализа следует определять в зависимости от результатов предыдущих проверок и изменяющегося уровня приемлемого риска. Оценка рисков обычно проводится сначала на верхнем уровне, при этом ресурсы направляются в области наибольшего риска, а затем на более детальном уровне, что позволяет рассмотреть специфические риски [3].

1.2.2 Метрики управления информационной безопасностью

Метрики информационной безопасности – это КПЭ, ключевые показатели эффективности (англ. KPI – Key Performance Indicators), которые позволяют количественно оценить работу персонала и систем,

обеспечивающих информационную безопасность. Метрики могут быть представлены графически в виде дашбордов, наглядно отображающих текущую эффективность выполнения задач.

Наличие четких и прозрачных KPI играет важную роль в организации работы службы информационной безопасности. По сути, они являются некими индикаторами состояния информационной защиты компании, позволяющими производить ее мониторинг, выявлять слабые места и обеспечивать улучшение процессов и инструментов киберзащиты, а также определять соответствие стандартам и лучшим практикам.

Кроме того, с помощью KPI руководство службы безопасности может демонстрировать топ-менеджменту и собственникам бизнеса эффективность работы службы и получать финансовые вложения, необходимые для ее развития. А руководству компании, непосредственно не задействованному в области обеспечения информационной безопасности, KPI помогают правильно оценивать текущую ситуацию и принимать взвешенные и обоснованные управленческие решения.

1.3 Нормативно-правовая основа реализации системы мониторинга вторжений в каналы связи

В составе российского законодательства в области обеспечения информационной безопасности выделяют федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации.

Основным документом в данной сфере является Конституция РФ, в которой описаны основные нормы и правовые основы информационной безопасности, такие как положение правового статуса субъекта информационных отношений, основные принципы информационной безопасности и т.д. В качестве примера можно назвать нормы по поиску,

получению и передаче информации любым законным способом (п.4.ст. 29), либо установка запрета на получение доступа к информации о частной жизни (ст.23).

Далее необходимо назвать Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» [26], в котором закреплены основные правовые аспекты реализации безопасности личности, общества и государства.

В федеральном законе от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [16] описаны основные базовые нормы, касаемо всей системы законодательства. В нем описываются все определения и положения, связанные с правовым регулированием отношений в сфере информационного обмена и обеспечения информационной безопасности. В законе определены основные правовые вопросы по режимам распространения и документирования информации.

Федеральным законом от 21 июня 1993 № 5485-1 «О государственной тайне» [27], Федеральными законом от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» [28] и от 27.07.2006 г. № 152-ФЗ «О персональных данных» [29] описываются основные правовые режимы обработки информации с ограниченным доступом, в том числе информации, относящейся к коммерческой и государственной тайне.

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [30] определяет основные нормы обеспечения защиты информации при организации электронного документооборота и электронного взаимодействия с органами государственной и муниципальной власти.

Уголовным кодексов РФ [16] предусмотрена ответственность в случае совершения преступления в сфере компьютерной безопасности, помимо этого в нем имеются порядка пятидесяти статей, каждая из которых устанавливает определенную степень уголовной ответственности в случае нарушений имеющихся запретов в информационной сфере.

Трудовым кодексом РФ [25] устанавливаются правовые основы обработки и защиты персональных данных сотрудников предприятия, устанавливают степень ответственности за нарушение данных норм.

В Кодексе об Административных Правонарушениях [14] в главе 13 определена административная ответственность в случае возникновения нарушения, связанного с областью связи и защиты информации. В данном разделе содержится более 90 статей, определяющих виды ответственности за совершение проступков информационного характера.

Помимо федеральных законов также разработано большое количество правовых актов подзаконного характера, в состав которых входит большое количество документации, регулирующей сферу правового обеспечения защиты информации и обеспечения информационной безопасности.

Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [17] осуществляет установку запрета на организацию подключения информационных систем, сетей и вычислительных станций, посредством которых обрабатывается информация уровня государственной тайны, к сетям международного информационного обмена. Также, для обеспечения защиты информации в государственных учреждениях должны использоваться средства защиты, прошедшие обязательную сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Перечисленные требования способствуют обеспечению должного уровня защиты информации, относящейся к государственной тайне.

В приказе ФСО России от 07.08.2009 N 487 [16] утверждается Положение о сегменте информационно-телекоммуникационной сети Интернет, которая имеет прямое предназначение для федеральных органов

государственной власти и органов государственной власти субъектов Российской Федерации.

Также российское правовое пространство долгое время имеет в своем обороте выражение «служебная информация ограниченного распространения», подразумевающее под собой «служебную тайну». В положении Правительства РФ № 1233 от 3 ноября 1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти» [13] определены основные правовые аспекты и основы, связанные с информацией ограниченного характера.

Одним из основополагающих документов на территории РФ, на основании которого должна проводиться оценка угроз информационной безопасности, является методика Федеральной Службы по Техническому и Экспортному Контрою от 5 февраля 2021 г.

Необходимость моделирования угроз установлена основными нормативными документами ФСТЭК России в области безопасности информации для государственных информационных систем, информационных систем персональных данных и значимых объектов критической информационной инфраструктуры (КИИ). Согласно нормативным требованиям, модели угроз необходимы для решения двух задач:

- на стадии создания информационной систем и информационно-телекоммуникационных сетей – для определения предъявляемых к ним требований безопасности информации;
- на стадии их эксплуатации - для выявления новых актуальных угроз и принятия решения о необходимости модернизировать систему защиты информации.

На практике операторы информационных систем нередко пренебрегают моделированием угроз, считая, что достаточно реализовать только те меры защиты, которые определены в нормативных документах.

2 Исследование процессов управления информационной безопасностью АНПОО «Учебно-курсовой комбинат»

2.1 Опыт внедрения системы управления информационной безопасностью

В рамках процедур по обеспечению информационной безопасности в АНПОО «УКК» реализованы следующие меры:

- разработан документ, содержащий перечень правил и требований в области противопожарной безопасности, в помещениях организации установлены датчики задымления, а также система оповещения о пожаре;
- в состав должностных инструкций сотрудников включены пункты, в которых указаны требования по неразглашению корпоративной информации и тайны;
- разработано и активно используется положение об осуществлении конфиденциального документооборота;
- на рабочих местах пользователей установлено антивирусное программное обеспечение;
- на контроллере домена реализовано разграничение прав доступа, а для каждой учетной записи обязательно присвоен пароль для авторизации.

Последние пункты реализованы в рамках возможностей используемой серверной операционной системы – на ней настроены службы Active Directory, для каждого пользователя создана учетная запись, для которой задано имя пользователя и пароль на автоматизацию в системе. Помимо этого, для каждой учетной записи обязательно указывается его ФИО, присваивается членство в группе пользователей, а также состав разрешений и запретов на доступ к существующим ресурсам информационного пространства организации [15].

Для доступа к рабочей среде каждый пользователь должен ввести свои учетные данные – логин и пароль учетной записи в домене. После того, как эти данные будут введены, они будут проверены на сервере в базе данных учетных записей, и если соответствие будет обнаружено, то пользователь сможет работать далее. В рамках серверной операционной системы осуществляется ведение журнала событий, в котором фиксируются все основные действия пользователей при работе в рамках домена организации. С целью обеспечения информационной безопасности все пользователи, не относящиеся к административному персоналу, не имеют возможность получения доступа к сети Интернет. Помимо этого, в рамках мероприятий по обеспечению сетевой безопасности используются следующие инструменты:

– ограничен доступ к сети Интернет;
– реализована антивирусная фильтрация;
– предусмотрен контроль содержания трафика.

В рамках обеспечения локальной безопасности реализован ряд мероприятий:

– антивирусный контроль;
– установлен персональный межсетевой экран;
– настроены процедуры резервного копирования данных;
– ведется протоколирование доступа к сервисам данных.

2.2 Проведение исследований и обработка их результатов для АНПОО «Учебно-курсовой комбинат»

Полное наименование организации: Автономная некоммерческая профессиональная образовательная организация «Учебно-курсовой комбинат». Сокращенное наименование организации: АНПОО «УКК»

Дополнительное профессиональное образование осуществляется в АНПОО «УКК» посредством реализации дополнительных профессиональных программ:

а) Программы профессиональной переподготовки:

1) «Безопасность и охрана труда»;
2) «Безопасная эксплуатация лифтов»;
3) «Экология, охрана окружающей среды, экологическая безопасность»;
4) «Пожарная безопасность»;

б) Программы повышения квалификации в области:

1) промышленной безопасности;
2) экологической безопасности;
3) гражданской обороны;
4) пожарной безопасности;
5) безопасности лифтов, эскалаторов и пассажирских конвейеров, подъемных платформ для инвалидов.

Профессиональное обучение осуществляется в АНПОО «УКК» посредством реализации основных программ профессионального обучения:

– Программ профессиональной подготовки по профессиям рабочих, должностям служащих.
– Программ переподготовки рабочих, служащих.
– Программ повышения квалификации рабочих, служащих.

Обучение осуществляется в АНПОО «УКК» посредством реализации программ обучения по:

– Охране труда.
– Методам и приемам оказания первой помощи пострадавшим на производстве.
– Охране труда при работах на высоте.
– Допуск к работам повышенной опасности.

Схема структуры управления АНПОО «Учебно-курсовой комбинат» представлена на рисунке 1.

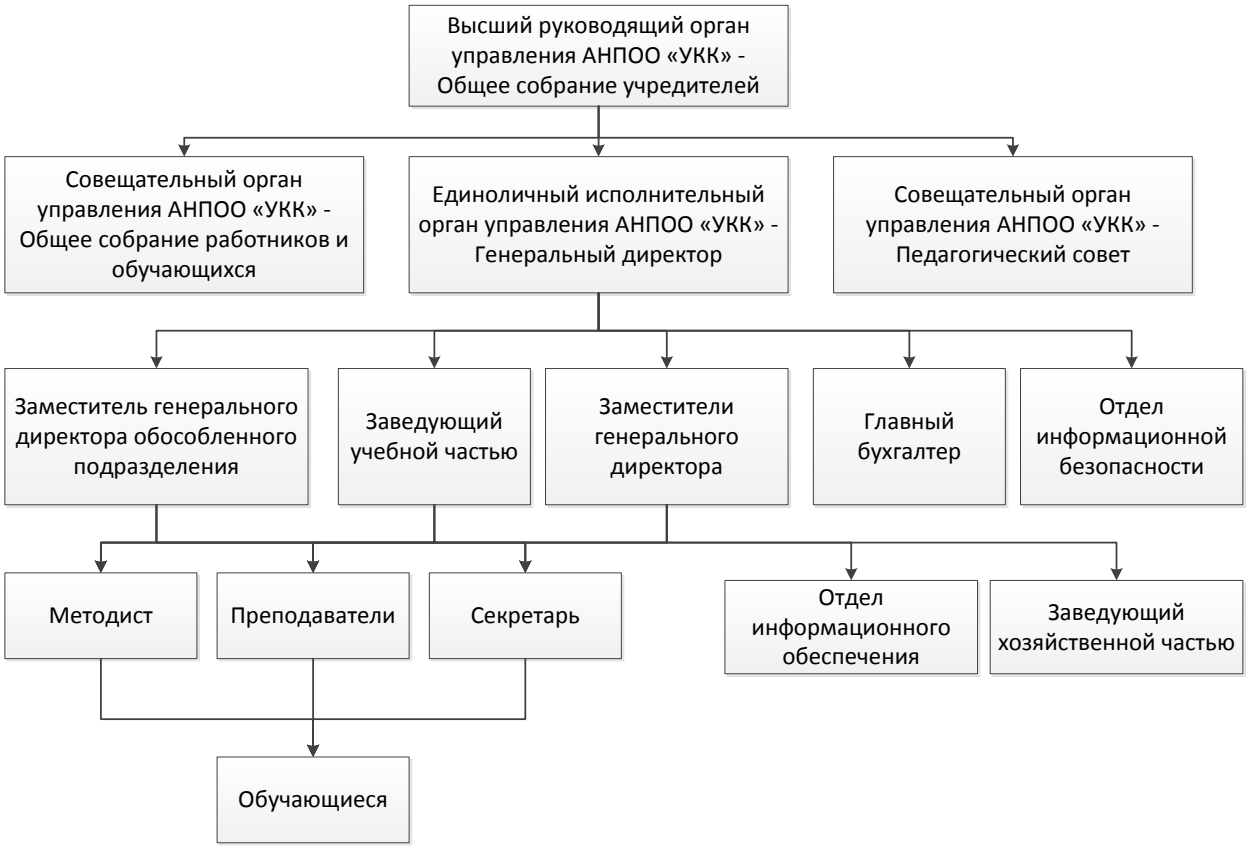

Рисунок 1 – Схема структуры управления АНПОО «Учебно-курсовой комбинат»

Подразделением, ответственным за обеспечение информационной безопасности организации, является отдел информационного обеспечения, формируемый из состава преподавателей и системного администратора. Именно ими обеспечивается работа, связанная с настройкой уровней и прав доступа, обеспечения антивирусной защиты и иных процедур по обеспечению информационной безопасности в АНПОО «Учебно-курсовой комбинат».

В АНПОО «Учебно-курсовой комбинат» используются следующие нормативно-правовые документы, на основании которых строится вся деятельность организации:

– Устав;

– Правила внутреннего трудового распорядка;

- Правила внутреннего распорядка обучающихся Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о режиме учебных занятий Автономную некоммерческую профессиональную образовательную организации «Учебно-курсовой комбинат»;
- Правила приёма обучающихся в Автономную некоммерческую профессиональную образовательную организацию «Учебно-курсовой комбинат»;
- Положение о порядке и основаниях перевода, отчисления и восстановления обучающихся Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о видах, порядке изготовления и формах документов установленного образца в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о порядке заполнения, выдачи, учёта и хранения документов установленного образца Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о документах, подтверждающих обучение в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение об использовании электронного обучения, дистанционных образовательных технологий при реализации образовательных программ в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;

- Положение о проведении промежуточной аттестации в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о проведении итоговой аттестации в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о видах, формах и процедуре внутренней системы оценки качества разработки и реализации дополнительных профессиональных программ в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о практической подготовке обучающихся Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение о порядке оформления возникновения, приостановления и прекращения отношений между АНПОО «УКК» и обучающимися и (или) их родителями;
- Положение о зачете АНПОО «УКК» результатов освоения обучающимися учебных предметов, курсов, дисциплин (модулей), практики, дополнительных образовательных программ в других организациях, осуществляющих образовательную деятельность;
- Положение о соотношении учебной (преподавательской) и другой педагогической работы в пределах рабочей недели или учебного года в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
- Положение об обучении по индивидуальному учебному плану в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;

– Положение о видах и условиях поощрения обучающихся за успехи в учебной, общественной, творческой деятельности в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
– Положение о порядке и форме зачета результатов обучения в качестве результата промежуточной аттестации при представлении обучающимся документов, подтверждающих освоение им образовательной программы или её части в виде онлайн-курсов в иной организации;
– Положение об организации и осуществлении образовательной деятельности в Автономной некоммерческой профессиональной образовательной организации «Учебно-курсовой комбинат»;
– Положение о порядке проведения аттестации педагогических работников Автономной некоммерческой профессиональной образовательной организацией «Учебно-курсовой комбинат».

Для организации эффективных процессов обмена информацией между структурными подразделениями организации в АНПОО «УКК» реализована локальная вычислительная сеть. На рисунке 2 представлена схема технической архитектуры АНПОО «УКК».

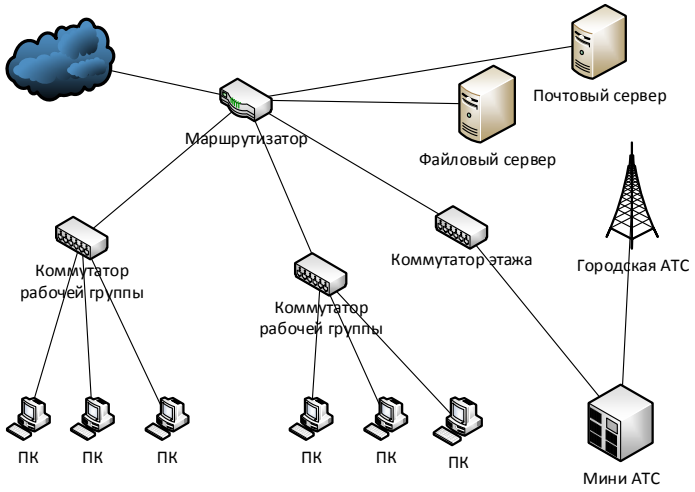

Рисунок 2 – Основная часть технической архитектуры АНПОО «УКК»

Все потоки информации проходят через локальный сервер предприятия, на котором размещена информационная база, в которой хранятся данные как о сотрудниках и контрагентах организации, а также вся рабочая документация.

Схема программной архитектуры АНПОО «УКК» представлена на рисунке 3.

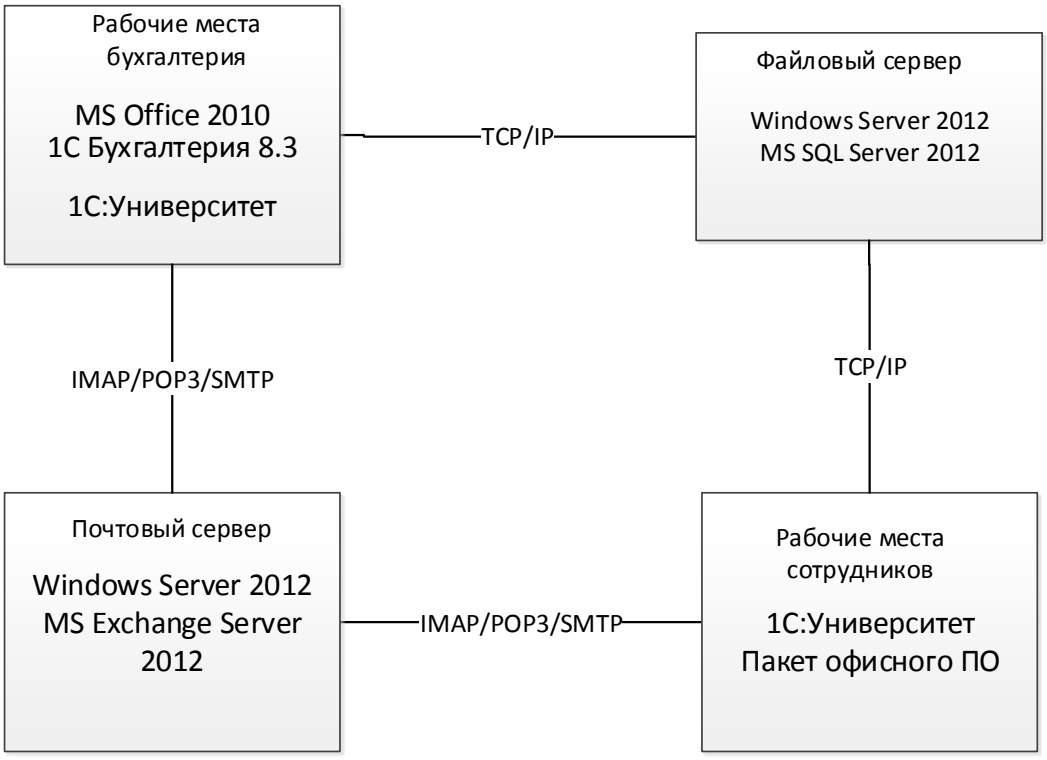

Рисунок 3 – Основная часть программной архитектуры

В основе программной архитектуры АНПОО «УКК» находятся операционные системы семейства Windows – Windows Server 2012 на серверных платформах и Windows 10 на рабочих местах пользователей.

2.3 Концептуальное моделирование предметной области

Для реализации концептуальных моделей предметной области было принято решение об использовании технологи моделирования бизнес-процессов IDEF0, что позволит подробно описать бизнес-процесс реализации механизмов информационной безопасности.

В рамках процедур по обеспечению информационной безопасности в АНПОО «УКК» реализованы следующие меры: разработан документ, содержащий перечень правил и требований в области противопожарной безопасности, в помещениях организации установлены датчики задымления, а также система оповещения о пожаре; в состав должностных инструкций сотрудников включены пункты, в которых указаны требования по неразглашению корпоративной информации и тайны; разработано и активно используется положение об осуществлении конфиденциального документооборота; на рабочих местах пользователей установлено антивирусное программное обеспечение; на контроллере домена реализовано разграничение прав доступа, а для каждой учетной записи обязательно присвоен пароль для авторизации.

2.4 Разработка и анализ модели бизнес-процесса «как есть»

Под информационной безопасностью понимаю уровень защищенности информации в обрабатываемой среде организации, что обеспечивает её формирование, применении и развитие в интересах персонала, клиентов и контрагентов организации [20].

Процесс обеспечения информационной безопасности включает в себя деятельность по обеспечения отсутствия утечек информации, а также несанкционированного и непреднамеренного воздействия на информацию, которую необходимо защитить [10]

К процессу защиты информации относится целый комплекс

мероприятий, основное направление которых заключается в обеспечении должного уровня информационной безопасности на предприятии [21].

На основании вышесказанного важно отметить тот факт, что выявление проблем по осуществлении информационной безопасности начинается с выявления субъектов информационных отношений и интересов данных субъектов, что напрямую имеет связь с применением информационной системы.

На рисунках 4 и 5 представлены IDEF0 диаграммы осуществления защиты информации в АНПОО «УКК» «Как есть». На данных диаграммах представлен основной недостаток реализации данного процесса – отсутствие автоматизированного выполнения данного процесса, а также применения специализированного программного обеспечения. Проверка осуществляется на основании графика выполнения проверка.

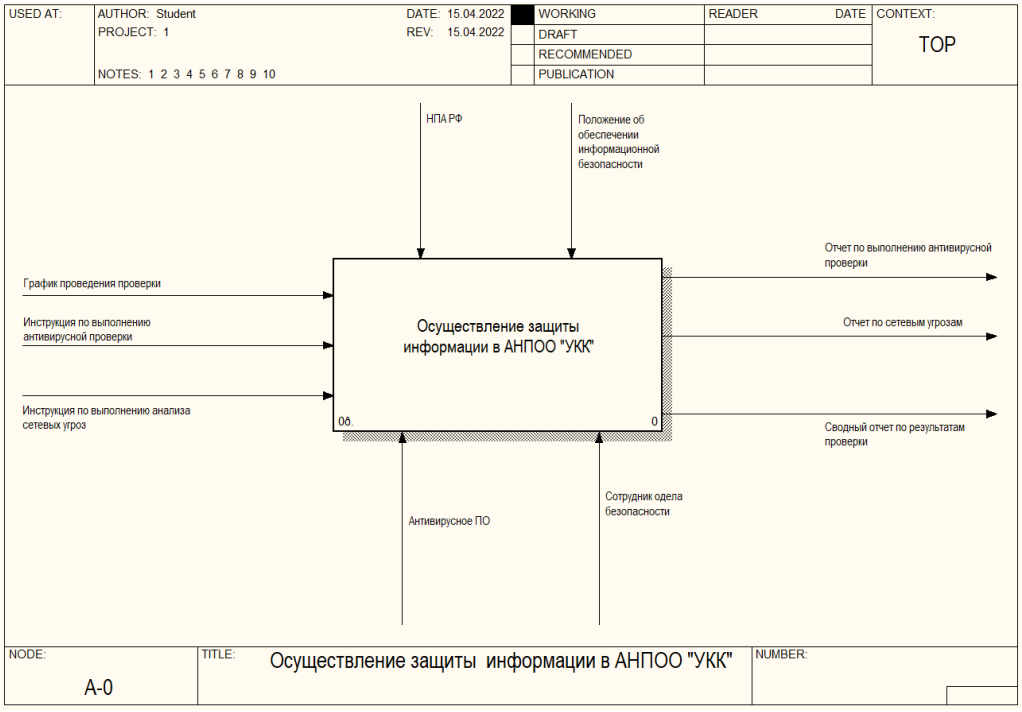

Рисунок 4 – IDEF0 диаграмма осуществления защиты информации в АНПОО «УКК» «Как есть»

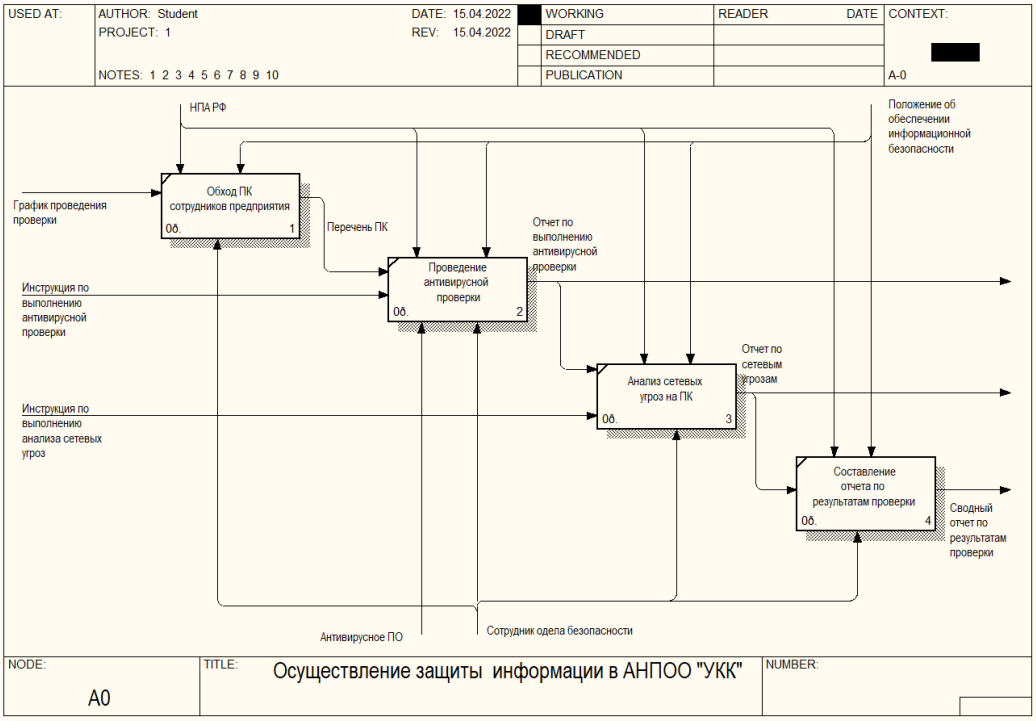

Рисунок 5 –Декомпозиция IDEF0 диаграммы осуществления защиты информации в АНПОО «УКК» «Как есть»

Сотруднику отдела безопасности приходится лично обходить все компьютеры организации и выполнять проверку вручную, после чего так же вручную подготавливать отчет по результатам выполненной проверки. При этом используется отчет, полученный от антивирусного программного обеспечения касаемо результатов антивирусной проверки.

Как видно из представленных диаграмм, на текущий момент в АНПОО «УКК» отсутствует система, позволяющая выполнять мониторинг состояния каналов связи и проникновений в сети организации. Также отсутствует функционал мониторинга состояния сетевых устройств и оборудования по обеспечению защиты, подключенного к сети организации. Это является серьезным недостатком, который планируется устранить в рамках данной работы.

2.5 Обоснование необходимости автоматизированного варианта решения и формирование требований к новой технологии

Оценка выполнения основных задач по обеспечению информационной безопасности выполнялась в несколько этапов – сначала было выполнено разбиение всех задач по обеспечению информационной безопасности, после чего уже выполнялся непосредственно анализ уровня их выполнения. Полученные в результате оценивания текущего выполнения мероприятий в области информационной безопасности в АНПОО «УКК» представлены в таблице 1

Таблица 1 – Анализ выполнения основных задач по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	Степень выполнения
Организация защиты данных, относящихся к коммерческой тайне или секретной информации	Выполнено частично
Проведение работ в области реализации правовых, организационных, а также программно-аппаратных мер защиты данных, относящихся к коммерческой тайне или секретной информации	Выполнено частично
Основные задачи по обеспечению информационной безопасности	Степень выполнения
Реализация защищенного документооборота	Выполнено частично
Защита данных от необоснованного и несанкционированного доступа	Не выполнено
Организация работ по обнаружению и устранению возможных каналов утечки данных	Выполнено частично
организация охраны здания организации	Выполнено полностью
организация защиты и шифрования системы передачи информации, составляющей коммерческую тайну и секретную информацию	Не выполнено
развертывание видеонаблюдения на территории и в помещениях организации	Не выполнено
обеспечение защиты каналов передачи данных	Выполнено частично

Для оценки использовалась трехуровневая шкала – «Не выполнено», «Выполнено частично» и «Выполнено полностью».

Для оценки рисков необходимо произвести анализ данной таблицы. При этом необходимо учитывать не только компоненты информационной системы, но и персонал, а также техническую структуру ИС. При осуществлении оценки используется ценовая шкала, демонстрирующая соответствие для каждого актива состава возможных угроз информационной безопасности. Как наиболее подходящий вариант была использована шкала с выделением низкого, среднего и высокого уровней критичности.

В рамках решаемой задачи обеспечения информационной безопасности следует выделить потенциальных нарушителей информационной безопасности. К ним следует отнести: ссотрудников организации; технический персонал организации; недобросовестный клиент; конкуренты.

2.6 Постановка задачи на разработку проекта создания/внедрения АИС

Как было установлено ранее, в организации на текущий момент времени отсутствуют такие элементы, как система контроля доступа, система видеонаблюдения, а также охранной пожарной сигнализации. Система сигнализации реализована частично – установлены звуковые излучатели, датчики открытия дверей и окон, а также тревожная кнопка. С учетом развития современных технологий в области обеспечения информационной безопасности и обеспечения защиты помещений данные решения являются устаревшими и требуют существенной модернизации.

Реализация системы видеонаблюдения и охранной-пожарной сигнализации выполняется для обеспечения сохранности, а также визуального наблюдения и регистрации в формате записи на электронном носителе текущих событий [8], касаемо следующих процессов:

– круглосуточный контроль происходящих на территории охраняемого объекта событий, которые требуют дистанционного визуального контроля, а также запись данных событий;

- сохранение полученных записей на внешних носителях в формате архива, последующий просмотр данного архива;
- возможность осуществления в параллельном режиме процедур записи и просмотра видеоизображений, а также выполнения их обработки и передачи по локальной сети;
- просмотр получаемых изображений на мониторе в режиме разбиения на квадраты, а также в режиме вывода изображения с одной из камер видеонаблюдения в полноэкранный режим;
- предоставление возможности организации удаленного просмотра и мониторинга состояния объекта посредством сетей передачи данных;
- обеспечение актуального состояния дверей и ворот на территории помещения;
- оповещения в режиме реального времени о проникновению на территорию охраняемого объекта;
- оповещения о возникновении задымления или возгорания на территории охраняемого объекта.

Целями реализации системы видеонаблюдения и охранной-пожарной сигнализации является:

- обеспечение защиты помещений охраняемого удаленного объекта телерадиовещания от проникновения злоумышленников или вандалов, осуществление своевременного реагирования с целью пресечения противоправных действий, а также непосредственно защита имущества;
- обеспечение безопасности и защиты охраняемого объекта от возможных возгораний;
- ведение учета передвижений и выполнения работ на территории объекта удаленного телерадиовещания в режиме реального времени;

– формирование базы видеозаписей за определенный временной период, которая позволит контролировать и отслеживать цепочку временных события для последующего упрощения розыскных, оперативно-следственных и иных мероприятий;
– предоставление возможности по осуществлению удаленного подключения к камерам видеонаблюдения для демонстрации изображений с них в режиме реального времени;
– снижение до минимального уровня возможного ущерба, который возникает в результате вандализма, либо воровства;
– повышение уровня защиты удаленного объекта телерадиовещания.

Для любой сети видеонаблюдения и сигнализации основным требованием является качественное и бесперебойное её функционирование для всех пользователей данной сети [22]. Технические требования к сети передачи данных:

– сеть передачи данных должна быть спроектирована на основе технологии Ethernet и протокола IP.
– скорость канала для подключения зданий к сети передачи данных должна быть не менее 1000 Мбит/с.
– пропускная способность магистральной сети передачи доступа должна быть не менее 10000Мбит/с.

В состав локальной вычислительной сети, которая будет использована в качестве инструмента передачи данных необходимо включить следующие набор структурных элементов:

– информационная кабельная подсистема, обладающая высоким уровнем пропускной способности;
– обязательно использование конфигурируемого активного оборудования с подключением к сети Интернет.

При реализации кабельной подсистемы важно обязательно опираться на требования стандарта ISO/IEC 11801. В рамках данного стандарта следует

стремиться не превышать длину кабеля в 150 метров от информационного порта коммутационного оборудования до сетевой розетки [19].

Для кабельных подсистем в рамках локальной вычислительной сети важно предусмотреть обеспечение требований по защите кабеля от повреждения с прокладкой его в специальных кабельных каналах, а также крепление его посредством специальных кабельных стяжек.

Видеокамеры и видеорегистраторы в рамках реализуемой системы видеонаблюдения могут быть использованы как аналогового, так и цифрового формата. Основным требованием к камерам видеонаблюдения является обеспечение высокого качества изображения на видеозаписи.

Работа с системой видеонаблюдения должна быть реализована с применением бесплатного программного обеспечения. Данное ПО должно обеспечить необходимый состав функций по работе с системой видеонаблюдения:

- запись изображений с видеокамеры;
- вывод изображений на экран в формате разделения изображения с разных камер;
- вывод изображения на экран в формате масштабирования изображения с одной камеры;
- выполнения процедур просмотра видеозаписей в архиве.

Размещение и монтаж видеокамер на территории объекта должны быть выполнены в соответствии с минимальной высотой, рекомендуемой производителем.

В системе питания как для системы видеонаблюдения, так для охранно-пожарной сигнализации важно обеспечить систему стабилизации напряжения, с целью исключения скачков напряжения и искажений в системе электропитания, а также устранения наводок на систему видеонаблюдения, что в противном случае может привести к ухудшению качества сигнала с видеокамер – для аналоговых видеокамер это приведет к

возникновению помех на изображения, а для цифровых – к потере кадров. Поэтому важно обеспечить защиту системы от перепадов напряжения.

На случай возникновения ситуаций с отключением электроэнергии важно предусмотреть наличие собственного источника бесперебойного питания [24], который обеспечит электропитанием оборудование в составе системы видеонаблюдения и охранно-пожарной сигнализации на срок не менее часа после переключения на резервное электропитание.

Для системы видеонаблюдения важно обеспечена следующих функций:

– осуществление просмотра изображений с камер в режиме реального времени;
– осуществление записи изображения с видеокамер и последующее хранение записей за период не менее одного месяца.

В зависимости от поставленных задач, система видеонаблюдения должна обеспечить следующие режимы работы: осуществление постоянной записи изображения, запись изображения по команде оператора, осуществление записи после того, как сработал детектор движения, а также выполнение записи на основании заранее назначенных временных интервалов. С полученными записями система должна предоставить возможность просмотра их как в прямом, так и в обратном порядке. Выполнять покадровый переход вперед и назад, выполнять остановку и паузу просмотра записи, осуществлять выбор и увеличение фрагмента полученного изображения.

Система пожарной охранной сигнализации должна предоставлять сведения о нарушении периметра охраняемого объекта, открытия дверей, проникновения в контейнер с оборудованием, возникновения задымления или пожара на территории охраняемого объекта.

Система видеонаблюдения должна обеспечить возможность ведения архива видеозаписей за период не менее одного календарного месяца при работе в режиме максимального разрешения изображения с видеокамер.

При этом в применимом программном обеспечении должна быть функция сохранения отдельного отрезка из видеозаписи и сохранения данного отрезка в отдельный файл, с последующим переносом данного файла на различные внешние носители.

Важно обеспечение защиты системы видеонаблюдения, а также охранной пожарной сигнализации, и архива системы видеонаблюдения от несанкционированного управления, или операций копирования и обработки видеоизображения.

2.7 Разработка модели бизнес-процесса «как должно быть»

На рисунке 6 представлена IDEF0 диаграммы осуществления защиты информации в АНПОО «УКК» «Как должно быть».

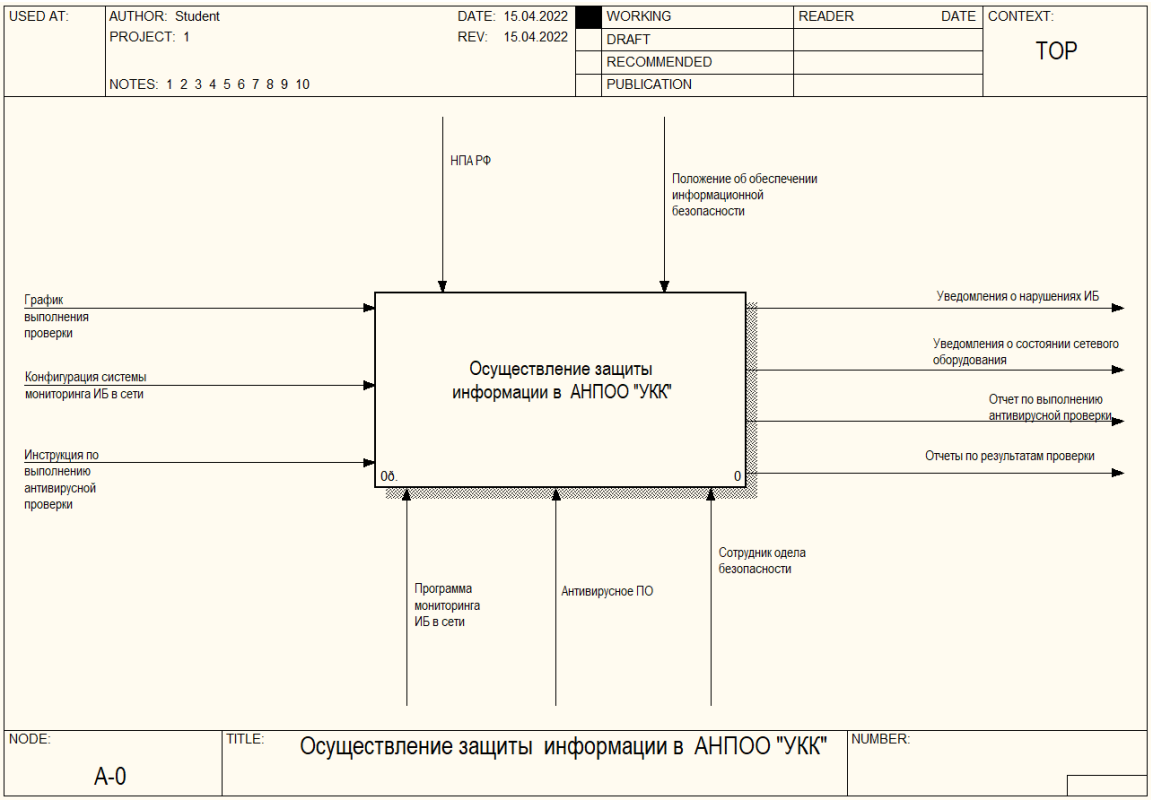

Рисунок 6 – IDEF0 диаграмма осуществления защиты информации в АНПОО «УКК» «Как должно быть»

Здесь продемонстрировано использование специализированного программного обеспечения, выполнение проверки которым осуществляется автоматически, как и формирование итоговой документации. В частности, остается график проведения проверки, но он уже касается проверки компьютеров на наличие вирусных угроз. Добавляются входные сведения касаемо конфигурации системы обеспечения информационной безопасности. На выходе процесса, помимо формируемого отчета, добавлены уведомления о нарушениях информационной безопасности и о уведомления о состоянии сетевого оборудования и устройств защиты.

На рисунке 7 представлена декомпозиция IDEF0 диаграммы осуществления защиты информации в АНПОО «УКК» «Как должно быть».

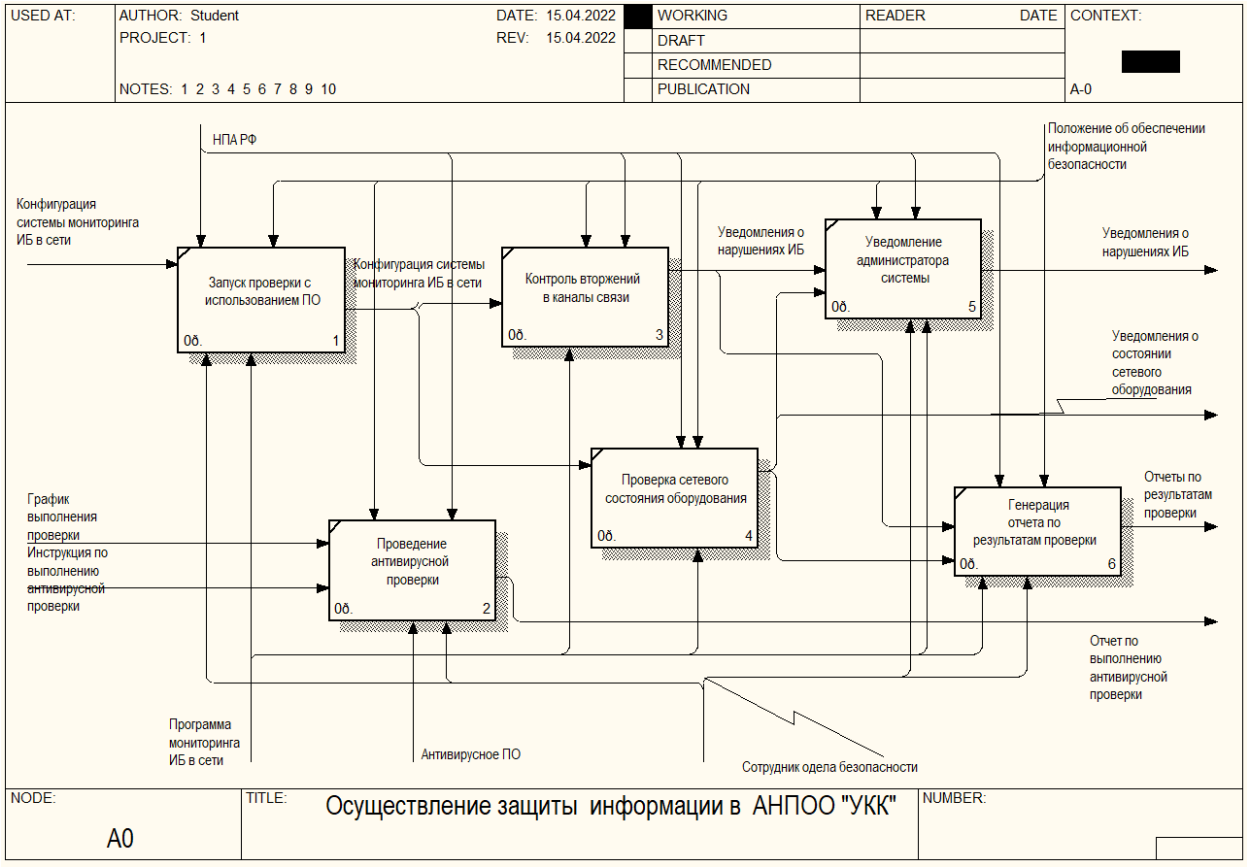

Рисунок 7 – Декомпозиция IDEF0 диаграммы осуществления защиты информации в АНПОО «УКК» «Как должно быть»

Основное отличие предлагаемого варианта – выполнение проверки каналов связи и сетевого оборудования в автоматическом режиме. Сотрудникам службы безопасности вручную потребуется выполнять только антивирусную проверку, мониторинг угроз в локальной сети организации будет выполняться автоматически. При этом, помимо отчетов, которые формируются сотрудниками, система будет предоставлять уведомления в случае обнаружения угроз, либо при изменении статуса контролируемого оборудования, которые впоследствии могут быть приобщены к формируемым отчетам.

На основании представленных моделей необходимо сделать вывод, что реализуемая система позволит сотрудникам отдела информационного обеспечения реализовать большее функций по обеспечению информационной безопасности, при этом без временных затрат на реализацию мониторинга оборудования и сети, так как это будет выполняться в автоматическом режиме. А в случае обнаружения нарушения информационной безопасности администратору системы будет выдано соответствующее уведомление.

Говоря об автоматизации деятельности по обеспечению информационной безопасности необходимо построить диаграмму вариантов использования автоматизированной системы. Данная диаграмма представлена на рисунке 8.

Рисунок 8 – Диаграмма вариантов использования системы

Пользователь системы будет осуществлять работу с системой в плане конфигурирования её касаемо действий при обнаружении различных категорий угроз. При получении уведомлений пользователь может назначать действия для выявленной угрозы в том случае, если системой не было ничего предпринято. При этом сама система осуществляет взаимодействие с внешними системами – сетевым оборудованием и каналами передачи данных, анализируя их состояние.

2.8 Рекомендации по совершенствованию процессов разработки и внедрением системы управления информационной безопасностью для АНПОО «Учебно-курсовой комбинат»

На текущий момент времени существует три варианта реализации стратегии информационной безопасности – это оборонительная, наступательная и упреждающая стратегии.

В том случае, если будет выбрана оборонительная стратегия, то при исключении каких-либо вмешательств в непосредственную работу

информационной системы, то будет получена возможность нейтрализации лишь наиболее опасных угроз информационной безопасности. Как правило для это выполняют специальную «защитную оболочку», в рамках которой разрабатываются дополнительные организационные меры, реализуются программные средства допуска к ресурсам в рамках информационной системы, осуществляется выбор и внедрение аппаратных инструментов организации контроля помещений, в которых размещено активное сетевое, а также серверное оборудование.

При выборе наступательной стратегии осуществляется активная борьба со всеми существующими угрозами информационной безопасности. В рамках данной стратегии возможна установка специального программно-аппаратного обеспечения, используемой для аутентификации пользователей, внедряются максимально современные инструменты резервирования и восстановления данных, повышать уровень доступности системы с применением различных методик резервирования.

Говоря об упреждающей стратегии, подразумевается проведения наиболее тщательного исследования всех возможных угроз в рамках информационной системы организации, после чего вырабатывается целый комплекс мер, направленных на их устранение на самых ранних стадиях их возникновения. Одной из важнейших составляющих данной стратегии обеспечения информационной безопасности является осуществление оперативного анализа информации касаемо наиболее актуального отечественного и мирового опыта в области обеспечения информационной безопасности.

В качестве методов реализации комплексной системы управления рисками в важно использовать следующие инструменты: организация эффективного управления ИТ-инфраструктурой; организация управления процессами информационной безопасности; организация управления идентификацией, авторизацией и доступом с распределением ролей и сквозной отчетностью; обеспечение целостности данных; обеспечение

конфиденциальности критичной информации;

Необходимость учитывать требования по обеспечению информационной безопасности при реализации информационной системы предприятия заключается в обязательных требованиях по сохранности информации. Ведь наличие ошибок при реализации информационной системы может привести к потере данных, а в случае наличия уязвимостей системы защиты информации, то злоумышленник может легко получить доступ к охраняемым данным. А недостаточная продуманность графического интерфейса делает его неудобным для пользователя, что может только увеличить вероятность возникновения ошибок пользователей при обработке данных – это приведет как к её искажению, так и к разрушению. По этой причине обеспечение информационной безопасности важно на каждом этапе реализации информационной системы.

3 Физическое проектирование системы обеспечения информационной безопасности

3.1 Разработка архитектуры системы

Первым шагом при реализации программного обеспечения строится диаграмма классов для реализуемой системы. В основе здесь будут угрозы и признаки угроз, на их основании будет формироваться журнал, в котором будут фиксироваться все события, связанные с различными угрозами. На основании данных классов будет осуществляться функционирование системы мониторинга каналов передачи данных. Диаграмма классов представлена на рисунке 9.

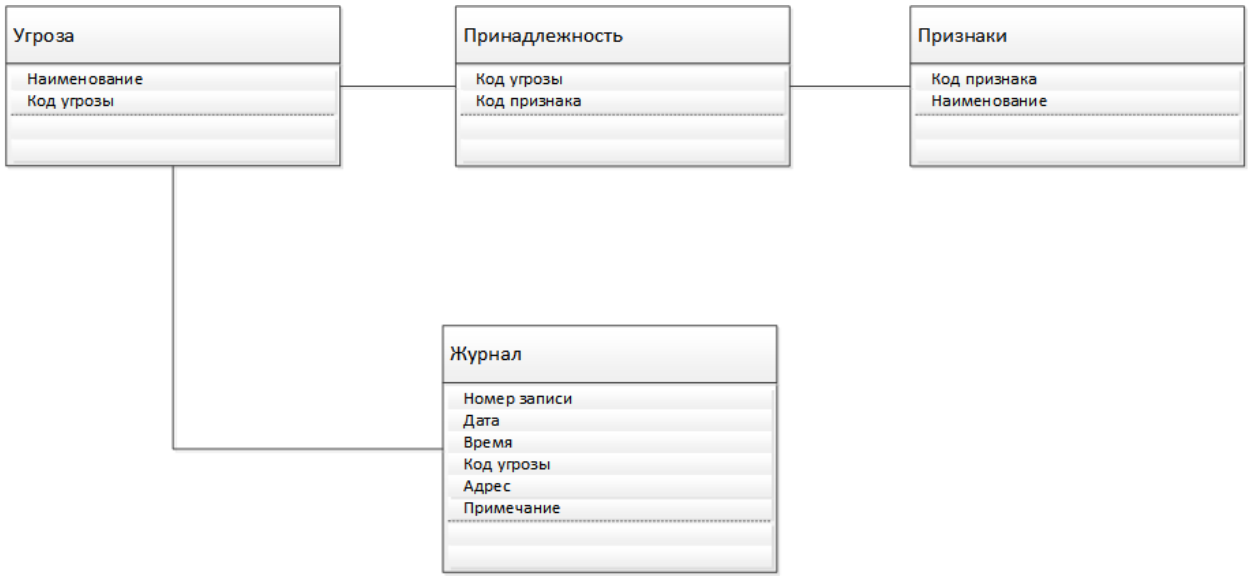

Рисунок 9 – Диаграмма классов системы мониторинга вторжений

На основании указанных сведений будет осуществляться работа по обеспечению информационной безопасности в рамках локальной вычислительной сети организации. Для программного продукта, выполняющего мониторинг состояния оборудования в структуре системы

обеспечения информационной безопасности реализована своя диаграмма классов, изображенная на рисунке 10. В данном случае используется класс, работающий непосредственно с оборудованием, и класс, в котором формируется журнал, в составе которого ведется учет изменения статуса оборудования в сети.

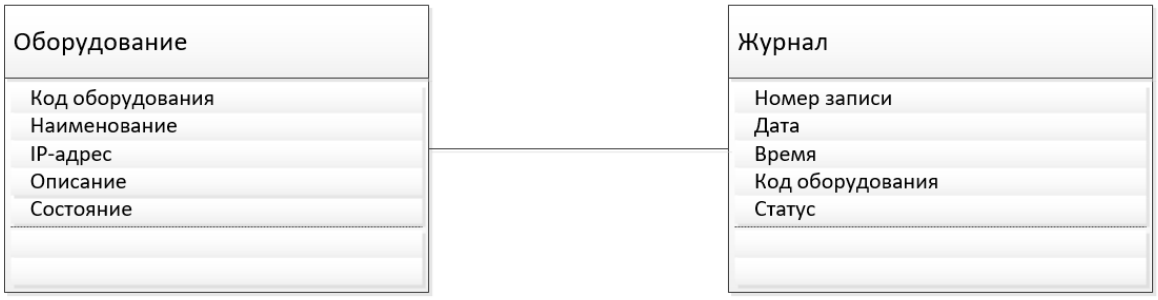

Рисунок 10 – Диаграмма классов системы мониторинга состояния оборудования в сети

На основании реализованных диаграмм классов будет выполняться проектирование информационного обеспечения реализуемых систем.

3.2 Выбор технологии разработки программного обеспечения АИС

При выборе способа осуществления процесса автоматизации выделяют несколько различных вариантов:

– Осуществить приобретение готового решения. Данный вариант приобретения информационной системы организацией приобретается готовое решение и настроенная модель ведения бизнеса. В качестве преимуществ данной методики является низкий уровень затрат на автоматизацию и высокий показатель надежности. Однако к числу минусов относится необходимость выполнения перестройки деятельности организации в

соответствии с приобретаемой моделью, а также отсутствие специфичной управленческой отчетности.

– Выполнить приобретение адаптируемого решений и комплекса услуг по его внедрению. Данный подход позволяет организации получить некоторое универсальное решение, которое будет адаптировано под специфику функционирования организации. В данном случае качество выполненной адаптации в прямом смысле будет зависеть от того, как будет выполнена дополнительная настройка системы. Для этого важно точно знать все особенности ведения учета в организации, для чего наиболее подходящим вариантом реализации будет совместная работа организации, выполняющей внедрение и настойку системы, с сотрудниками организации [11].
– Привлечение собственных специалистов для создания собственного программного продукта. Для данного варианта приобретения информационной системы характерно получение программного продукта, имеющего полное соответствие всем поставленным требованиям.

На основании анализа существующих методов приобретения информационной системы было принято решение о разработке собственного программного продукта.

Процесс проектирования информационной системы может быть представлен как многоступенчатый процесс, в результате выполнения которого будет создана, либо модернизирована информационная система. При этом в обязательном порядке используется упорядоченная совокупность методов и инструментов проектирования. В отличии от моделирования, в данном процессе работа ведется с еще несуществующим объектом, а основной задачей данного процесса является реализация информационной системы в области:

– обработки некоторых объектов в составе реализуемой базы данных;
– реализации программного обеспечения, реализующего функционал выполнения запросов к данным;
– осуществление учета работы конкретной среды, либо технологии.

Рассматривая стадию проектирования информационной системы в виде отдельного этапа необходимо разместить её между анализом требований и непосредственно разработкой информационной системы. При этом следует учитывать тот факт, что на практике данное разделение практически невозможно. Это обусловлено тем, что процесс проектирования начинается с определения основных целей реализации проекта, после чего может продолжаться как на стадии реализации, так и на стадии тестирования.

Технология проектирования представляет собой регламентированную последовательность технологических операций, которые выполняются на основании заранее выбранного метода. Данный метод в полной мере описывает последовательность выполняемых процедур и операций

Для выбираемой технологии проектирования информационной системы выделяется ряд требований: используемая технология должна обеспечить минимальные затраты, как трудовые так и стоимостные, необходимые для выполнения операций проектирования и последующего сопровождения проекта; технология должна являться основой, обеспечивающей тесную взаимосвязь между выполнением проектирования и последующего сопровождения проекта; технология должна обеспечивать максимальное увеличение уровня производительности труда проектировщиков; технологией должна обеспечиваться высокая надежность процессов по проектированию и последующей эксплуатации информационной системы; при использовании выбранной технологии важно максимально простое ведение всей рабочей документации.

3.3 Разработка модели данных АИС

С целью моделирования структуры информационной базы данных реализуется ER-модель. Построение реализуется на основании методологии IDEF1X.

Для работы программного продукта потребуется реализация информационной базы. Для этого реализуется модель базы данных, представленная на рисунке 11.

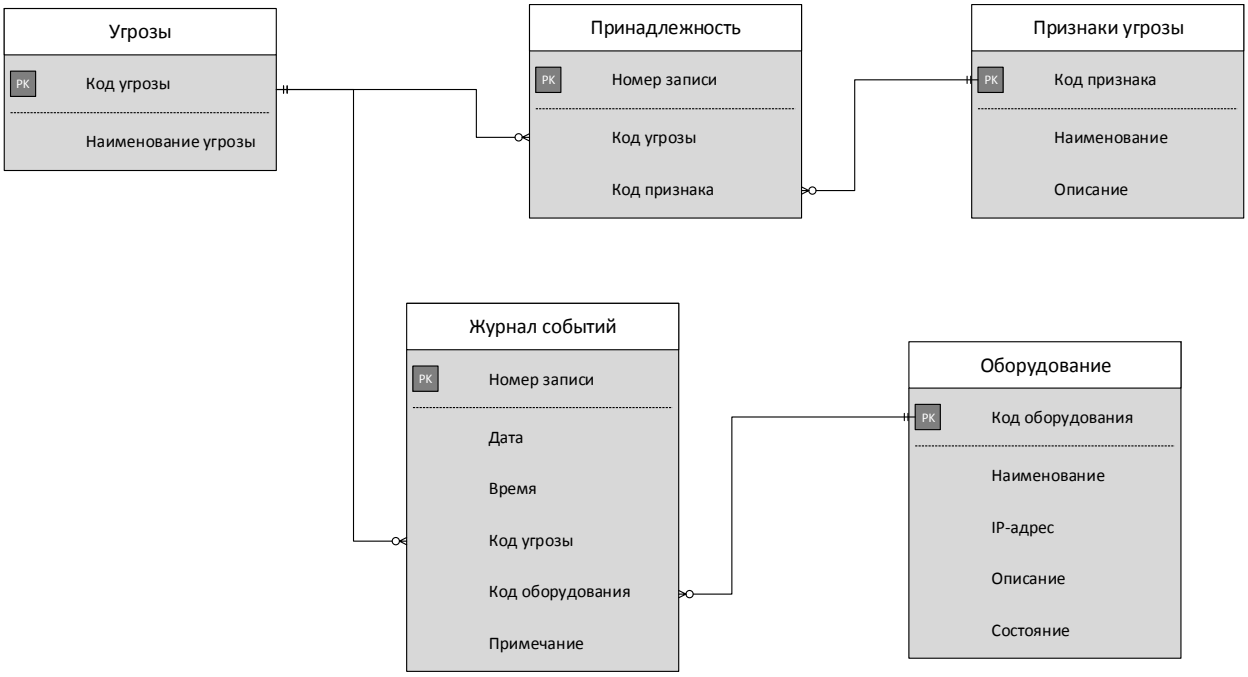

Рисунок 11 – Модель базы данных системы обеспечения информационной безопасности

Представленная модель будет являться основой для хранения всей информации в разрабатываемого инструмента обнаружения вторжений в каналы связи и мониторинга состояния оборудования.

3.4 Разработка программного обеспечения АИС

Для обеспечения защиты информации в рамках каналов связи предлагается реализации собственного инструмента обнаружения вторжений в каналы связи. Рассмотрим схему организации средства мониторинга и защиты от угроз ИБ, изображенные на рисунке 12.

С целью выполнения анализа трафика, который будет собран как на периметре, так и внутри сети, для оценки его на наличие внедренных в него вредоносных протоколов и сервисов, применяется Network Traffic Analysis (NTA) и Network Behavior Analysis (NBA). Осуществляя процедуры по сравнению сигнатур, а также выполняя поведенческий анализ система NTA/NBA получает возможность оперативно получить сведений о работе вредоносного программного обеспечения.

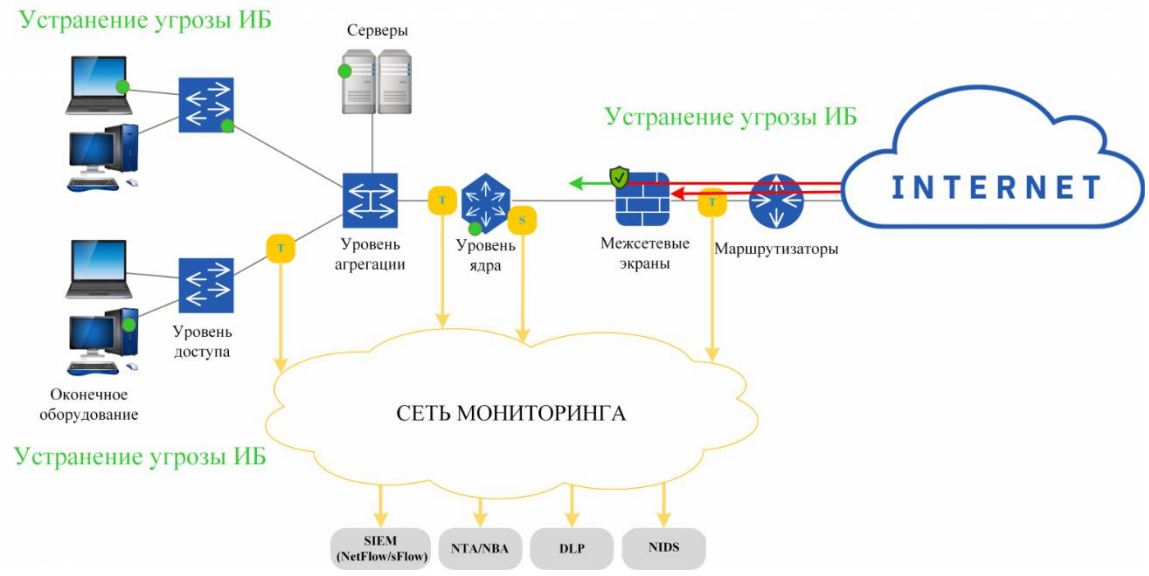

Рисунок 12 – Схема реализуемого средства анализа вторжений

Наличие функционала по обработке зашифрованного трафика, а также наличие механизма анализа протоколов появляется возможность выявления аномалий в трафике. Механизмы поведенческого анализа и машинного

обучения используются с целью выявления странной активности в работе сетевых сервисов, а также попытки подбора учетных данных, что выявляется посредством отлова большого количества неуспешных аутентификаций в сетевых сервисах и службах. В роли вспомогательного инструмента в реализованном средстве применяется архитектура Prelude, выступающая в качестве менеджера, агента управления событиями безопасности LML, модуля корреляции, базы данных и интерфейсной подсистемы Prewikka. На рисунке 13 представлена схема реализации модели обнаружения вторжений.

Реализация средства мониторинга была осуществлена на основании совокупности инструментов, функционирующих на базе операционной системы Linux.

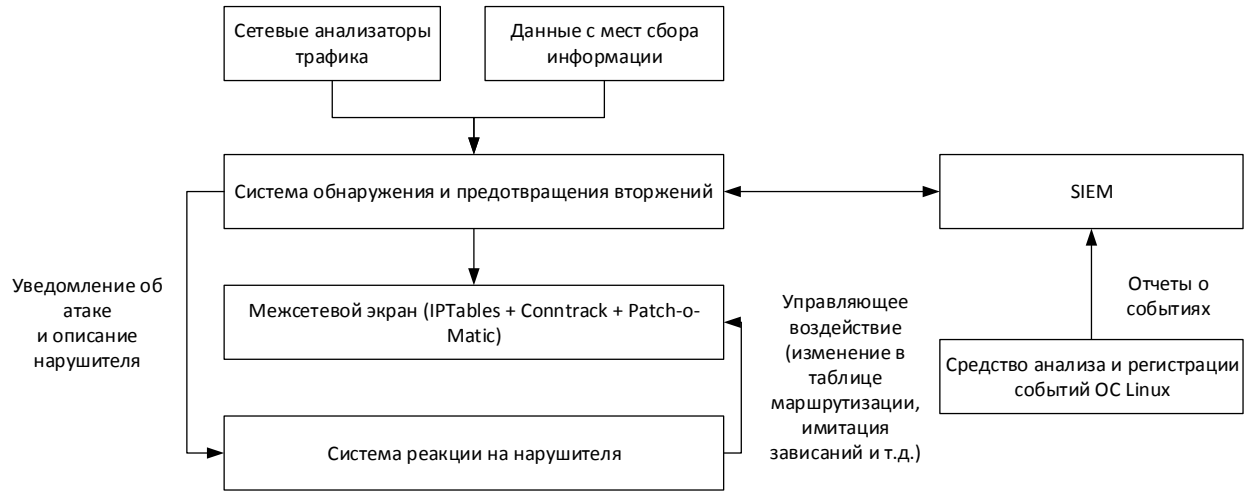

Рисунок 13 – Схема реализации проектируемого средства мониторинга

Для этого в состав технической архитектуры потребуется внедрение аппаратной платформы, которая будет играть роль сервера для средства мониторинга вторжений. В состав реализованного средства мониторинга сходя следующие элементы:

– IDS/IPS Bro;

– комплексный межсетевой экран на базе Netfilter с использованием заплат на ядро POM и трассировщиком соединений;
– SIEM-систему Prelude OSS;
– Системный журнал Rsyslog-сервер;
– Систему реакции на нарушителя.

Основой реализованного средства мониторинга вторжений выступает программный пакет IDS/IPS Bro, представляющий собой фреймворк, инсталлируемый в ОС Linux, и используемый для осуществления анализа трафика. В результате его установки и настройки серверная платформа реализуется механизмы средства обнаружения вторжений.

Bro работает на основе скриптов.

Сбор информации происходит с датчиков, устанавливаемых на рабочие места пользователей, а также сетевой анализатор трафика, встроенный в брандмауэр.

Реализованное средство мониторинга включает в свой состав несколько модулей, описанных ранее, что позволяет организовать грамотную борьбу с большим перечнем сетевых угроз за счет выставления «ловушек», а также фальсификации параметров сети. Данное средство мониторинга может быть гибко настроено, и позволяет в случае необходимости сконфигурировать иной механизм атаки посредством замены, либо доработки отдельных компонентов средства мониторинга, а также установки дополнительных модулей и т.д.

3.5 Описание функциональности АИС

На рисунке 14 представлено окно настройки сценария сканирования трафика.

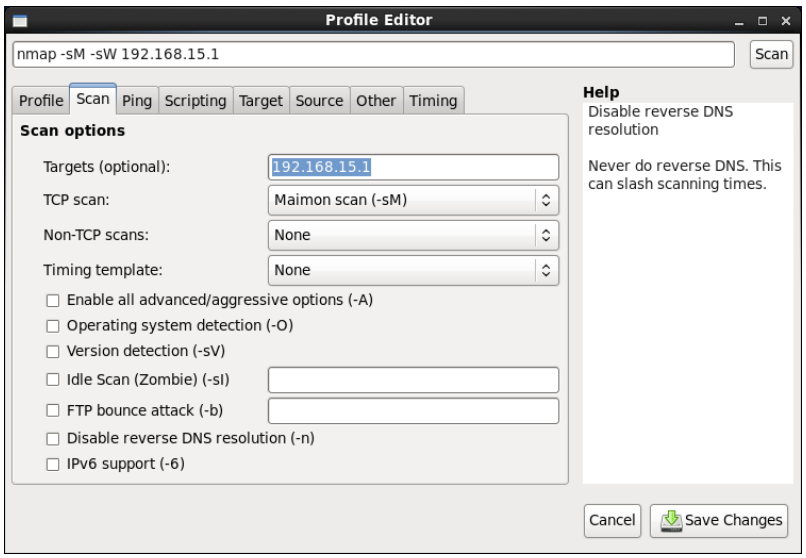

Рисунок 14 – Окно настройки сценария сканирования трафика

Работа данного скрипта заключается в том, что при попытке сканирования сети появляется предупреждение в логе notice (по умолчанию он находится в каталоге с датой в /var/opt/bro/logs/) и производится запись в журнале событий как показано на рисунке 15.

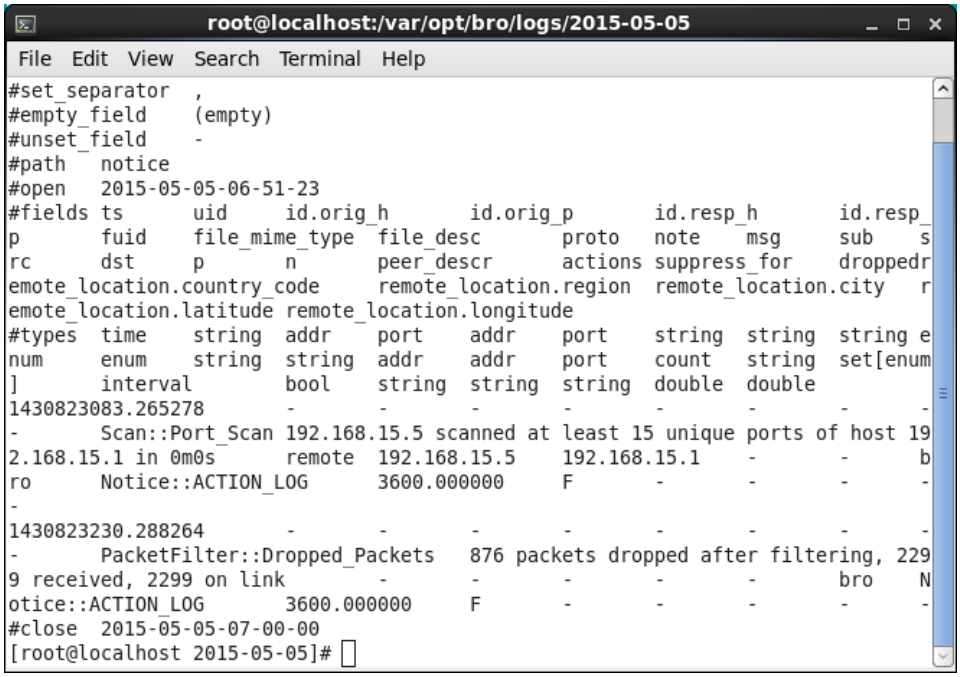

Рисунок 15 – Запись в журнале событий о сканировании сети

Платформа построена таким образом, что в случае нагрузки часть пакетов отбрасывается — это позволяет избежать перегрузки.

Помимо предложенной системы мониторинга защиты был реализован собственный программный продукт, осуществляющий анализ текущего состояния установленных аппаратных средств защиты – видеокамер, а также компонентов СКУД.

Принцип работы программного продукта довольно простой – формируется таблица с перечнем оборудования, в которой указывается наименование, описание расположения, IP-адрес и состояние. Программой выполняется проверка доступности оборудования по IP-адресу посредством команды Ping, после чего оборудование, которое доступно по сети, подсвечивается зеленым цветом (рисунок 16). В случае, если оборудование недоступно, оно будет подсвечено красным цветом (рисунок 17). Код программы представлен в приложении Б.

Рисунок 16 – Окно программного продукта. Все оборудование из перечня доступно

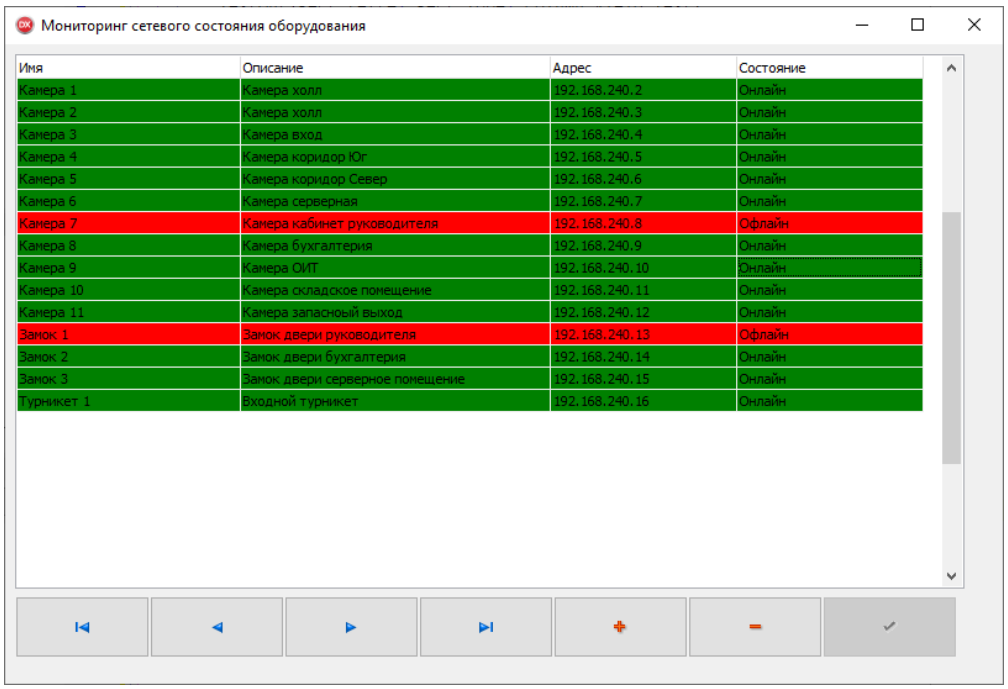

Рисунок 17 – Окно программного продукта. Отображение не активного оборудования

На основании реализованных систем будет достигнуто совершенствование уже имеющихся механизмов обеспечения информационной безопасности, что снизит риски возникновения нештатных ситуаций и вероятность финансовых потерь в результате реализации угроз информационной безопасности.

3.6 Оценка и обоснование экономической эффективности разработки системы защиты

Независимо от затрагиваемой в рамках проекта автоматизации сферы жизнедеятельности, любая из них сейчас является довольно зависимой от использования персональных компьютеров и оргтехники с целью автоматизации самых различных процессов. Для того, чтобы произвести оценку уровня эффективности, получаемой в результате использования данных средств автоматизации, возможно использование нескольких,

существенно отличающихся друг от друга, показателей. На основании данных показателей могут быть отображены такие значения, как уровень прагматической эффективности, технической, эксплуатационной, социальной и экономической эффективности. Выполняя оценку получаемой в результате внедрения автоматизированного варианта решения задачи эффективности, к числу показателей уровня эффективности чаще всего относят:

- показатель, демонстрирующий степень достоверности информации, с учетом проводимых с ней процедур по её обработке, преобразованию и передаче;
- показатель, демонстрирующий уровень защиты информации в рамках автоматизированного варианта решения задачи или комплекса задач;
- показатель, демонстрирующий степень точности в обработке данных или в выполняемых расчетах;
- показатель, демонстрирующий объем выводимых в рамках отчетной документации данных, с учетом требований пользователей;
- показатель, отражающий степень быстродействия программного продукта.

Говоря об уровне технической эффективности проекта, необходимо отметить, что данного рода показатели демонстрируют степень полученных улучшений в области технического совершенствования системы в целом и автоматизируемого процесса в частности. Также осуществляется оценка текущего уровня технической оснащенности организации и функционирования средств автоматизации и информационных систем в рамках предприятия в целом, и автоматизируемого бизнес-процесса в частности [4].

Помимо технической эффективности существует также уровень надежности, который, как следует из названия, демонстрирует, насколько надежной является информационная система. В состав данного показателя

также может быть включена степень функциональности программы, количество использующих её пользователей, уровень производительности ИС и т.д.

Также при оценке эффекта могут быть использованы обобщающие показатели эффективности, которые на основании собственных критериев могут отобразить насколько эффективной является информационная система. К данным показателям относятся:

- показатель, отображающий годовой экономический эффект, получаемый в результате использования информационной системы;
- показатель, демонстрирующий экономический эффект в отношении к капитальным вложениям на реализацию и/или внедрение информационной системы;
- показатели, отображающие изменения в трудоемкости операций по обработке информации до и после внедрения информационной системы;
- показатель, демонстрирующий уровень трат на обработку информации;
- показатель, отображаемый степень экономии финансовых средств в результате автоматизации процесса обработки информации и т.д. [18].

Говоря о годовом экономическом эффекте, следует учесть, что данный показатель зависит от результата внедрения и последующей эксплуатации программного обеспечения. Чаще всего данный показатель выражается в некоторой стоимостной форме, которая отражает либо увеличение прибыли организации, либо наоборот снижение затрат по определенным статьям расходов, получаемые в результате автоматизации деятельности вследствие внедрения информационной системы [9].

С целью расчета срока окупаемости внедряемой информационной системы должны быть рассчитаны показатели экономической

эффективности, а перед этим определен уровень затрат на реализацию и внедрение программного продукта. Для проведения указанного расчета был выполнен сбор основных данных, представленных в таблице 2.

Таблица 2 – Данные для расчета себестоимости

Наименование показателя	Единицы измерения	Обозначение	Значение
Норма амортизации компьютера	%	H_A	15
Стоимость компьютера	руб.	$C_к$	28000
Стоимость 1 кВт электроэнергии	руб.	$C_{кв}$	4,32
Мощность компьютера	кВт/ч	$M_к$	0,75
Ставка программиста	руб.	$C_{пр}$	35000
Норма отчислений на дополнительную заработную плату	%	$H_{доп}$	60
Фонд рабочего времени в год	ч	$Ф_в$	1981

Расчёт показателя, демонстрирующего уровень затрат на организацию одного машинного часа работы, выполняется на основании формулы (1).

$$\mathrm{С_{м/ч}} = \mathrm{АМ_ч} + \mathrm{С_{эл}} \quad (1)$$

где $C_{м/ч}$ – показатель, демонстрирующий уровень стоимости одного машинного часа работы, выраженный в рублях;

$AM_к$ – показатель амортизации используемого персонального компьютера за один машинный час работы, выраженный в рублях;

$C_{эл}$ – показатель, демонстрирующий стоимость электроэнергии, требуемой для обеспечения одного часа работы персонального компьютера, выраженный в рублях.

Для получения показателя, демонстрирующего уровень амортизации персонального компьютера, применяется формула (2).

$$\mathrm{А_{М_к}} = \frac{\mathrm{С_к} * \mathrm{Н_а}}{\Ф_в * 100\%}, \quad (2)$$

где $С_к$ – цена персонального компьютера в руб;

$Н_А$ – показатель, отображающий норму амортизации используемого персонального компьютера;

$Ф_в$ – фонд рабочего времени в год, ч.

Применив формулу (2) получим значение амортизации используемого персонального компьютера: $\mathrm{А_{М_к}} = \frac{1700 * 15\%}{1981 * 100\%} = 2{,}1$ р.

Для расчета уровня трат на обеспечение одного часа работы компьютера используется формула (3).

$$\mathrm{С_{эл}} = \mathrm{М_к} + \mathrm{С_{кв}} \quad (3)$$

где $М_к$ – мощность персонального компьютера, кВт/ч;

$С_{кв}$ – цена одного киловатт-часа электроэнергии в рублях.

Использую формулу (3) получим: $\mathrm{С_{эл}} = 0{,}75 + 4{,}32 = 3{,}24.$

Все полученные показатели подставляем в формулу (1), получаем: $\mathrm{С_{м/ч}} = 3{,}24 + 2{,}1 = 5{,}34.$

Для получения значения трат, которые потребуются при осуществлении оплаты труда, используется формула (4).

$$\mathrm{С_{тр}} = (\mathrm{З_{пр}} + \mathrm{отч}) * \mathrm{Т_н} \quad (4)$$

где $З_{пр}$ – часовая заработная плата разработчика;

Отч – отчисления с заработной платы, выраженные в процентах;

$Т_н$ – время, требуемое на реализацию программного продукта. Причем в рамках реализуемого продукта время, требуемое на написание программного продукта в полном объеме, соответствует времени работы персонального компьютера.

Для расчета часовой заработной платы разработчика используется формула (5).

$$З_{пр} = \frac{Ст_{пр}}{Ф_{вм}}, \quad (5)$$

где $Ст_{пр}$ – оклад разработчика в рублях;

$Ф_{вм}$ – фонд рабочего времени в месяц, ч.

Подставив в данную формулу исходные значения, получим часовую заработную плату разработчика: $З_{пр} = \frac{35000}{165} = 212\text{ р. }10\text{ к.}$

Расчет дополнительной заработной платы разработчика осуществляется на основании формулы (6).

$$З_{пр} = \frac{З_{пр} * Н_{доп}}{100\%}, \quad (6)$$

где $З_{пр}$ – основная заработная плата разработчика в рублях;

$Н_{доп}$ – показатель, демонстрирующий уровень отчисление от основной заработной платы на дополнительную плату.

Используя формулу (6) выполним расчет уровня дополнительной заработной платы разработчика: $З_{пр} = \frac{212{,}1 * 60\%}{100\%} = 127\text{ р. }30\text{ к.}$

Уровень общей заработной платы вычисляется на основании формулы (7).

$$З_{общ} = З_{пр} + З_{доп} \quad (7)$$

где $З_{общ}$ – общая заработная плата разработчика, выраженная в рублях.

Используя формулу (7), получим значение общей заработной платы: $З_{общ} = 212{,}1 + 127{,}3 = 339\text{ р. }40\text{ к.}$

Следующим шагом будет выполнен расчет отчислений на социальное страхование, фонд занятости и пенсионный фонд. Для этого используется формула (8).

$$\text{Отч} = \left(\text{О}_{\text{сс}} + \text{О}_{\text{фз}} + \text{О}_{\text{пф}}\right) * \text{З}_{\text{общ}} \quad (8)$$

где $O_{сс}$ – отчисления на социальное страхование, равное 2,9% от общей заработной платы;

$O_{фз}$ – отчисления в фонд медицинского страхования, равные 5,1% от общей заработной платы;

$O_{пф}$ – отчисления в пенсионный фонд, равные 22% от общей заработной платы.

Расчет перечисленных выше отчислений выполнен ниже:

$$\text{Отч} = (2{,}9\% + 5{,}1\% + 22\%) * 339{,}4 = 101\ \text{р.}\ 82\ \text{к.}$$

Собрав воедино все полученные значений, выполним расчет итогового значений показателей трат по оплате труда разработчика: $\text{С}_{\text{тр}} = (339{,}4 + 101{,}82) * 40 = 17648\ \text{р.}\ 80\ \text{к.}$

Последним шагом расчета стоимостных показателей реализации проекта выполняется расчет себестоимости программного продукта. Для этого используется формула (9).

$$\text{С}_{\text{пр}} = \text{С}_{\text{м/ч}} * \text{Т}_{\text{н}} + \text{С}_{\text{тр}} \quad (9)$$

где $C_{м/ч}$ – стоимость машинного часа работы, руб;

$T_{н}$ – время на реализацию программного продукта;

$C_{тр}$ – уровень затрат на оплату труда разработчика программного продукта.

На основании формулы (9) получим значение себестоимости программного продукта: $\text{С}_{\text{пр}} = 5{,}34 * 40 + 17648{,}8 = 17862\ \text{р.}\ 40\ \text{к.}$

Заключение

Развитие персональных компьютеров и вычислительных сетей привело не только к росту их функционала и возможностей, но и стало причиной появления большого числа проблем, в особенности связанных с информационной безопасности. Обеспечение защиты данных всегда решалась по-разному, поэтому как в рамках компьютерных сетей и сетей передачи данных, так и в принципе при реализации защиты информации в масштабах любого современного предприятия также применяется большое число методов и средств.

Использование большого числа инструментов при обработке и передаче данных только актуализировало проблемы обеспечения защиты данных и вывело их на более высокий уровень, так как развитие техники привело и к развитию инструментов получения несанкционированного доступа к данным. На текущий момент времени можно выделить внушительный перечень угроз информационной безопасности, направленных на кражу, хищение, модификацию, либо уничтожение информации. Независимо от направления угрозы, её успешная реализация может привести к возникновению существенного ущерба. При этом важно помнить, что наиболее важной классификацией угроз будет являться их подразделение на внутренние и внешние. Внутренние угрозы исходят от сотрудников организации, а внешние – от внешних факторов.

Большой состав методик по обеспечению защиты информации могут быть направлены в большом числе различных направлений защиты – защищать данные от кражи, удаления, модификации и т.д. На основании того факта, какие средства использованы с целью их реализации, все средства защиты могут быть подразделены на программный, аппаратные, физические и нормативно-правовые. На основании требований и подходов при реализации системы защиты информации могут быть использованы как собственные разработки, так и готовые решений от сторонних разработчиков

и производителей. А для обеспечения максимального эффекта чаще всего одновременно применятся несколько видов защиты, чтобы формируемая система защиты получилась комплексной.

Большое количество реализованных систем защиты демонстрирует максимальный уровень эффективности при построении систем защиты информации при сочетании правовых, организационных и технических мер защиты. При обеспечении указанного сочетания средств защиты главное определить степень конфиденциальности защищаемых данных, степень опасности, а также наличие уже имеющихся в организации средств защиты. Как правило, состав технических средств обеспечения информационной безопасности в общей сумме составляет лишь незначительную часть в отношении правовых и организационных мер защиты, однако важно подобрать их в максимальном соответствии с требованиями по защиты данных в организации.

В результате выполнения работы была достигнута поставленная цель – осуществлена разработка системы безопасности для АНПОО «Учебно-курсовой комбинат».

Для достижения поставленной цели были решены следующие задачи:

- рассмотрены основные вопросы обеспечения информационной безопасности, методы и средства защиты информации;
- выполнен анализ деятельности организации;
- осуществлен выбор состава оборудования для реализации системы защиты;
- реализованы проектные решения для модернизации средств защиты информации.

Список используемой литературы

1 ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий = Ч. 1. Введение и общая модель : [Текст]. - Взамен ГОСТ Р ИСО/МЭК 15408-1-2008 ; введен 2013-12-01. – М. : Стандартинформ, 2014. - V, 50 с.; 29 см.

2 ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий = Ч. 2. [Текст]. - Взамен ГОСТ Р ИСО/МЭК 15408-2-2008 : введен 2014-09-01. – М. : Стандартинформ, 2014. - V, 155, [1] с.; 29 см.

3 ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий = Ч. 3. Компоненты доверия к безопасности [Текст]. - Взамен ГОСТ Р ИСО/МЭК 15408-32008 : введен 2014-09-01. – М. : Стандартинформ, 2014. - V, 145, [1] с.; 29 см.

4 Баранова, Е. К. Информационная безопасность и защита информации [Текст] : учеб. пособие / Е. К. Баранова, А.В. Бабаш. - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. - ISBN 978-5-369-01450-9

5 Бондарев, В. В. Введение в информационную безопасность автоматизированных систем [Текст] : учеб. пособие / В. В. Бондарев. - М. : Издательство МГТУ им. Н. Э. Баума- на, 2016. - 250 с. - ISBN 978-5-7038-4414-4.

6 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с.

7 Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с.

8 Гришина Н. В. Организация комплексной системы защиты информации [Текст] / Н.В. Гришина. - М. : Гелиос АРВ, 2017. - 256 с. - ISBN 978-5-85438-171-0.

9 Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Текст] : учеб. пособие для студентов высших учебных заведений, обучающихся по специальностям 090103 "Организация и технология защиты информации", 090104 "Комплексная защита объектов информатизации" направления подготовки "Информационная безопасность" / Ю. Н. Загинайлов. - Барнаул : Изд-во АлтГТУ, 2015. - 252 с. - ISBN 978-5-7568-0867-4.

10 Информационные технологии, телекоммуникации и системы управления : международная конференция студентов, аспирантов и молодых ученых (3; 2017; Москва) : Международная конференция студентов, аспирантов и молодых ученых "Информационные технологии, телекоммуникации и системы управления" [Текст] : [в рамках форума молодых ученых "ИТ: глобальные вызовы и новые решения"] : сборник докладов / [Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Институт радиоэлектроники и информационных технологий - РТФ]. – М. :Эдитус, 2017. - 286 с. - ISBN 978-5-00058-522-1

11 Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Текст] : учеб. пособие для студентов высших учебных заведений, обучающихся по специальностям 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М. В. Мецатунян. – М. : Форум, 2014. - 255 с. - ISBN 978-5-91134-856-4.

12 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с.

13 Ковалев, П. Д. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов юридических специальностей / П. Д. Ковалев, Д. П. Ковалев. - Южно-Сахалинск : Южно-Сахалинский ин-т экономики, права и информатики, 2016. - 112 с.

14 "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 11.06.2022). // СПС «КонсультантПлюс». [Электронный ресурс]. Интернет-ресурс. URL: http://www.consultant.ru/document/cons_doc_LAW_34661/

15 Кузнецов, И. Н. Бизнес-безопасность [Текст] / И. Н. Кузнецов. - 4-е изд. – М. : Дашков и К°, 2016. - 416 с. - ISBN 978-5-394-02654-6.

16 Лапина, М. А. Информационное право [Текст] : учеб. пособие для студентов высших учебных заведений, обучающихся по специальности 021100 "Юриспруденция" / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; под ред. И. Ш. Килясханова. – М. : ЮНИТИ : Закон и право, 2012. - 335 с. - ISBN 5-238-00798-1.

17 Лапонина, О. Р. Криптографические основы безопасности [Текст] : учеб. Пособие / О. Р. Лапонина. - М. : НОУ "Интуит", 2016. – 242 с. - ISBN 978-5-9556-0102-1.

18 Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 6-е изд., стер. – М. : Академия, 2012. - 330 с. - ISBN 978-5-7695-9222-5.

19 Мэйволд, Э. Безопасность сетей : [самоучитель] / Эрик Мэйволд ; [пер. с англ.: Г. Г. Трубникова]. – М. : СП ЭКОМ : Бином. Лаб. знаний, 2005 (Ульяновск : Ульяновский Дом печати). - 527 с. - ISBN 5-9570-0046-9.

20 Нестеров, С. А. Основы информационной безопасности [Текст] : учеб. пособие / С. А. Нестеров. – СПб. : Лань, 2017. - 321 с. - ISBN 978-5-8114-2290-6.

21 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с.

22 Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности [Текст] : учеб. пособие для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 "Информационной безопасность" / Ю. А. Родичев. - СПб. : Питер, 2017. - 254 с. - ISBN 978-5-496-02434-1.

23 Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации [Текст] :федер. Закон [Принят Гос. Думой 8 июля 2006 года : Одобрен Советом Федерации 14 июля 2006 года]. – М. : Инфра- М, 2006. - 16 с.; 20 см. - (Федеральный закон; Вып. 38 (364)).; ISBN 5-16-002879-X.

24 Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - Электрон. текстовые данные. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 424 с. - Режим доступа: http://www.iprbookshop.ru/52161.html.— ЭБС «IPRbooks».

25 Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 02.08.2020) / «Российская газета», N 256, 31.12.2001.

26 Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 09.11.2020) "О безопасности". // СПС «КонсультантПлюс». [Электронный ресурс]. Интернет-ресурс. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=367298

27 Федеральный закон РФ "О государственной тайне" от 21.07.1993 N 5485-1. // СПС «КонсультантПлюс». [Электронный ресурс]. Интернет-ресурс. URL: http://www.consultant.ru/document/cons_doc_LAW_2481/

28 Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ. // СПС «КонсультантПлюс». [Электронный ресурс]. Интернет-ресурс. URL: http://www.consultant.ru/document/cons_doc_LAW_48699/

29 Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. // СПС «КонсультантПлюс». [Электронный ресурс]. Интернет-ресурс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/

30 Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ. // СПС «КонсультантПлюс». [Электронный ресурс]. Интернет-ресурс. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/

Приложение А

Конфигурационные файлы реализованного средства обнаружения вторжений

```
yandex.ru. IN SOA spruce.threeroomco.com.
(2002043004 ; serial (последовательный номер)
3600       ; refresh (обновление)
600        ; retry (повторное обращение)
604800     ; expire (срок действия)
86400      ; default_ttl (время жизни)
)
google.com. IN A     192.168.1.1
birch                IN A     192.168.1.2
spruce               IN A     192.168.1.3
fsb.ru. IN A     192.168.1.4
www IN CNAME gingko
kelp IN CNAME jacques.pangaea.edu.
@ IN MX    10 birch.threeroomco.com.
@ IN MX    20 mail.pangaea.edu.
@ IN NS    spruce.threeroomco.com.
# <...>
## Загружаем модули предупреждения и статистики
@load base/frameworks/notice
@load base/frameworks/sumstats
# <...>
## Экспортируемые переменные и константы
export {
   # <...>
   ## Для обнаружения неудачных попыток соединения с тем или иным
```

портом эти попытки должны укладываться в заданный интервал времени.

Если этот интервал будет избыточным, могут происходить ложные срабатывания. Переопределяемый

```
const port_scan_interval = 5min &redef;
# <...>
```

Пороговое количество уникальных портов на одном хосте, после превышения которого в заданном интервале времени должно происходить обнаружение сканирования

```
const port_scan_threshold = 15.0 &redef;
# <...>
}
event bro_init() &priority=5
{
# <...>
```

При запуске Bro мы создаем преобразователь данных (Reducer), уменьшающий объем данных, поставляемый в потоке наблюдения (observation stream) под именем scan.port.fail. Reducer в данном случае выбирает исключительно уникальные попытки, причем выбор зависит от порогового количества уникальных портов

```
local r2: SumStats::Reducer = [$stream="scan.port.fail",
$apply=set(SumStats::UNIQUE),
$unique_max=double_to_count(port_scan_threshold+2)];
```

Создаем также общую статистику с порогом, после превышения которого вызывается колбэк-функция, производящая определенные действия — в данном случае формирующая уведомление о том, что за определенное время ($epoch) порог сканирования уникальных портов был кем-то превышен

```
SumStats::create([$name="port-scan", ## Имя общей статистики
$epoch=port_scan_interval, ## Интервал времени, в течение
```

которого будет собираться статистика. По его истечении она сбрасывается

$reducers=set(r2), ## Набор преобразователей, которые используются для создания общей статистики

$threshold_val(key: SumStats::key, result: SumStats::Result) = ## Предоставляет функцию, которая считает некую величину, необходимую для внутреннего измерения пороговой величины

{

return result["scan.port.fail"]$unique+0.0;

},

$threshold=port_scan_threshold, ## Пороговая величина, по достижении которой вызывается колбэк-функция

$threshold_crossed(key: SumStats::key, result: SumStats::Result) = ## Наконец, определяем колбэк-функцию, срабатывающую по достижении порога

{

local r = result["scan.port.fail"];

local side = Site::is_local_addr(key$host) ? "local" : "remote"; ## Устанавливаем, откуда идет сканирование — со стороны внешнего мира или же из локальной сети

local dur = duration_to_mins_secs(r$end-r$begin); ## Длительность попыток сканирования

local message = fmt("%s scanned at least %d unique ports of host %s in %s", key$host, r$unique, key$str, dur); ## Формируем сообщение для NOTICE

NOTICE([$note=Port_Scan,

$src=key$host,

$dst=to_addr(key$str),

$sub=side, ## Нужно для политики предупреждений

$msg=message,

```
                $identifier=cat(key$host)]); ## Вызываем обертку из фреймворка Notice, которая затем вызывает внутреннюю функцию, что в конечном счете приводит к появлению предупреждения
                }]);
        }
        ## Функция, вызываемая для получения потока наблюдения (observation stream)
        function add_sumstats(id: conn_id, reverse: bool)
          {
          local scanner = id$orig_h; ## Хост, с которого производится соединение
          local victim = id$resp_h; ## Хост, к которому подключаются
          local scanned_port = resp_p; ## Порт назначения
          # <...>
          if ( hook Scan::port_scan_policy(scanner, victim, scanned_port) ) ## Если срабатывает данный хук (а он, судя по всему, должен срабатывать практически всегда), мы фиксируем данные в наблюдении. Первый параметр — имя наблюдения, второй — ключ, ну а третий — собственно собираемые данные
            SumStats::observe("scan.port.fail", [$host=scanner, $str=cat(victim)], [$str=cat(scanned_port)]);
          }
        # <...>
        event connection_attempt(c: connection)
          {
          local is_reverse_scan = F;
          if ( "H" in c$history )
            is_reverse_scan = T;
```

```
    ## Вызов функции сбора общей статистики
    add_sumstats(c$id, is_reverse_scan);
    }
# <...>
```

Приложение Б

Исходный код системы мониторинга оборудования видеонаблюдения и сигнализации

```
unit Unit1;
interface
uses
  Winapi.Windows, Winapi.Messages, System.SysUtils, System.Variants, System.Classes, Vcl.Graphics,
  Vcl.Controls, Vcl.Forms, Vcl.Dialogs, Data.DB, Vcl.ExtCtrls, Vcl.DBCtrls,
  Vcl.Grids, Vcl.DBGrids, Data.Win.ADODB;

type
  TForm1 = class(TForm)
    ADOTable1: TADOTable;
    ADOConnection1: TADOConnection;
    DBGrid1: TDBGrid;
    DBNavigator1: TDBNavigator;
    ADOTable1Id: TAutoIncField;
    ADOTable1Имя: TWideStringField;
    ADOTable1Адрес: TWideStringField;
    ADOTable1Описание: TWideStringField;
    ADOTable1Состояние: TWideStringField;
    DataSource1: TDataSource;
    TrayIcon1: TTrayIcon;
    Timer1: TTimer;
    procedure DBGrid1DrawColumnCell(Sender: TObject; const Rect: TRect;
      DataCol: Integer; Column: TColumn; State: TGridDrawState);
```

```
    procedure Timer1Timer(Sender: TObject);
function TForm1.Ping(const AHost : string; const ATimes : integer;
out AvgMS:Double) : Boolean;
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

{$R *.dfm}

function TForm1.Ping(const AHost : string; const ATimes : integer;
out AvgMS:Double) : Boolean;
var
R : array of Cardinal;
i : integer;
begin
Result := True;
AvgMS := 0;
if ATimes>0 then
with TIdIcmpClient.Create(Self) do
try
Host := AHost;
ReceiveTimeout:=999; //TimeOut du ping
```

```
SetLength(R,ATimes);
{Pinguer le client}
for i:=0 to Pred(ATimes) do
begin
try
Ping();
Application.ProcessMessages; //ne bloque pas l'application
R[i] := ReplyStatus.MsRoundTripTime;
except
Result := False;
Exit;

end;
if ReplyStatus.ReplyStatusType<>rsEcho Then result := False; //pas d'écho, on renvoi false.
end;
{Faire une moyenne}
for i:=Low(R) to High(R) do
begin
Application.ProcessMessages;
AvgMS := AvgMS + R[i];
end;
AvgMS := AvgMS / i;
finally
Free;
end;
end;
```

```
procedure TForm1.DBGrid1DrawColumnCell(Sender: TObject; const Rect:
TRect;
  DataCol: Integer; Column: TColumn; State: TGridDrawState);
begin
 if
DBGrid1.DataSource.DataSet.FieldByName('Состояние').AsString='Онлайн'
then
 begin
  with  DBGrid1.Canvas do
  begin
     Brush.Color:=clGreen;
     FillRect(Rect);
     TextOut(Rect.Left+2,Rect.Top+2,Column.Field.Text);
   end;
 end;

  if
DBGrid1.DataSource.DataSet.FieldByName('Состояние').AsString='Офлайн'
then
 begin
  with  DBGrid1.Canvas do
  begin
     Brush.Color:=clRed;
     FillRect(Rect);
     TextOut(Rect.Left+2,Rect.Top+2,Column.Field.Text);
   end;
 end;

end;
```

```
procedure TForm1.Timer1Timer(Sender: TObject);
var ip:string;
begin
DBGrid1.DataSource.DataSet.First;
While not DBGrid1.DataSource.DataSet.eof do begin
Ip:= DBGrid1.DataSource.DataSet.FieldByName('Адрес').AsString ;
if TForm1Ping(Ip, 10, 3) = true then
DBGrid1.DataSource.DataSet.FieldByName('Состояние').AsString:='Онлайн'
else
DBGrid1.DataSource.DataSet.FieldByName('Состояние').AsString:='Офлайн'
DataSet.Next;
end;
end;
end.
```