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)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Методы администрирования безопасности в распределенной КИС

Студент Е. В. Зуев
(И.О. Фамилия) (личная подпись)

Научный руководитель канд. пед. наук Е.А. Ерофеева
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

Тематика использования распределенных информационных систем является актуальной и напрямую связана с тенденцией интеграции к единой информационной централизации орг. структур, как в корпорациях, так и в средних компаниях, что привело к необходимости использования консолидированных информационных систем. Посредством распределения информационных ресурсов, обеспечивается обработка данных, хранимых на разных серверах, различных аппаратных и программных платформах, представленные в разнообразных форматах.

Преимуществом распределенных информационных систем является легкость в расширении, использование всеобщих стандартов и протоколов, обеспечивающие возможность объединения своих ресурсов с другими системами информатики, предоставляющие пользовательские интерфейсы, нужные для выполнения своих обязательств.

В данной работе рассмотрены основные сведения о распределенных информационных системах: описаны истоки их эволюции, проведен анализ функциональных средств для дальнейших работ с ресурсами информации, рассматриваются типы и концепция функционирования распределенных систем.

Цель работы: изучить теоретические аспекты пользования систем и основные принципы работы и их функционала.

Задачи работы:

- описать области пользования систем;
- изучить их классификацию;
- проанализировать программную и аппаратную реализацию распределенных систем.

Объектом исследований выступают: распределенные информационные системы.

Предметом исследований является:

- - проведения анализа программных и аппаратных средств реализации рассматриваемых систем;
- результаты, при помощи которых можно провести анализ методов по администрированию безопасности, используя при этом распределённые корпоративные ИС;
- результаты, при помощи которых можно провести анализ и классифицировать события, которые происходят в системе с точки зрения возможности их вовремя зафиксировать;
- результаты, при помощи которых можно провести анализ методов, которые разработаны для построения реальной системы по администрированию информационной безопасности ИС.

Научная новизна данной работы заключается в том, что был сделан корректный выбор объекта исследования, которым является система по администрированию информационной безопасности, а также в данной работе выполнена классификация событий, которые были установлены в результате наблюдения и разработаны для соответствующих расчётов параметров мониторинга событий информационной безопасности математические модели с учетом соответствующих затрат с экономической точки зрения.

Практическая ценность данной работы заключается в том, что разработаны методы, при помощи которых можно обеспечить полноценное администрирование безопасности, что стало возможным благодаря программному обеспечению. Разработанные методики, при помощи которых можно организовать работу службы по администрированию и обеспечению функциональной информационной безопасности.

1. Теоретические аспекты использования распределенных информационных систем

1.1. Общие характеристики задач, решаемых с использованием распределенных информационных систем

Использование распределенных информационных систем связано с разветвлённостью сетью филиалов. Архитектура схожего рода была широко известна во времена, когда не было разработок централизованных информационных систем, не хватало каналов связи, функционирование было не стабильным, создание и обслуживание требовало значительных вложений и не представлялось экономически целесообразным на тот период.

На рисунке 1 изображена схема принципиальная распределенных баз данных.

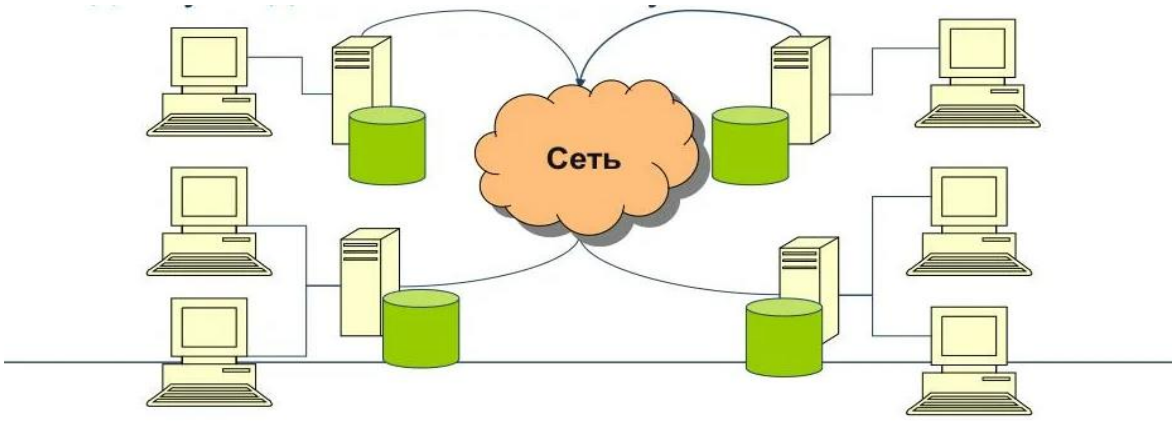

Рисунок 1 – Схема принципиальная распределенных баз данных

Для распределенной архитектуры БД характерны особенности:

- каждый узел системы является самостоятельной единицей и имеет собственную Систему Управления БД (СУБД);
- каждый пользователь независимо от узла, может получить доступ к любому из серверов как в единой базе.

Из недостатков можно отметить сложность администрирования всей системы в целом и в зависимости от сложности коммутации узлов, значительные временные затраты получения информации.

Примеры распространенных систем с распределенной архитектурой:

- электронная почта на платформе Lotus Domino;
- ПО на платформе «1С»: Предприятие; Управление персоналом; Склад; Бухгалтерия и учет; службы на основе каталогов;

Распределенные системы сохраняют данные на серверах, рассредоточенных по нескольким аппаратным платформам. При этом возможны варианты прямого использования через систему распределенных вычислений, либо через систему репликации данных. Во втором случае осуществляется движение информации по периферийным базам и в определенный момент времени отправляются на центральный сервер, с которого получают административные инструкции, обновления классификаторов и др. Подобные системы организации хранения и получения информации связаны с потерей ее актуальности в момент времени, когда производится обмен данными. Период времени обмена данными устанавливается администратором и напрямую зависит от аппаратных средств реализации, а так же архитектуры создания распределенной системы как единого комплекса автоматизации и управления данными.

Функции распределенной архитектуры включают:

- консолидация данных в территориально распределенных сетях;
- использование различных программных и аппаратных платформ;
- организация управлением общего доступа пользователей к каждому из сегментов системы;
- централизованное администрирование территориально удаленных участков It-инфраструктуры как единого комплекса.

С потоками данных, циркулирующими в распределенных системах, возможно проводить консолидацию, с дальнейшей отработкой запросов.

Архитектура систем реализует возможность работы, как с файл-серверными, так и с клиент-серверными системами.

Распределенные системы с клиент-серверной архитектурой обеспечивают работу с большим разнообразием типов прикладных программ, Web-приложений, мобильных приложений. Серверные ресурсы реализуют репликацию данных, представляемых как в форме сегментов базы данных, так и файлов документации различных типов. Обеспечивается возможность организации защиты информации на уровне СУБД, на уровне приложений и анализа протоколов работы системы. Распределенная архитектура системы обеспечивает распределенную загрузку вычислительной техники, так как запросы пользователей производятся не к одному, а к множеству серверам, что обеспечивает необходимый уровень производительности приложений.

Недостатком является необходимость дополнительных работ в администрировании приложений, связанные с настройкой обмена данными и устранение конфликта данных при репликациях. Данный фактор напрямую влияет на уровень подготовки специалистов администрирования систем и требует более высокой степени подготовки .

Функционал распределенной архитектуры информационных систем обеспечивает возможность подключения неограниченного количества баз данных, являющихся сегментами систем, которые интегрируются в один единый комплекс.

На сегодняшний день разнообразие рынка создает конкуренцию и развитие информационных технологий, но в свою очередь порождает возможность интеграции разного рода систем и зачастую реализация единого формата обмена данными без дополнительных манипуляций просто невозможен. Во многих сферах отсутствие дополнительной информации лишает объективного вывода информации что лишает возможности проведения машинного анализа в принципе и приводит к субъективным решениям.

Основные требования при организации распределенных БД:

- директивное установление правил функционирования;

- определение единого формата данных при проведении репликаций.

Реализация подобных информационных систем необходима в случаях, когда проводится централизация организационной структуры компании и технологические процессы предполагают необходимость работы с консолидированными данными. При этом в единой информационной базе устанавливается разграничение доступа, соответствующее функциональным обязанностям сотрудников.

Также внедрять распределённые ИС можно тогда, когда важно контролировать модификацию данных в тех структурных подразделениях компании, которые работают дистанционно или удалённо.

Для того, чтобы правильно организовать работу распределенных информационных систем, это необходимо сделать в несколько этапов. Первый этап заключается в том, что необходимо проведение специальных подготовительных работ. Для этого важно определить структуру данных такой информационные системы, после чего установить правило, согласно которым данные мигрируют между базами информационных систем, которые входят в них. Важно при этом также определить такие правило, согласно которым будут срабатывать ограничения при любой модификации данных.

Следующий этап предполагает проведение подготовительных работ, связанных с повышением функциональности распределенной информационной системы. В таком случае необходимо выбрать такое программное обеспечение, которое будет оптимальным для проведения организации работы информационной базы, которая является распределенной и работает по соответствующим правилам, определение которых выполнено в результате того, что правильно проведены подготовительные работы. Здесь же необходимо сконфигурировать программный продукт, который выбран для того, чтобы организовать и

полноценно обеспечить эффективность управления распределенными информационными системами.

1.2. Обзор средства работы с распределенными данными

Далее определим перечень требований к инструментарию автоматизации работы с распределенными системами. При проектировании систем, имеющих подобную архитектуру, необходимо учитывать: специфику используемых операционных систем, поддерживаемые технологии обмена данными и архитектуру защиты информации.

Рассмотрим наиболее часто используемые методы управления данными в распределенных информационных системах.

Фрагментация и дублирование

В рамках данного метода производится разделение таблиц с информацией на сегменты, между которыми проводится обмен данными (репликации). Данный способ используется, когда использование единой базы предполагает работу с таблицами большого объема и обращение к ним приводит к снижению производительности клиентских приложений. Таким образом, разделение таблиц на сегменты сокращает нагрузку на серверы, так как физическое расположение таблиц разделено по различным аппаратным платформам, при этом в каждом из сегментов вычисления производятся с высокой производительностью, так как каждый из сегментов имеет меньший объем.

Использование словарей данных и директорий

Административные настройки форматов обмена данных хранятся в специализированных таблицах, словарях данных. Также для решения задач, связанных с обменом информацией, требует наличия данных, используемых для хранения адресной информации о территориально распределенных серверах, используемых на них СУБД.

Технологии журналирования изменений данных

Использование данных технологий предполагает настройку правил обмена данными при проведении движений в сегментах базы данных (так как в данном случае по каналам связи передается на вся актуализированная информация, а лишь проведенные изменения в сегментах баз). При этом необходимо обеспечить логическую целостность баз, возможность отработки конфликтов при репликациях.

Технологии обеспечения целостности данных

Данная технология позволяет проводить оперативную настройку отправки данных во все связанные таблицы при изменениях ключевых реквизитов.

1.3 Организация использования распределенных систем

Проведем описание основных подходов к организации использования распределенных систем:

- на центральном сервере проводится создание эталонных образов баз данных
- средствами СУБД проводится настройка форматов обмена данными между узлами распределенной сети
- устанавливается периодичность обмена данными.
- при необходимости – создание древовидной архитектуры, предполагающей создание подчиненных серверов второго, третьего уровня и др.

Схема древовидной архитектуры распределенной базы данных приведена на рисунке 2.

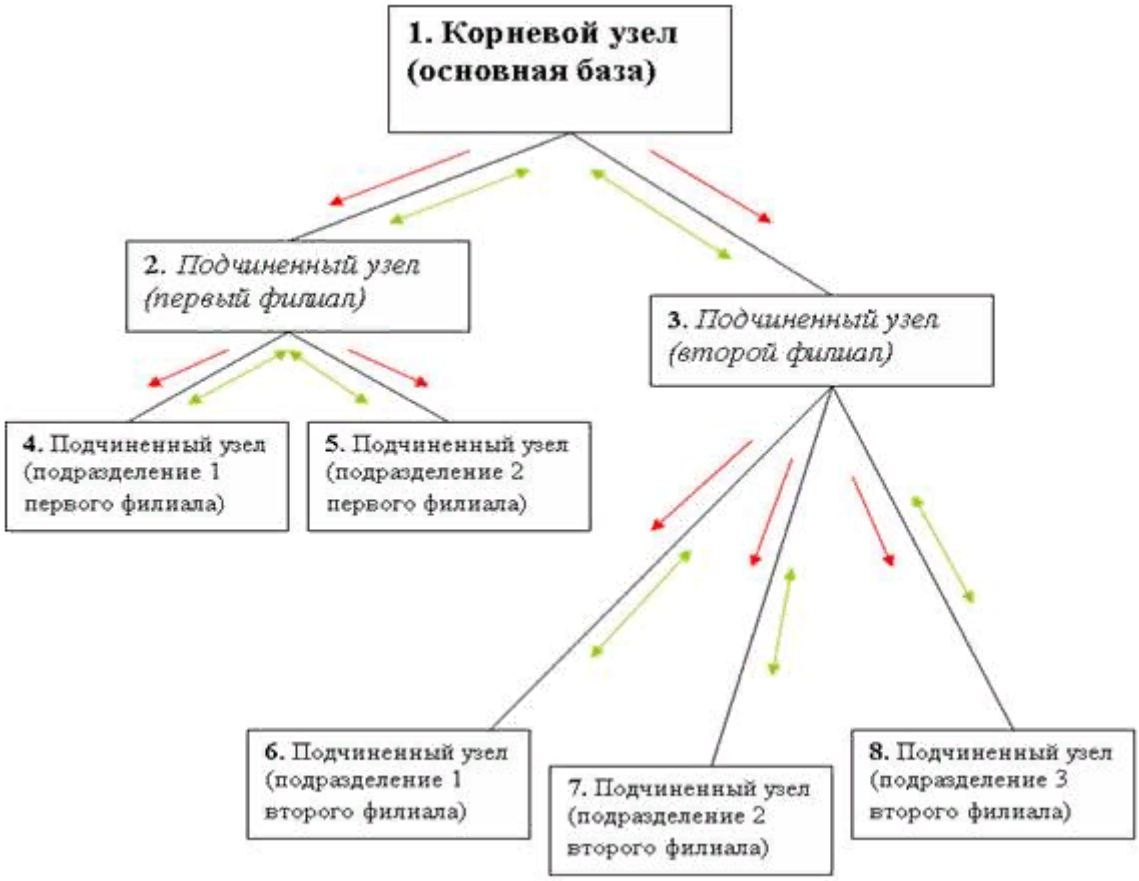

Рисунок 1 – Древовидная архитектура распределенной БД

В данном примере узел 1 представляет собой корневой сервер, на котором проводится настройка обмена данными и проводится слияние сегментов БД.

Узел 1 получает обновления с серверов, установленных в узлах 2 и 3. Для серверов, установленных в узлах 4 и 5 корневым является сервер, установленный в узле 2. Для серверов, установленных в узлах 6, 7 и 8 корневым является сервер, установленный в узле 3.

Каждый из серверов, входящий в древовидную распределенную сеть, осуществляет обмен данными с подчиненными и одним вышестоящим сервером в соответствии с настроенными правилами. Права на управление сегментами древовидной сети определяются аналогично – администратор сервера может управлять только подчиненными серверами. Изменения,

проведенные на вышестоящем сервере, применяются только к нижестоящим серверам.

Порядок обмена информацией в распределенных базах данных включает [5]:

- в базе-источнике формируется список изменённых объектов за период после проведения репликации;
- формирование пакета в формате XML, в который входит информация по движению данных;
- временное закрытие доступа на запись к измененным объектам на период выгрузки;
- отправка файла с выгрузки на вышестоящий узел;
- запись изменений из полученных пакетов выгрузки данных;
- блокировка записи на время записи данных из полученных пакетов.

2. Программная и аппаратная реализация распределенных вычислений

2.1 Классификация кластерных вычислений

Далее рассмотрим задачи, к решению которых оптимально подходят алгоритмы кластерных вычислений.

Реализация кластеров контейнеров возможна с помощью настроек размещения в компоненте, который отвечает за работу контейнера и проводить задание их размеров.

Процесс создания кластера контейнеров предполагает:

- подготовку, при которой необходимо убедиться во включении кластеров в поддерживаемом развертывании;
- проверку наличия необходимых прав.

При настройке кластеров в компоненте контейнеров автоматически производится подготовка указанного числа контейнеров. Далее проводится равномерное распределение запросов между всеми контейнерами в кластере.

Можно изменять размер кластера таким образом, чтобы было возможно добавление или удаление какого-либо из подготовленных контейнеров или приложений в данном кластере. В процессе изменения размера кластера в среде исполнения необходимо учитывать работу всех связанных фильтров и правил размещения.

Необходимо также отметить, что Open Source-система Kubernetes, которая необходима для того, чтобы решать соответствующие задания по обеспечению высокой эффективного управления контейнерами кластерами. Её появление было связано с разработками, которые происходили в компании Гугл на протяжении 10 лет, когда осуществлялась эксплуатация специальные технологии, дающий возможность изолировать процессы виртуальной среде. Её называют Borg.

Технология Kubernetes в настоящее время считается очень выгодной платформой для того, чтобы можно было выполнять оркестрацию

контейнеров. С помощью можно осуществлять управление кластерами виртуальных машин, а также можно обеспечить руководство Linux контейнерами в качестве единой платформы. На сегодняшний день она лидирует в области таких разработок, которые применяются для того, чтобы можно было внедрять соответствующие платформы для компаний среднего и крупного бизнеса.

При этом Kubernetes предназначена для того, чтобы выстраивать эффективную систему, позволяющую распределять контейнеры по узлам кластеров. Это всё зависит от того, какие параметры в текущие нагрузки и соответствуют ли потребности необходимой работе сервисов. С её помощью можно обеспечивать обслуживания большого количества хостов одновременно, а также отслеживать их состоянии, контролировать совместную работу и обеспечивать репликации с проведения масштабирования, а также балансировать параметры нагрузки.

На протяжении трех месяцев поступают обновление этой системы. Улучшается программное обеспечение главным образом для того, чтобы развивать систему защиты, а также увеличивать объёмы применяемые данных и обеспечивать их масштабируемость.

Вторым крупным игроком на рынке систем по оркестрации контейнеров является система Docker Swarm. Данное решение, разработанное в 2013 г., значительно упростило процесс развертывания полноценных виртуальных систем. По сути, с данного момента стало возможным осуществлять обновление совместно с значительным количеством вычислительных мощностей. При этом можно запускать большое количество приложений, которые изолированы друг от друга с выстраивание нужной конфигурации из виртуализировать данных прикладных систем, что можно делать при этом очень быстро.

Технология по обеспечению контейнерной кластеризации, которая называется Docker Swarm, появилась позже, чем сама платформа. Но

используя её, можно решить при этом задачи, которые связаны с объединением докер хостов в общий виртуальный хост.

Такая платформа совместима с Docker API. Поэтому пользователи, которые использовали инструменты данные платформы, могут применять контейнерные кластеры, управление которых осуществляется при помощи в данной системы. Можно при этом использовать большое количество Docker-контейнеров.

Технология Swarm интересна в первую очередь представителям малых и средних предприятий, объем запуска задач в которых не более 60 тыс. контейнеров и до 1500 нод. Благодаря там, что она автоматически совместима с Docker,

Разработчики заинтересовались данной платформой, поскольку это позволяет развивать бизнес-модели, которые дают возможность наращивать облачное присутствие. При этом существенную поддержку оказываетMicrosoft Azure, которая также поддерживает платформу Swarm.

На сегодняшний день данная технология в условиях современного рынка пока не является сильно популярной, в отличие от Kubernetes, и корпоративный рынок последнюю платформу существенно поддерживает. При этом большинство Swarm выступает в качестве основного механизма для того, чтобы обеспечивать будущую облачную стратегию развития.

Третьим основным игроком на рынке кластеризации контейнером является система Apache Mesos. Её основными положительными моментами является отказоустойчивость, которая также является централизованной и используется для того, чтобы управлять кластерами. С её помощью можно выполнять объединение отдельных узлов в группы согласно необходимым требованиям, что впоследствии даёт возможность обеспечивать им изоляцию от остальных информационных ресурсов и управлять системой полноценно.

Суть работы Такой системы заключается в том, что она является обратной модели виртуализации. Если использовать традиционный подход, при котором необходимо раздробить вычислительные среды, включающие

большое количество физических машин, на их виртуальные копии. При этом им необходимо предоставить свою квоту из общих ресурсов ЦОДа. данная система оказывает обратное явление, объединяя при этом соответствующие объекты в Единый виртуальный ресурс. При этом образовываются большие кластеры и увеличивается эффективность системы управления инфраструктурой серверов с Выдели для каждого кластера индивидуального пула ресурсов.

Подходы Mesos позволяют значительно упрощать процедуры по развертыванию и управлению, проводить перемещение приложений, запущенных в контейнерах, с одного места на другое, быстро переходить в публичное облако.

Разработчиками Windows до недавнего времени предлагались следующие технологии виртуализации: виртуальные машины и виртуальные приложения Server App-V. Каждая из них имеет работает в своем сегменте, обладает своими достоинствами и недостатками. В настоящее время ассортимент расширился — в Windows Server 2016 включены контейнеры (Windows Server Containers). Основным отличием является то, что в системе предложены следующие виды контейнеров: контейнеры Windows и контейнеры Hyper-V. В TP3 были доступны только первые.

Если использовать контейнеры семейства Hyper-V, то с их помощью можно получить дополнительные уровни, которые связанные с изоляцией. При этом происходит выделение собственного ядра каждому из контейнеров, а параллельно выделяются соответствующие ресурсы памяти. Ты это изоляция исполняет гипервизор данного семейства, а не ядро. Это приведет к тому, что можно будет достичь аналогичного уровня изоляции, которые существуют в виртуальных машинах, но затраты при этом будут существенно ниже, чем при виртуализации, но они будут уступать контейнером Windows. Для возможности использования такого типа контейнеров необходима установка на хосте роли Hyper-V. Контейнеры Windows по большей части подходят для применения в доверенных средах,

например когда на серверах производится запуск приложений от одной организации. Когда сервер используется множеством компаний и необходимо обеспечивать больший уровень изоляции, использование контейнеров Hyper-V, вероятнее, будут более рациональным решением.

Важной особенностью контейнеров в Win 2016 является то, что выбор типа проводится не в момент создания, а в моменты деплоя. То есть запуск любого контейнера может производиться как Windows, и как Hyper-V.

2.2. Реализация распределенной архитектуры информационной системы в БД Lotus Domino

Одним из примеров использования распределенной архитектуры данных является корпоративная почтовая система Lotus, включающая следующие сегменты:

- работа с почтовыми сообщениями;
- управление корпоративной документацией;
- работа со специализированными форумами;
- управление системой консолидации отчетности с использованием встроенных средств обработки табличных данных.

Lotus Domino (как серверная часть) и Notes (как клиентская часть) представляет собой систему распределенных баз, к которым возможно предоставление доступа сотрудникам в соответствии с их функциональными обязанностями, в которую встроены сервисы корпоративной электронной почты, а также система обмена мгновенными сообщениями.

В силу того, что БД Lotus – документно-ориентированная, а в работе корпораций возможно использование значительного количества документов, для обеспечения необходимых характеристик производительности целесообразно использовать распределенную архитектуру.

При этом отчетность, формируемая в табличных сервисах Lotus в территориальных узлах, может автоматически отправляться на вышестоящие узлы и далее формировать консолидированные сведения как в разрезе компании полностью, так и по подразделениям.

Системы, основанные на технологиях Lotus, обеспечивают возможности автоматизации документооборота на уровнях [4]:

- структурных подразделений представительств компаний;
- компании в целом;
- системы коммуникаций компании с внешними контрагентами.

На рисунке 3 приведена схема архитектуры БД Lotus.

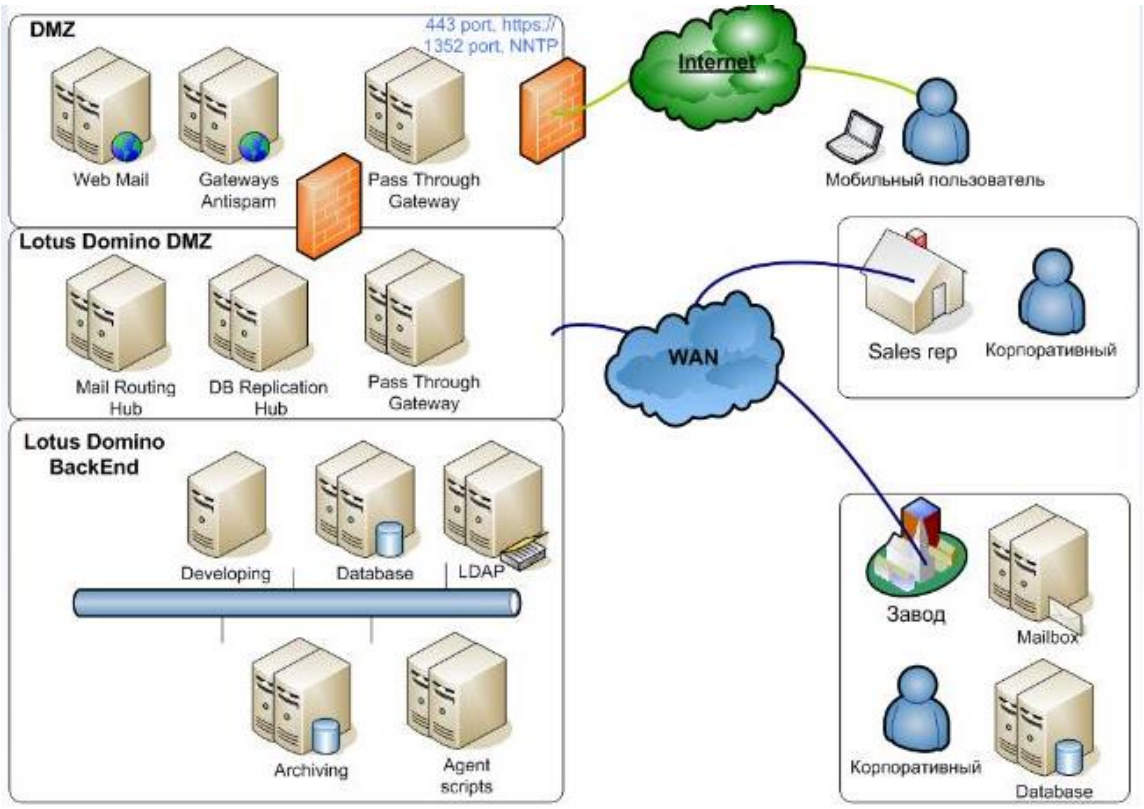

Рисунок 2 – Архитектура распределенной БД Lotus

Как показано на рисунке 3, сегменты распределенной БД Lotus включают уровень конечных пользователей, баз данных промежуточного и

верхнего уровней, распределенные почтовые сервисы. Далее рассмотрим особенности обеспечения защиты информации при передаче данных средствами Lotus.

Компоненты для мониторинга и блокировки конфиденциальных данных, передаваемой через коммуникационные каналы, могут представлять собой аппаратуру с установленным программным обеспечением, посредством которого обеспечивается выполнение соответствующих функций мониторинга состояния защиты от утечек конфиденциальных данных.

Подсистема сканирования уязвимостей используется для поиска расположения информационных ресурсов с конфиденциальными данными. Посредством указанного модуля производятся операции, связанные со сканированием файловых ресурсов, СУБД и других видов хранилищ информации. По результатам сканирование осуществляется формирование отчета по каждому узлу. Кроме этого, если провести настройку политики сканирования, имеются возможности резервирования ресурсов с конфиденциальной информацией в выделенную защищённую область, которая может представлять собой выделенный на сервере ресурс, к которому проведена установка прав доступа в соответствии с требованиями защиты информации. Это позволит усовершенствовать процесс управления защищаемыми ресурсами, а также повысить эффективность работы с защищаемыми ресурсами.

С использованием сетевого модуля проводится мониторинг исходящего трафика корпоративной сети, что позволяет специалистам по информационной безопасности выявлять активность пользователей на внешних ресурсах, анализировать правомерность отправки той или иной информации за пределы сети предприятия. При необходимости, в случае обнаружения отправки конфиденциальной информации модуль позволяет заблокировать данный процесс.

Клиентская часть данного ПО позволяет [7]:

- осуществлять резервное копирование или перемещение ресурсов, содержащих конфиденциальные сведения, на выбранный внешний носитель;
- работать с буфером обмена;
- осуществлять поиск конфиденциальных данных на локальных ресурсах рабочих станций;
- осуществлять копирование скриншотов работы пользователей на выделенный ресурс;
- мониторинг активности и протоколирование действий пользователей при работе с ресурсами, определенными в настройках программы;
- установка разрешений на печать документов определенного типа с протоколированием и возможности блокировки вывода на принтер.

Функционал систем класса DLP включает [10]:

- категорирование данных, используемых в работе информационной системы по уровню конфиденциальности с возможностью учета ссылок на их расположение;
- анализ уровня защищенности файловых ресурсов, содержащих конфиденциальные данные;
- мониторинг изменений защищаемых файловых ресурсов и учет данных пользователей, которые вносят изменения.
- обеспечение защиты файловых ресурсов в соответствии с заданными политиками безопасности (может включать управление правами доступа, мониторинг активности, блокировку, резервирование, использование системы оповещений).

Механизмы обеспечения защиты конфиденциальных данных, реализованные в системах класса DLP, включают [19]:

- мониторинг каналов связи и анализ передаваемого входящего и

исходящего трафика;

- проведение подробного анализа передаваемой по сети информации;
- механизмы защиты конфиденциальных данных в системах класса DLP предполагают работу на уровнях: Data-in-Motion, Data-at-Rest, Data-in-Use.

Data-in-Motion – уровень данных, передаваемых по сетевым каналам, включающий технологии [8]:

- Web – трафик с использованием протоколов HTTP / HTTPS;
- трафик Интернет-месседжеров;
- трафик электронной почты по протоколам IMAP, SMTP, POP и пр.;
- трафик беспроводных сетей;
- анализ передаваемых данных по FTP.

Data-at-Rest – анализ данных, хранящихся на уровнях рабочих станций пользователей, серверов, сетевых хранилищах и др.

Data-in-Use – уровень данных, обрабатываемых в процессе работы с прикладными системами.

Защита от утечек информации обеспечивается посредством организационных и технологических решений. Используемые инструменты определяются уровнем конфиденциальности сведений в соответствии с присвоенной категорией:

- секретные сведения;
- конфиденциальные сведения;
- информация для служебного использования;
- общедоступные данные.

После категорирования данных определяется перечень аппаратных средств, посредством которых обеспечивается необходимый уровень защиты от утечек.

Обеспечение эффективной защиты возможно при использовании

проактивных модулей защиты (DLP-системы), реактивных модулей (работающих с архивом событий), а также административных компонент, посредством которых возможен учет событий, связанных с защитой информации в системе.

Посредством проактивных технологий проводится анализ потоков информации и блокировка / протоколирование фактов, связанных с попытками передачи защищаемых данных.

С помощью реактивных модулей обеспечиваются возможности протоколирования и архивации сведений при обнаружении фактов утечек информации за пределы корпоративной сети или несанкционированного копирования на неучтенные носители. Также имеются возможности работы с журналом событий, включая проведение выборок по пользователям, типам событий, времени фиксации.

Функционал, связанный с контролем активности пользователей, позволяет вести мониторинг и оперативно реагировать на попытки несанкционированной передачи или копирования информации.

Функционал, связанный с управлением системой, предполагает проведение настроек мониторинга, учет защищаемых ресурсов, критериев обнаружения инцидентов информационной безопасности.

Программное обеспечение класса DLP, обеспечивает возможности точного сравнения данных, работу с шаблонами ключевых фраз, организацию файлового хранилища для помещения в карантин данных, подозрительных на наличие в передаваемой информации защищаемых ресурсов.

Рассмотрим принципы классификации DLP-систем.

Для внедрения того или иного решения класса DLP необходимо обеспечить его максимальное соответствие системной архитектуре предприятия. Системы класса DLP классифицируются на активные, пассивные и комбинированные.

В пассивных DLP-системах анализ событий происходит постфактум,

отсутствуют возможности своевременного блокирования событий, но при этом имеется полный набор инструментов анализа протоколов с выводом полной информации об инциденте.

Использование данного типа систем эффективно, когда более важно определение источника утечки информации, чем проведение блокировки активности злоумышленника. Системы проводят анализ аккаунтов в системах электронной почты, мессенджерах, используют снифферы, анализаторы трафика.

Системы копируют сообщения в специальный архив и далее проводят полный анализ их атрибутов (дата, отправитель, получатель, контент, характер передаваемого сообщения, уровень конфиденциальности).

В активных DLP-системах реализован сервис блокировки данных при обнаружении признаков утечки. В настройках системы определяется критерий отнесения данных к запрещенным для передачи. Весь трафик, выходящий за пределы локальной сети компании, проходит через анализатор, который имеет возможности контроля и фильтрации. Недостаток использования системы – замедление работы приложений, работающих с внешними Интернет-ресурсами, а также недостаточный набор инструментов для анализа трафика.

Для обучения сотрудников работе защищаемой информацией в некоторых DLP-системах возможна настройка работы с уведомлениями, которые отсылаются пользователям при попытке передачи запрещенных данных.

Комбинированные DLP-системы востребованы в случаях, когда нужен одновременно и подробный анализ трафика и своевременная блокировка передачи данных. В данном случае активная часть системы проводит фильтрацию трафика, подозрительного на наличие передачи запрещённых данных, пассивный компонент проводит анализ с формированием отчета для администратора о обнаружении признаков утечки конфиденциальных данных. На рисунке 4 приведена архитектура комбинированной DLP-

системы.

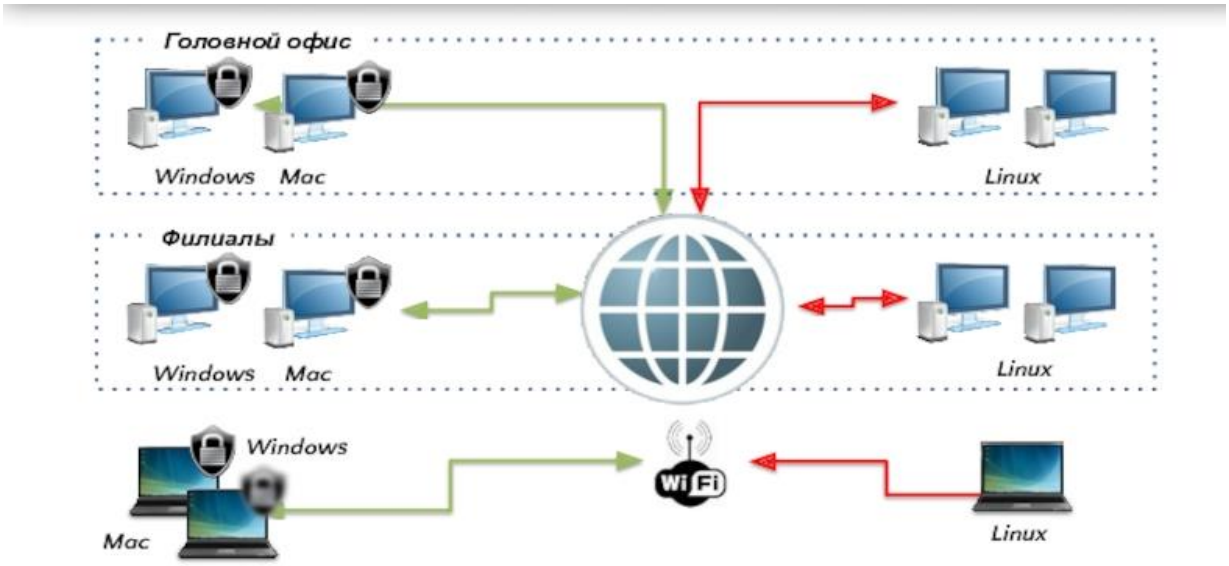

Рисунок 3 – Схема архитектуры комбинированной DLP-системы

Работа систем DLP включает использование алгоритмов выявления прецедентов утечки информации различного вида: вероятностных, детерминистских, комбинированных.

Вероятностные алгоритмы производят лингвистический анализ передаваемых данных, сканируют их «цифровые отпечатки». Алгоритмы в данном случае не требуют значительных вычислительных мощностей, но при этом результат анализа не гарантирует полноты проведения анализа трафика по признакам утечки конфиденциальной информации.

Использование детерминированного подхода (анализ меток файлов), обеспечивает надежность выявления признаков утечки информации, при этом данные алгоритмы не обладают достаточным уровнем гибкости. Посредством комбинированных алгоритмов возможно проведение анализа среды хранения информационных ресурсов и мониторинга процесса обработки данных, что обеспечивает возможности получения оптимального эффекта при выявлении фактов утечки информации и соблюдения требований к защищенности при хранении данных.

При анализе данных в DLP-системах используются алгоритмы контекстного и лингвистического анализа, работы с цифровыми отпечатками,

сопоставления файловых ресурсов с шаблонными, работы с регулярными выражениями и словарями. Работа с шаблонами и словарями эффективна в некоторых областях, например, при контроле платежных реквизитов, номеров документов и идентификаторов другого вида [17].

При использовании контекстных и лингвистических алгоритмов проводится построение статистических отчетов, анализируются морфологические признаки содержимого передаваемых файлов, анализируется контекст, категория получателя данных. Указанный алгоритм является эффективным при работе с для динамическими данными. При работе с цифровыми отпечатками проводится анализ атрибутов файлов, информации о времени создания, владельце, версии, контрольной сумме.

Настройка активных DLP-систем предполагает, что весь исходящий трафик проходит через модуль анализа, который осуществляет поиск признаков запрета на передачу контента с использованием алгоритмов [20]:

- анализа сигнатур через поиск в массиве данных признаков запрещенной информации например, по наличию текста, внесенного в специальный словарь, с которым проводится сверка;
- лингвистические алгоритмы работают с словоформами, проводят анализ всего потока текста (через расчет уровня встречаемости определенных слов);
- работа с цифровыми отпечатками предполагает контрольных сумм передаваемых файлов;
- использование регулярных выражений предполагает возможности поиска схожих шаблонов и форматов передаваемых данных (например, при передаче СНИЛС, ИНН, платежных реквизитов);
- метки - установка на файлы, содержащие конфиденциальную информацию, специальных «меток»;
- алгоритмы искусственного интеллекта в DLP-системах обеспечивают возможности обучения системы в целях выявления

объектов, имеющих признаки передачи конфиденциальных сведений.

Схема контроля трафика с помощью DLP-системы показана на рисунке 5.

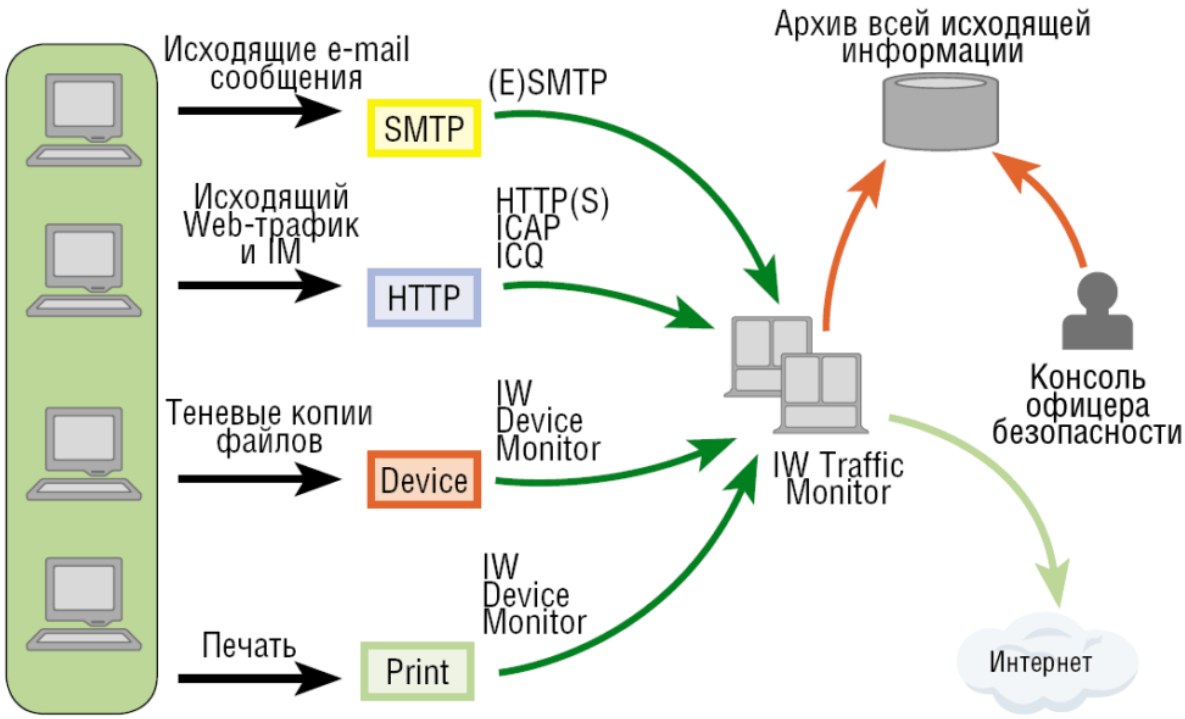

Рисунок 4 - Схема контроля трафика с помощью DLP-системы

На рисунке 6 приведена схема архитектуры DLP-системы.

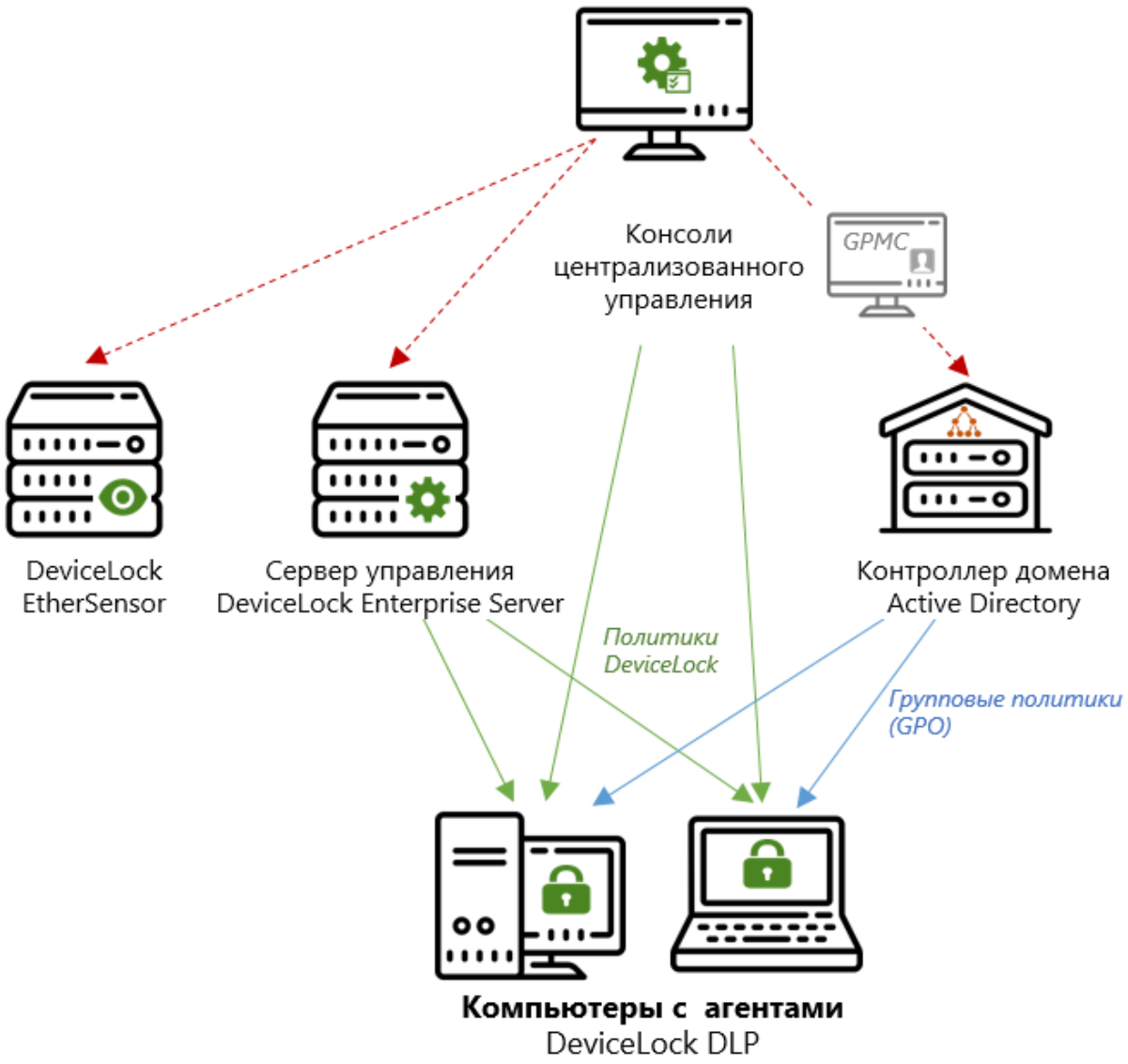

Рисунок 5 – Схема архитектуры DLP-системы

Метод стоп-слов предполагает вычисления количество выявленных в потоке данных последовательностей символов, внесенных администратором в словарь, содержащий признаки конфиденциальности. При превышении определенного порога частоты трафик приобретает признак подозрения на наличие запрещенного контента.

Выводы по разделу

Рассмотрев технологию обеспечения защиты распределенных систем на платформе Lotus, было показано, что на каждом из сервером в древовидной архитектуре эффективно использовать систему класса DLP, которая осуществляет анализ проходящего через систему трафика.

3. Описание методов администрирования распределенных систем в условиях ООО «Вектор»

3.1 Общая характеристика ООО «Вектор»

Объектом исследования в рамках данной выпускной квалификационной работы является сеть магазинов ООО «Вектор». Приведем общую характеристику организации.

Профилем деятельности торговой сети является оптовая и розничная реализация электроники, мобильных телефонов и аксессуаров. Схема организационной структуры ООО «Вектор» показана на рисунке 5.

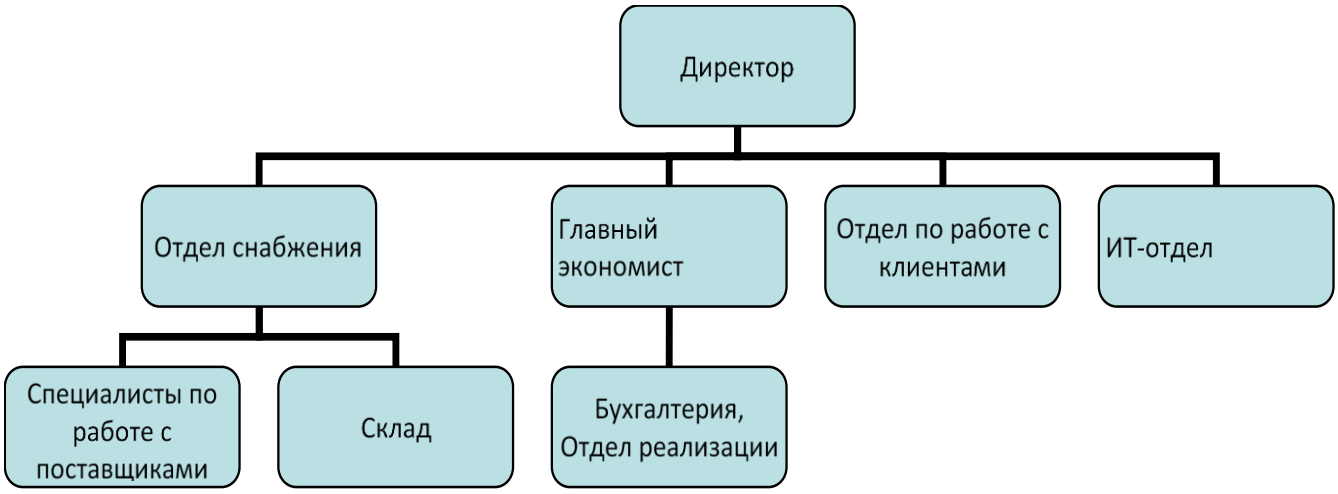

Рисунок 6 - Схема организационной структуры ООО «Вектор»

В настоящее время в ООО «Вектор» наблюдается рост продаж, темпы которого в последние годы замедлились, что связано с растущим уровнем конкуренции на рынке электроники, падением уровня платёжеспособного спроса. Таким образом, в ООО «Вектор» актуальны вопросы получения конкурентных преимуществ в целях увеличения торговых оборотов и развития бизнеса компании.

К основным преимуществам компании относятся:

- современное серверное оборудование;

- широкий ассортимент продукции;
- наличие гибкой системы оплаты реализуемых товаров;
- высокое качество реализуемой продукции;
- наличие партнерских программ с торговыми сетями и производителями мобильных телефонов и аксессуаров;
- заключенные договоры прямых поставок продукции с производителями мобильных телефонов и аксессуаров, что позволяет снижать стоимость продукции.

В настоящее время в связи с невозможностью достоверного прогнозирования объемов продаж мобильных телефонов и аксессуаров, их стоимости перед ООО «Вектор» возникает ряд угроз, связанных с нестабильностью объемов продаж.

Возможности сохранения и развития бизнеса ООО «Вектор» связаны с возможностью расширения взаимодействия с поставщиками (производителями мобильных телефонов и аксессуаров путем заключения договоров об объемах поставок и их графика) и с потребителями.

Проведение аудита информационной безопасности ООО «Вектор» позволит обеспечить стабильность функционирования ИТ-инфраструктуры компании, сократить уровень рисков, связанных с доступностью информационных ресурсов, а также утечек конфиденциальной информации.

На уровне предприятий деятельность по обеспечению защиты информации курируют либо специальные подразделения, либо специалисты, входящие в ИТ-подразделение компании.

В подразделениях по защите информации выделяются следующие направления деятельности:

- специалисты по организационному и документационному обеспечению защиты информации;
- специалисты по обеспечению охранной деятельности и физической защиты информации;
- специалисты по антивирусной защите;

- администраторы безопасности программных комплексов, курирующие вопросы разграничения полномочий пользователей, парольную защиту, обеспечение мер по резервному копированию информационных ресурсов;
- специалисты по криптографической защите информации.

Организационные меры информационной безопасности предполагают принятие мер по защите информации от нарушителей следующих типов:

- сотрудники организации, халатность которых может иметь негативные последствия для состояния защищенности информации;
- сотрудники организации, злонамеренно осуществляющие определенные действия, направленные на снижение уровня защищенности информации, либо на получение конфиденциальных сведений;
- сотрудники-инсайдеры, работающие на конкурирующие компании, деятельность которых направлена на получение информации, составляющей коммерческую тайну;
- физические лица, не являющиеся сотрудниками организации, осуществляющие деятельность по получению конфиденциальных сведений.

Организационные меры защиты включают комплекс административных, управленческих мероприятий, в соответствии с которыми определяется порядок работы систем по обработке данных, использованию ее ресурсов, деятельности обслуживающего персонала, а также технологии по взаимодействию пользователей с системой таким образом, чтобы минимизировать вероятность реализации угроз безопасности персональных данных (либо максимально снизить размер ущерба при их реализации).

Виды угроз для объектов защиты могут быть разнообразными. Далее приведены примеры некоторых видов угроз, каждой из которых

сопоставляются технологические решения, подкрепленные документационным обеспечением (таблица 1).

Таблица 1 - Типовые угрозы безопасности информации

Угрозы	Технологии защиты	Документационное обеспечение
Осуществление визуального съёма отображаемых данных (в присутствии посторонних лиц в процессе обработки данных)	Блокирование экрана с использованием электронных ключей	Список выделенных помещений
Активность вредоносного ПО	Установка АВЗ	«Инструкция по обеспечению антивирусной защиты»
Сетевые атаки	Криптографическая защита	Журнал настроек криптографического ПО
Аппаратные закладки	Тестирование аппаратных систем	«Акт тестирования устройств на наличие закладок»
Программные закладки	Тестирование программных систем	«Акт тестирования программ на наличие закладок»
Несанкционированное копирование баз данных	Внедрение системы разграничения доступа	Матрицы доступа
Накопление пользовательских данных	Периодическая очистка временных файлов	Инструкция по работе с ПО
Ошибки в ПО	Подготовка данных для разработчиков	«Акт об устранении ошибок»
Ошибочные действия работников	Комплекс защитных мер	«Лист ознакомления пользователей с инструкциями»
Чрезвычайные ситуации	Резервное копирование	«Порядок эвакуации носителей информации при возникновении ЧС»
Компрометация электронной подписи	Вывод из строя скомпрометированных ключей	«Инструкция по генерации ключей электронной подписи», «Инструкция по обеспечению криптографической защиты»
Компрометация паролей	Смена паролей	«Инструкция по обеспечению парольной защиты»

В ходе работы над данным проектом мной было проведено изучение организационной структуры предприятия в области защиты информации.

В таблице 12 показано распределение функций в области защиты информации в ООО «Вектор»

Таблица 2 - Распределение функций в области защиты информации в ООО «Вектор»

Должность	Обязанности	Ответственность
Начальник отдела	Контроль соблюдения требований защиты информации в подразделении	Ответственность за выявленные нарушения в области защиты информации в подразделении
Заместитель директора	Курирует работу комиссии по расследованию инцидентов в области информационной безопасности, утверждение актов проверки по защите информации, Положений, подписание приказов.	Ответственность за состояние защиты информации в компании
Администратор безопасности	Мониторинг состояния защиты информации при работе технических систем, анализ состояния системы защиты от утечек данных, антивирусной защиты, администрирование программ, используемых в деятельности по защите информации, подготовка проектов распорядительных документов в области защиты информации	Ответственность за состояние защиты информации в компании в части технической реализации
Сотрудник компании	Исполнение требований защиты информации на рабочем месте	Ответственность за нарушение требований защиты информации

Таким образом, в условиях ООО «Вектор» создана организационная структура, обеспечивающая выполнение требований информационной безопасности, включающая как специалистов по защите информации, так и ответственных в подразделениях предприятия, что обеспечивает распределение уровней ответственности и эффективность выполнения работ по защите информации.

3.2. Описание объектов защиты

Современные информационные технологии связаны в единое пространство высокотехнологичных и наукоёмких методов управления разработкой коммуникационных сетей с информационными ресурсами и инфраструктурой компании, включающими в себя компоненты [4]:

- по управлению проектированием коммуникационных систем;
- по управлению маркетинговыми технологиями, экономикой и финансами;
- по управлению ИТ-инфраструктурой в условиях ООО «Вектор»;
- по управлению непроизводственной сферой.
- Основными компонентами ИТ-инфраструктуры ООО «Вектор» являются:
- автоматизированная система учета продаж, включающая системы автоматизации торговли и программное обеспечение по поддержке работы терминалов безналичной оплаты, имеющая распределенную архитектуру;
- система управления охранной и пожарной сигнализацией;
- система поддержки деятельности ООО «Вектор» (автоматизация кадрового учета, учета заработной платы и др.), имеющая распределенную архитектуру;
- системы обеспечения функционирования коммуникационных технологий и IP-телефонии.

В рамках данной работы проведен анализ системы защиты информации в корпоративной сети ООО «Вектор». Особенностью его использования является доступ к информационным ресурсам компании со стороны удаленных филиалов, либо со стороны клиентов, которым доступ предоставляется при заключении контрактов на обслуживание. Ресурсы серверного программного обеспечения используют виртуальную среду, так как программное обеспечение и формат баз данных достаточно разнороден,

при этом закупка дополнительного программного обеспечения нецелесообразна. В качестве виртуальных машин используется ПО VMWare.

Далее в рамках данной работы проведен анализ структуры локальной сети ООО «Вектор».

Информационная система исследуемой компании включает:

- Файловый сервер, на котором также развернуты виртуальные машины для работы с прикладными системами (1С: Предприятие и Управление системой антивирусной защиты), а также с файловыми ресурсами;
- Пользовательские компьютеры, объединённые в группы в соответствии с организационной структурой ООО «Вектор».

Система «1С: Предприятие» имеет распределенную архитектуру, центральный сервер которой расположен в головном офисе. Репликации производятся ежедневно в 18-00.

Основные параметры локальной сети организации приведены в таблице 1.

Таблица 3 - Основные параметры локальной сети ООО «Вектор»

№	Характеристика ЛВС	Значение
1	Число портов ЛВС	144
2	Подключения сетевых узлов	45
3	Количество коммутаторов (48 портов)	4
4	Офисная АТС (внутренние / городские линии)	12/65
5	Количество пользовательских компьютеров	40
6	Подключения принтеров, МФУ, других технологических устройств	4
7	Источник бесперебойного питания APC Symetria RM (используются для подключения коммутаторов и серверов)	1

На рисунке 2 приведена принципиальная схема технической архитектуры автоматизированной системы ООО «Вектор».

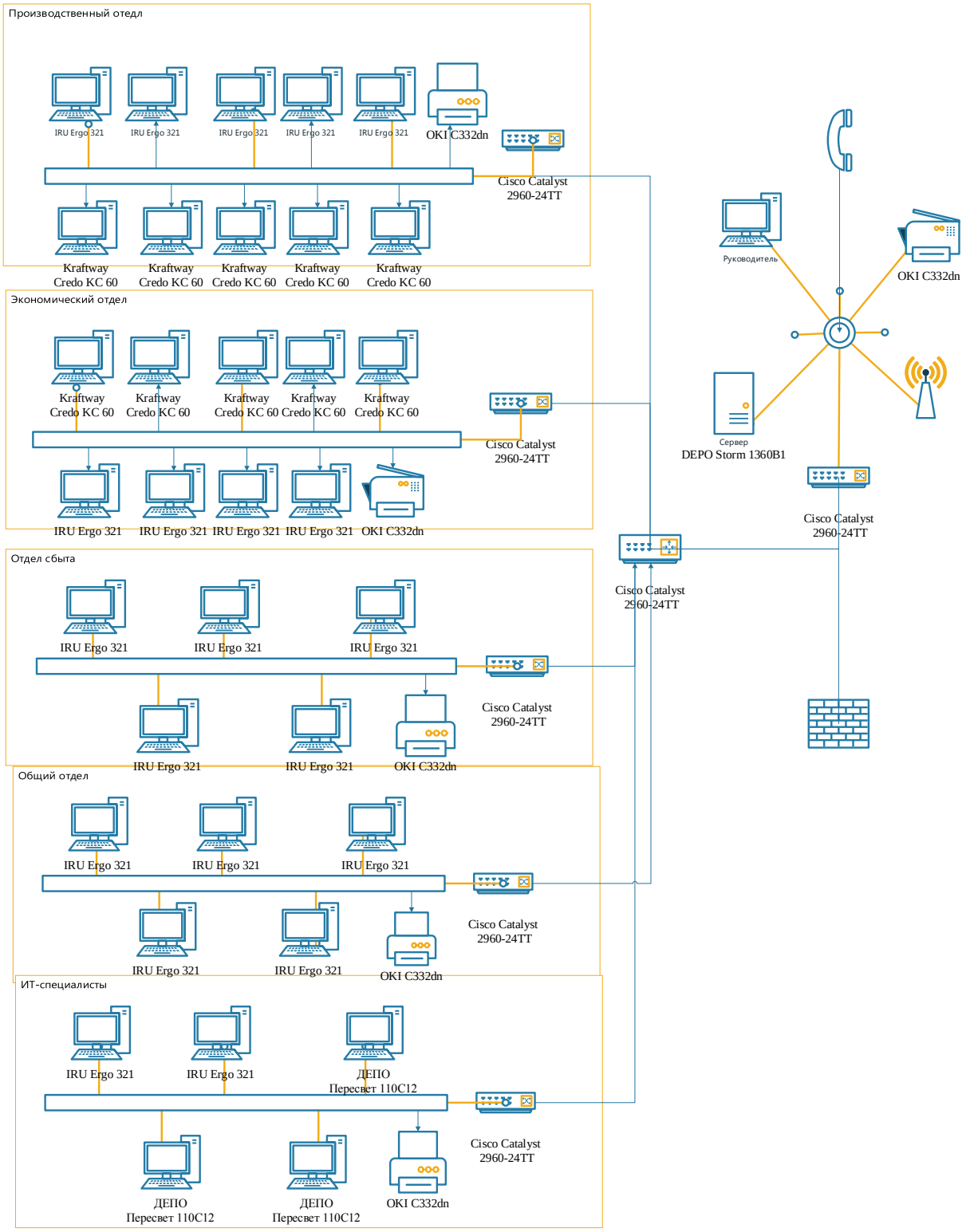

Рисунок 7 - Принципиальная схема технической архитектуры ООО «Вектор»

Технические параметры сервера DEPO Storm 1360B1, используемого в работе специалистов приведена в таблице 2.

Таблица 4 - Технические характеристики сервера DEPO Storm 1360B1

Характеристика	Значение
Процессор	Intel® Core™ i5-4590S, 3000МГц /4-Cores
Оперативная память	2 x 4096MB DDR3ECC DIMM Fully Buffered
HDD	4 x 3 TB SATA3 RAID
Дополнительно	DVD-RW

Таблица 5 - Технические характеристики рабочих станций специалистов

Характеристика	IRU Ergo 321	Kraftway Credo KC 60	ДЕПО Пересвет 110C12
Периферия	Клавиатура, мышь	Клавиатура, мышь	Клавиатура, мышь
Монитор	Acer G226HQLHbd, 21,5', 1920x1080 (16:9), 8мс, LED, 250 кд/м^2	Samsung c24rg50fqi 24, 1920x1080 (16:9), 16мс, LED, 200 кд/м^2	lg 24mp59g-24, 1920x1080 (16:9), 8мс, LED, 250 кд/м^2
Описание	Офисный ПК	Офисный ПК	Офисный ПК
Процессор	**Intel Core i3-2100** Sandy Bridge, 3100 МГц	AMD Ryzen 7 Pinnacle Ridge , 3000 МГц	Intel® Core™ i5, 3200 МГц
Память	4 GB DDR3	4 GB DDR4	4 GB DDR4
HDD	**Samsung** HD502HJ 500Гб	Western Digital WD Blue Desktop 500 GB (WD5000AZLX)	**Samsung** HD502HJ 500Гб
Оптический накопитель	ASUS DRW-24D5MT	Нет	ASUS DRW-24D5MT
Видеосистема	GIGABYTE GeForce GT 730 902Mhz PCI-E 2.0 2048Mb 1800Mhz 64 bit DVI HDMI HDCP	nvidia geforce gt 730	GIGABYTE GeForce GT 710 954MHz PCI-E 2.0 1024MB 5010MHz 64 bit DVI HDMI HDCP Low Profile
LAN	1GB/c	1GB/c	1GB/c
Размеры	~ 415 x 185 x 505мм	~ 420 x 190 x 500мм	~ 420 x 190 x 500мм

На рисунке 3 приведена схема программной архитектуры. В таблице 5 приведен перечень программных продуктов, используемых в технологии работы специалистов ООО «Вектор»

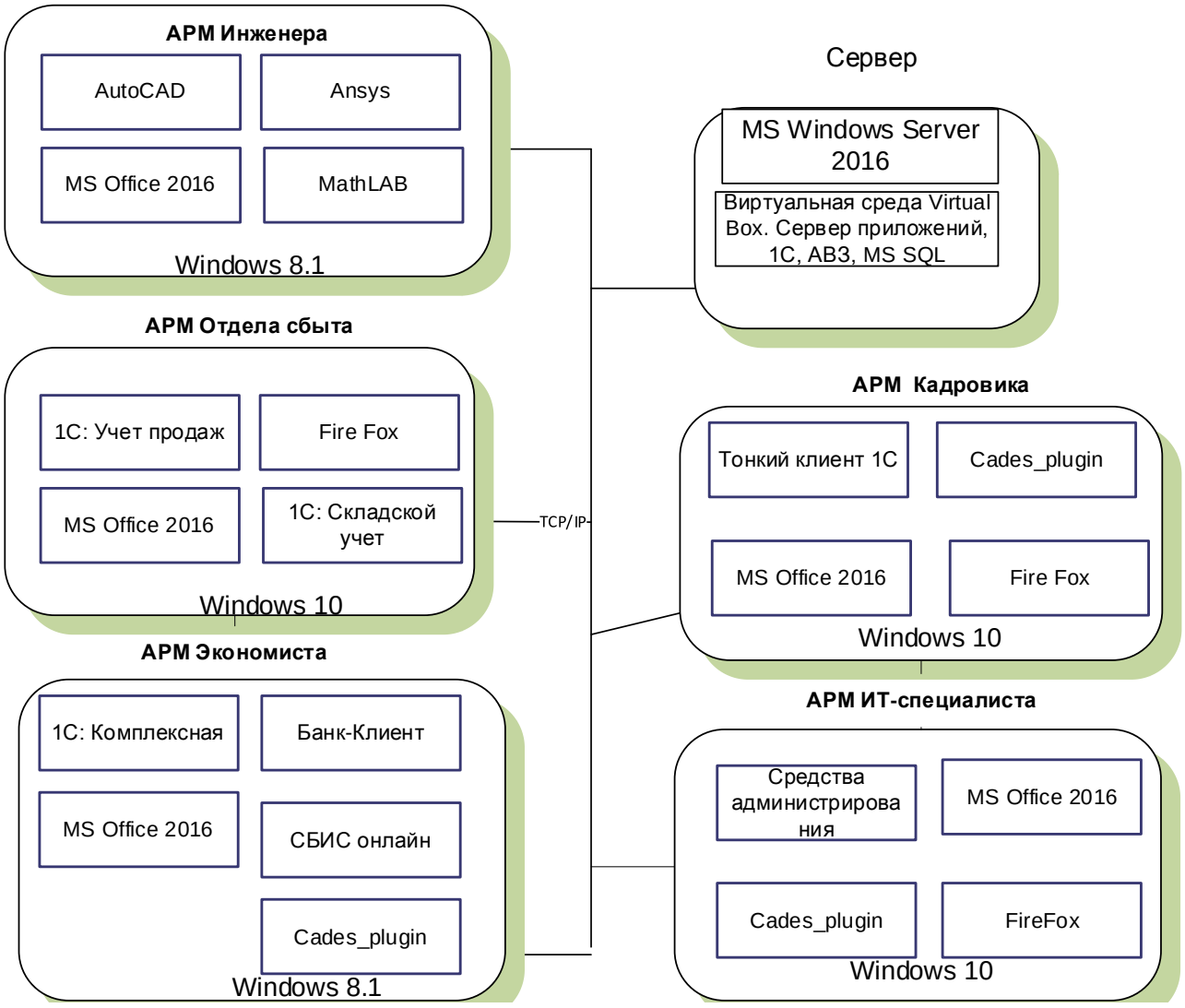

Рисунок 8 – Программная архитектура ООО «Вектор»

Таблица 6 - Перечень программных продуктов, используемых в технологии работы специалистов ООО «Вектор»

Наименование задачи	Технологическое решение	Расположение
АРМ Документооборот	Web-интерфейс	Web-сервер ООО «Вектор»
Учет техники	Тонкий клиент	MS SQL Server
1С 8.2: Бухгалтерский Учет	Тонкий клиент	Сервер 1С:Предприятие
1С 8.2: Комплексная	Тонкий клиент	Сервер 1С:Предприятие
Инженерные разработки	Auto CAD, Ansys, MathLAB	Файловый сервер
Учет договоров	Тонкий клиент	MS SQL Server
Сдача отчетности в ПФР	spu_orb	Рабочие станции специалистов по бухучету
SberSign	Тонкий клиент	Рабочие станции специалистов по бухучету

Таким образом, как показано в таблице 7, информационные ресурсы ООО «Вектор» включают в себя работу как с внутренними ресурсами, так и работу с информационными ресурсами сторонних организаций, что предполагает наличие дополнительных требований к системе информационной безопасности. Вопросы обеспечения информационной безопасности в корпоративной сети ООО «Вектор» курирует ИТ-отдел.

На рисунке 4 показана принципиальная схема распределенной корпоративной сети исследуемой организации. Защита корпоративной сети ООО «Вектор» осуществляется с использованием технологии VPN. Целью создания корпоративной сети является обеспечение доступа к информационным ресурсам компании с удаленных площадок (заводов, расположенных в удаленных регионах).

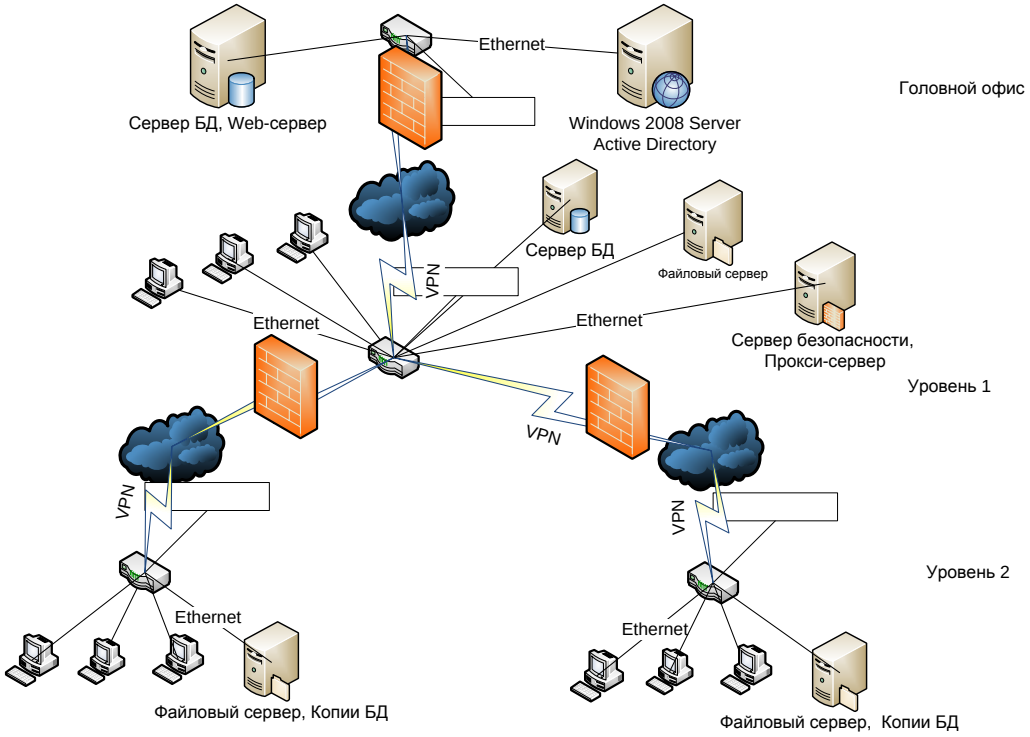

Рисунок 9 - Принципиальная схема распределённой корпоративной сети ООО «Вектор»

Настройка адресации и маршрутизации осуществляется с использованием встроенных средств администрирования, поставляемых с оборудованием маршрутизации.

Для соединения между узлами распределенной сети в условиях используемой компании предполагается использование программного средства OpenVPN, которое используется для защиты сетевых подключений на 2-м и 3-м уровнях OSI.

Схема организации распределённой сети на основе VPN, в условиях исследуемой компании показана на рисунке 11.

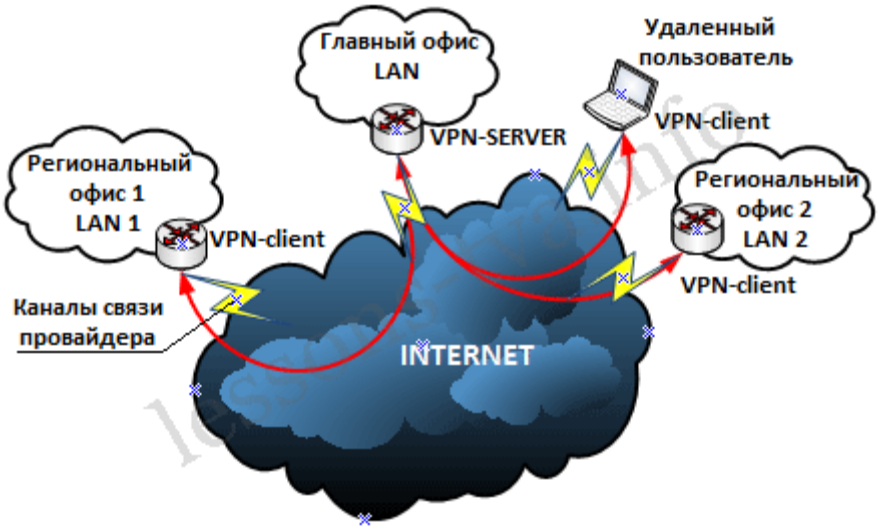

Рисунок 10 - Модель VPN, реализованная в условиях ООО «Вектор»

Конфигурирование защищенных сетевых подключений осуществляется на уровне сервера головного офиса компании. Применение политики безопасности на узлах распределённой сети производится с использованием клиентов VPN, обновление настроек безопасности осуществляется администратором с уровня центрального сервера.

Объектами защиты в распределённых сетях выступают:

- каналы передачи данных;
- головной и промежуточные серверы;
- сетевые узлы, входящие в защищённую сеть;
- аппаратные и программные системы информационной безопасности.

В рамках данной работы мной была проведена оценка объектов защиты информации в автоматизированной системе ООО «Вектор», результаты которой приведены в таблицах 7-8.

Таблица 7 - Объекты защиты информации при обработке данных в автоматизированной системе ООО «Вектор»

Вид информационной системы	Объекты защиты информации
1С: Бухгалтерский Учет	Данные бухгалтерского учета
1С: Складской учет	Персональные данные сотрудников
Ansys, AutoCAD, MATLAB	Инженерные разработки
1С: Зарплата и Управление персоналом	Персональные данные сотрудников
Учет договоров	Коммерчески значимая информация
АРМ Документооборот	Внутриорганизационная информация
Учет техники	Данные автоматизированной системы предприятия
Криптографические системы	Работа с ЭЦП в банковских системах и системах ЭДО

Таблица 8 - Объекты защиты информации при обработке данных неавтоматизированным способом в условиях ООО «Вектор»

Объект	Объекты защиты информации
Карточки сотрудников	Персональные данные сотрудников
Договоры с клиентами	Коммерчески значимая информация
Отчеты экономического отдела	Элементы коммерческой тайны
Кабельный журнал, информация по ЛВС	Данные о структуре локальной сети
Карточки ЭЦП	Система электронного документооборота

Таким образом, рассмотрев параметры существующей системы ООО «Вектор», можно сделать выводы:

- в условиях ООО «Вектор» используется корпоративная распределенная сеть, сегментами которой являются как информационные базы, так и система защиты информации;
- технология защиты распределенной сети реализована на платформе Open VPN;

- защита распределенной сети от угроз обеспечивает защиту от внешних вторжений, утечек информации, сетевых угроз другого вида;
- в ООО «Вектор» создана организационная структура, позволяющая решать задачи обеспечения информационной безопасности.

Далее рассмотрим более подробно компоненты обеспечения информационной безопасности в условиях корпоративной сети ООО «Вектор».

Основные проблемы в реализации политик единого информационного пространства компании связаны со сложностью организационной структуры компании, которая включает в себя множество юридических лиц различной формы собственности, задействованных в процессе организации оказания услуг по проектированию и возведению коммуникационной инфраструктуры.

Все технологические процессы в структуре ООО «Вектор» автоматизированы с использованием соответствующей информационной системы, нарушение функционала которой приведет к остановке соответствующего бизнес-процесса, что в значительной степени влияет на эффективность работы компании.

Угрозы информационной безопасности могут быть связаны с вероятностью сетевых вторжений, активностью вредоносного ПО, деятельностью злоумышленников, направленной на нарушение функций автоматизированной системы компании. Для оценки защищенности информационной системы компании необходимо проведение аудита состояния системы защиты информации по каждому из компонентов.

Нормативными документами в области обеспечения защиты информации в условиях службы информационной безопасности ООО «Вектор» являются:

- Положение об обеспечении информационной безопасности ООО «Вектор»;
- Положение об обеспечении защиты информации от вредоносного ПО и сетевых ресурсов ООО «ВЕКТОР»;
- Положение о криптографической защите и электронном документообороте ООО «ВЕКТОР».
- Мониторинг уязвимостей производится в соответствии со стандартами [17]:
- ISO 19011 «Руководящие указания по аудиту систем менеджмента».
- ISO 27006 «Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ИБ».
- ISO 27007 «Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента ИБ».

Служба каталогов Active Directory содержит информацию обо всех пользователях, компьютерах, серверах компании.

Данные об архитектуре защиты в компании содержат информацию об антивирусной защите, используемых системах физической защиты и защиты от сетевых атак, описание перечня защищаемых информационных ресурсов, таблицы управления доступом.

Криптографические системы содержат электронные ключи, сертификаты электронной подписи.

Виртуальные машины содержат установленные системы управления базами данных (СУБД) с информационными ресурсами, используемыми в прикладных программных комплексах.

Базы данных клиентов содержат персональные данные клиентов и коммерчески значимую информацию о сделках с ними.

Перечень видов первичной информации, с которой работают специалисты ООО «Вектор», представлен в таблице 7.

Таблица 9 - Перечень видов первичной информации ООО «Вектор»

Вид информации	**Отдел**	**Носитель**	**Способ обработки информации**
1	2	3	4
Служба каталогов Active Directory	IT-отдел	Windows 2012 Server	Автоматизированный
Данные об архитектуре защиты информации в компании	Отдел информационной безопасности	Положение о защите информации, положение об антивирусной защите, таблицы разграничения доступа	Неавтоматизированный
Криптографические системы	Отдел информационной безопасности	Копии сертификатов электронной подписи	Неавтоматизированный
Виртуальные машины	Отдел разработки и сопровождения	Файлы в формате vdi	Автоматизированный
Базы данных клиентов	Отдел разработки и сопровождения	СУБД MS SQL Server	Автоматизированный
Программные коды разработанных систем	Отдел разработки и сопровождения	Документы на бумажном носителе, база данных договоров	Неавтоматизированный
Бухгалтерский баланс	Экономический отдел	Документ на бумажном носителе, БД 1С: Предприятие	Неавтоматизированный

Программные коды разработанных систем – исходные коды программных продуктов, разработанные ИТ-специалистами компании.

Бухгалтерский баланс содержит информацию о финансовом состоянии компании.

На рисунках 12-13 приведена оценка информационных активов компании, в таблице 10 приведен перечень сведений конфиденциального характера в компании.

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка (ед. изм.)	Качественная
1	2	3	4	5	6	7
			Информационные активы			
Основная деятельность	Сертификаты электронной подписи	Файлы сертификатов, копии сертификатов на бумажных носителях	ИТ-отдел	Доверие клиентов, репутация	шт.	Высокая
	Базы данных производственной деятельности	Файл базы данных формата MS SQL Server	ИТ-отдел	Возможность ведения основной деятельности	шт.	Высокая
	Виртуальные машины	Файлы формата vdi	Отдел бухгалтерского учета	Возможность ведения основной деятельности	шт.	Высокая
	Файловый сервер	Документы на сетевом ресурсе	Отделы компании	Возможность ведения основной деятельности	шт.	Высокая
Защита информации	Персональные данные сотрудников и клиентов	Документ на бумажном и электронном носителе	Специалист по работе с персоналом	Выполнение требований законодательства	шт.	Высокая
	Ключи ЭП	Электронное хранилище ЭЦП	Отдел бухгалтерского учета	Выполнение требований законодательства	шт.	Высокая
Обеспечение безопасности	Служба каталогов	Active Directory		Выполнение требований законодательства	шт.	Высокая
			Активы программного обеспечения			
Основная деятельность	1С: Комплексная	Бухгалтерские документы в БД ПК	Отдел бухгалтерского учета	Выполнение регламентов работы с ПК	шт.	Средняя
	БД «Учет ЛВС»	Параметры ЛВС клиентов	ИТ-отдел	Выполнение регламентов работы с ПК	шт.	Средняя

Рисунок 12 - Оценка информационных активов ООО «Вектор»

1	2	3	4	5	6	7
			Физические активы			
	Сервер БД	Базы данных программных комплексов	ООО «Вектор»	Требования к сохранности информации в БД	шт.	Средняя
	Активное сетевое оборудование	Доступ к сетевым ресурсам ООО «Вектор»	ООО «Вектор»	Выполнение регламентов работы с оборудованием	шт.	Средняя
	Рабочие станции пользователей	Работа специалистов в автоматизированной системе	ООО «Вектор»	Выполнение регламентов работы с оборудованием	шт.	Низкая
	Файловый сервер	Хранилище документов	ООО «Вектор»	Выполнение регламентов работы с оборудованием	шт.	Низкая

Рисунок 13 - Оценка информационных активов ООО «Вектор»

Сведения, имеющие конфиденциальный характер в условиях ООО «Вектор»:

- бухгалтерская документация – сведения о начислениях заработной платы сотрудникам, налоговая и финансовая отчетность, доходы и расходы компании;
- кадровая информация – сведения о сотрудниках, работающих в компаниях – клиентах, где производится расчет заработной платы;
- информация об архитектуре информационных систем;
- информация об архитектуре и реализации системы антивирусной защиты и от НСД;
- данные, содержащиеся в договорах с клиентами.

Таблица 10 - Перечень сведений конфиденциального характера ООО «Вектор»

№ п/п	Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, № статей	Кто имеет доступ
1.	Данные об архитектуре службы каталогов	Конфиденциально	Внутренний стандарт предприятия	ИТ-специалисты, руководство
2.	Требования по обеспечению сохранения служебной тайны сотрудниками предприятия	Конфиденциально	Гражданский кодекс РФ ст. 139	Руководители подразделений, руководство
3.	Персональные данные сотрудников	ДСП	Федеральный закон 152-ФЗ	Специалисты по кадрам
4.	Закрытые ключи ЭП	Конфиденциально	Федеральный закон 63-ФЗ	Руководители подразделений, руководство
5.	Персональные данные клиентов	Конфиденциально	Федеральный закон 152-ФЗ	Отдел по работе с клиентами

Для оценивания степени ценности активов обычно используется метод ранжирования, при котором для каждого актива проводится сопоставление некоторого ранга (числа), обозначающего степень его ценности относительно других. Чем выше позиция в ранжировании, тем более ценным является актив. На рис. 14 показаны уровни ценности активов, установленные при проведении экспертного оценивания активов специалистами компании.

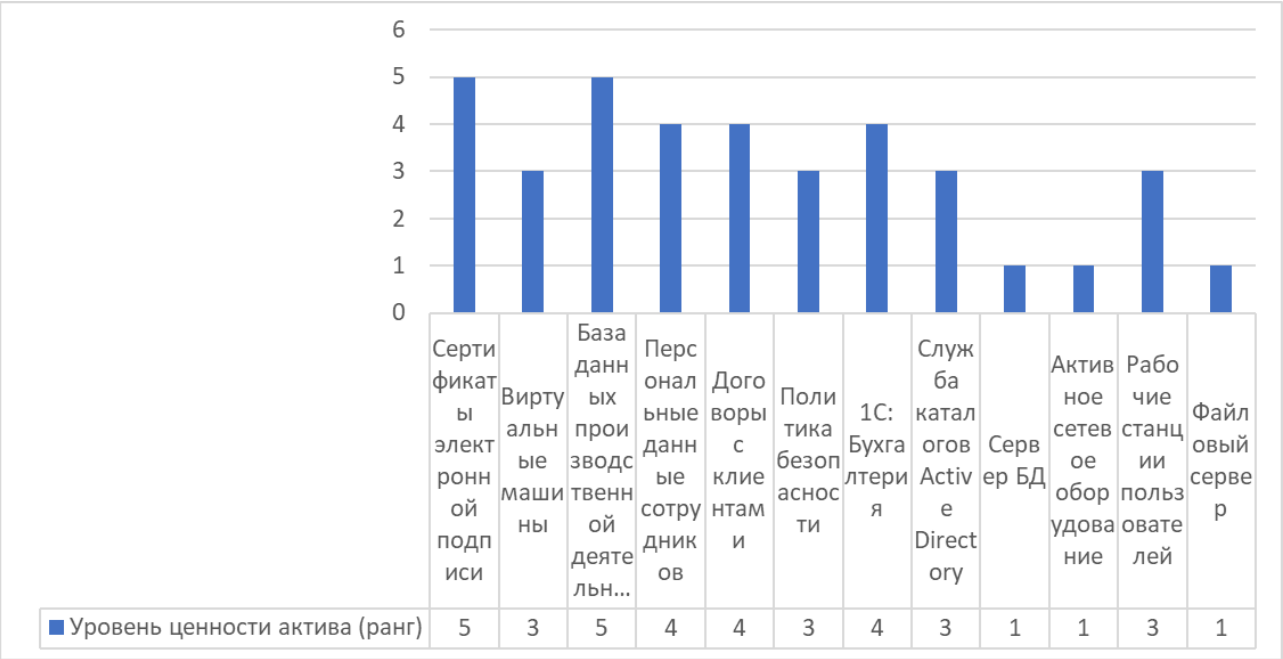

Рисунок 14 – Результаты оценки активов

Таким образом, активами, имеющим наибольшую ценность, являются:

- сертификаты электронной подписи;
- база данных производственной деятельности;
- персональные данные сотрудников;
- договоры с клиентами;
- 1С: Бухгалтерия (данные, содержащиеся в ПО 1С: Бухгалтерия).
- Выявленные уязвимости в системе защиты распределенной сети компании включают:
- отсутствие возможности подключения охранных систем к распределенной сети компании, что не позволяет

централизованно отслеживать состояние физической защиты информационных ресурсов компании;

- отсутствие возможности централизованного мониторинга состояния электропитания объектов аппаратного обеспечения информационной системы компании, так как не реализовано включение данного сегмента в распределённую сеть, что вызвано тем, что производителями серверные источники бесперебойного питания являются разные компании и поставляемое ими программное обеспечение не позволяет создать единую систему мониторинга;
- отсутствие внедренных систем защиты от атак, использующих методы социальной инженерии, что может снизить общий уровень защищенности системы.

Оценка стоимости реализации угроз информационной безопасности приведена в таблице 11.

Таблица 11 - Оценка стоимости реализации угроз информационной безопасности

Вид ущерба	**Перечень работ**	**Источник ущерба**	**Стоимость ущерба, тыс. руб.**
Простой системы вследствие реализации DDoS-атак	Подавление активности источника DDoS-атаки, перезапуск сервера	До 2 часов простоя работы специалистов	150
Простой системы на восстановление работы Web-сервера	Переустановка Web-сервера, восстановление базы	4 часа работы ИТ-специалистов, частичный простой работы компании	108
Предотвращение утечек данных	Выявление аппаратных закладок	Услуги мониторинга аппаратных закладок	80
		Итого	**338**

Алгоритм оценки уязвимостей информационным активам предполагает проведение анализа выполнения требований к защищенности распределенной сети в соответствии со стандартом ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Целью аудита может являться определения уровня защищенности распределенной системы, а также оценка степени уязвимости активов. В качестве аудиторов системы безопасности могут привлекаться как штатные сотрудники компании, так и привлеченные со стороны сертифицированные специалисты [16].

В рамках данной работы проведено проектирование системы безопасности ЛВС ООО «ВЕКТОР». Одной из основных задач обеспечения сетевой безопасности в компании является обеспечение защищенности информации при работе с сетевыми ресурсами. Информационные ресурсы компании работают в виртуальной среде, так как архитектура программного обеспечения и используемые СУБД являются разнородными, при этом приобретение дополнительного программного обеспечения не рассматривается. Платформа используемых виртуальных машин - VMWare.

В качестве угроз сетевой безопасности в условиях ООО «ВЕКТОР» рассматриваются:

- непреднамеренные утечки информации вследствие халатности персонала (например, вследствие утери носителей информации с файлами, содержащими персональные данные, получение доступа к файлам, содержащим ПДн или инженерные разработки, программные коды АСУ ТП, вследствие отсутствия системы разграничения доступа на сервере и неиспользования систем защиты документов, оставление доступа к компьютерам при необходимости выхода с рабочего места и др.);
- активность вредоносного ПО;
- угрозы сохранности персональных данных вследствие аппаратного сбоя;

- угрозы злоумышленников, связанные с намеренным получением персональных данных.

В перечень организационных мер, включающих административные и управленческие мероприятия по защите информации в ООО «ВЕКТОР» входят вопросы:

- ведение специальной номенклатуры дел в указанной области;
- назначение ответственных специалистов за обеспечение защиты информации в учебной части и в обеспечивающих подразделениях;
- проведение обучения сотрудников, доведение регламентов защиты информации под роспись.

В целях обеспечения безопасности информации АИС ООО «ВЕКТОР» принимаются меры правового, организационного, технического и морально-этического характера.

Перечень документов в области защиты персональных данных в условиях ООО «ВЕКТОР» включает:

- положение о защите персональных данных в условиях ООО «ВЕКТОР»;
- согласия на обработку персональных данных от сотрудников и родителей (законных представителей) учащихся;
- перечень информационных ресурсов, в которых производится обработка персональных данных;
- перечень сотрудников, допущенных к обработке персональных данных;
- перечень сотрудников, допущенных к обработке персональных данных неавтоматизированным способом.

Проведем анализ основных типов угроз сетевой безопасности.

Одним из критериев классификации сетевых угроз является их происхождение, в данном случае угрозы безопасности делятся на угрозы,

связанные с влиянием человеческого фактора и угрозы, связанные с особенностями работы аппаратного обеспечения.

Угрозами технического характера являются [10]:

- ошибки в работе программного обеспечения;
- проведение внешних DoS- и DDoS-атак;
- действие вредоносного программного обеспечения;
- осуществление несанкционированного съема информации;
- активность сетевых угроз.

В качестве мер по защите от угроз, связанных с халатностью сотрудников можно рассматривать:

- минимизацию технической возможности реализации инцидентов на узле распределенной сети путем предоставления минимально возможного набора прав пользователя;
- мониторинг активности учетных записей и при отсутствии действий в заданном промежутке времени прерывание сессии;
- принятие комплекса организационных мероприятий, выпуск инструкций и приказов, регламентирующих ответственность пользователей.

В качестве мер по защите от угроз, связанных с некомпетентностью сотрудников в области информационной безопасности, можно рассматривать:

- проведение технических учеб с пользователями информационной системы;
- включение требований в области защиты информации к необходимым компетенциям при отборе сотрудников;
- проведение аттестаций в области защиты информации, по итогам которых возможно предоставление либо закрытие доступа к необходимым в работе информационным ресурсам.

Диаграмма возможного ущерба от угроз информационной безопасности приведена на рисунке 13.

Рисунок 115 - Диаграмма возможного ущерба от угроз информационной безопасности

Как показано на рисунке 13, ущерб, обусловленный нарушениями требований информационной безопасности, может быть как прямым, связанным с потерей конфиденциальных данных, временными и материальными затратами на работоспособности приложений, а также вторичным, обусловленным репутационными потерями компании, связанными с оглаской сведений о качестве обеспечения данных, возможными появлениями каналов постоянного перехвата информации.

Таким образом, для каждой из угроз ИБ сопоставляется свой тип решений технологического и организационного характера, что при комплексном применении повышает общую защищённость системы.

Комплекс мероприятий в области защиты информации зависит от специфики решаемых задач, уровнем защищенности информационных ресурсов, моделью нарушителей. Таким образом, средства защиты информации необходимо выбирать в соответствии с актуальными угрозами.

Для того, чтобы обеспечить в полном объеме технологическое обеспечение по всем требованиям защиты конфиденциальности информации, подразделения ООО «ВЕКТОР» применяют специальные способы автоматизации (таблица 12). Введение в эксплуатацию каждого из программно-технических средств определяется локальным документом.

Таблица 102 - Описание технологических средств защиты информации

Программно-техническое обеспечение	Описание функции	Нормативная документация
Криптографические системы	Защита данных при передаче по коммуникационным каналам, работа с системами электронного документооборота	Положение о работе с криптографическими средствами
Антивирусные системы	Защита от вредоносного ПО	Положение об антивирусной защите
Сканеры безопасности	Мониторинг защищенности ресурсов распределенной сети	Положение об использовании сканеров безопасности

Анализ состояния защищённости системы в подразделениях, использующих узлы распределённой сети компании, осуществляется специалистами отдела информационной безопасности, которые как в удаленном режиме, так и с выездом на объект проводят анализ соответствия системы защиты информации принятым стандартам и регламентам.

В рамках анализа существующей системы использования сетевых ресурсов в условиях ООО «ВЕКТОР» были выявлены проблемы, связанные с возможностью передачи конфиденциальной информации по открытым каналам связи, что потенциально создает условия для компрометации передаваемых данных.

3.3 Программная компонента обеспечения защиты информации

Далее проведем анализ использования программных средств защиты информации в условиях исследуемой компании. Современные корпоративные версии антивирусных систем позволяют осуществлять защиту ИТ-инфраструктуры компаний со сложной территориально распределенной структурой.

При этом корпоративная версия антивирусного ПО в настоящее время позволяет не только управлять защитой от вредоносных программ, но и

предоставляет множество инструментов для работы администраторов распределенных сетей, включая возможности:

- управления серверами антивирусной защиты, установленных в узлах распределенной сети;
- удаленной установки обновлений программного обеспечения, как в области защиты информации, так и системного и прикладного;
- ведения мониторинга системных событий;
- получения оперативной информации о признаках наличия инцидентов информационной безопасности в любом из узлов распределенной сети.

Схема архитектуры антивирусной защиты ООО «Вектор» показана на рисунке 16.

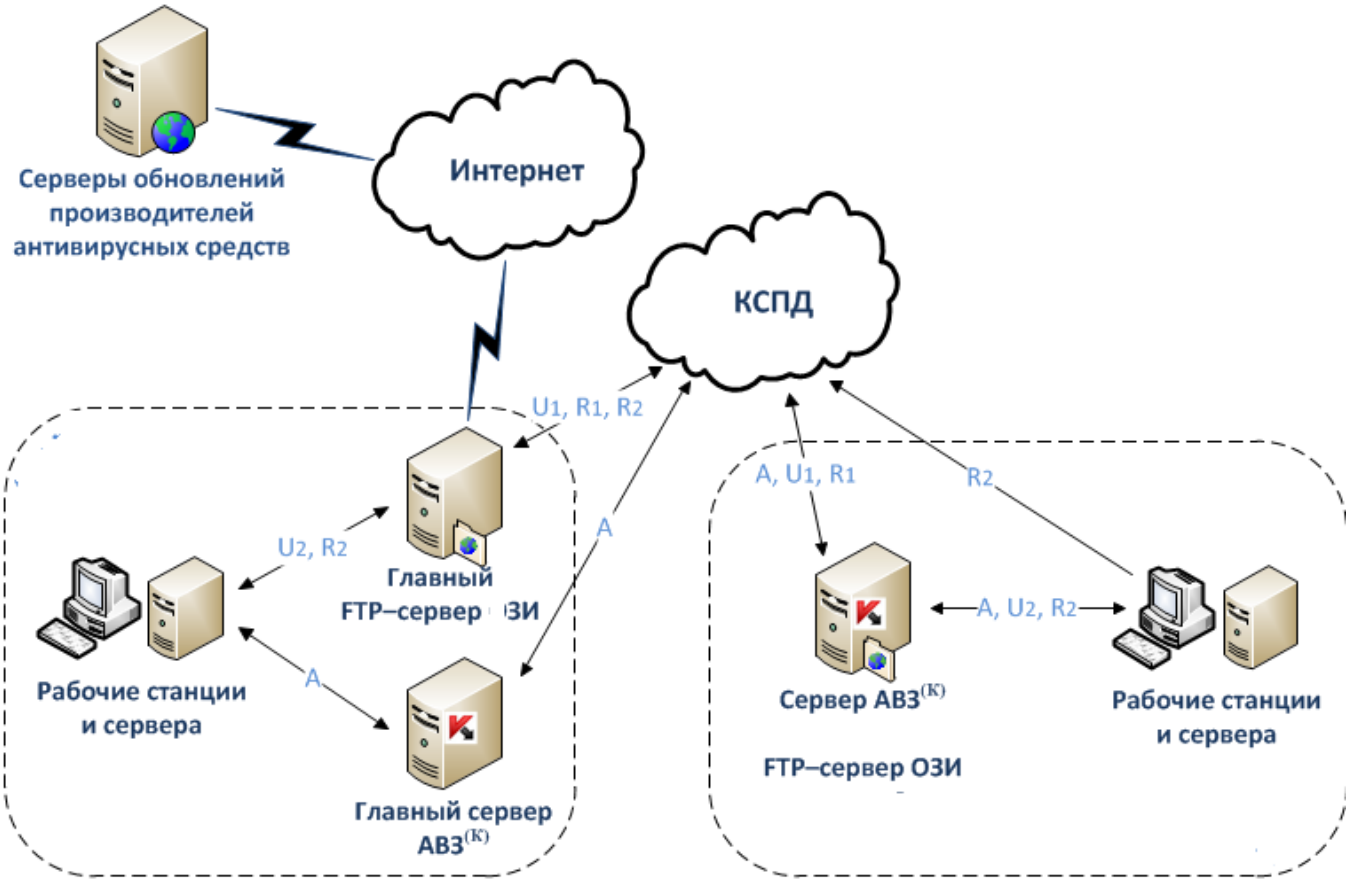

Рисунок 126 - Структура системы антивирусной защиты ООО «Вектор»

Таким образом, корпоративная система антивирусной защиты соответствует специфике распределённой сети, что предполагает:

- однократное получение обновления антивирусных баз и программных модулей с сервера производителя;
- распространение обновлений на подчинённые узлы корпоративной сети;
- установка настроек политики антивирусной защиты на уровне головного сервера и их распространение на подчинённые узлы. Политика может включать: допуск рабочей станции к использованию flash-накопителей, времени использования рабочей станции, возможность приостановки антивирусной защиты, допуск к возможности самостоятельной установки программ, запрет на запуск программ по их имени или контрольной сумме и др.

Проведем анализ бизнес-процессов мониторинга состояния информационной безопасности. На рисунок 17 приведена контекстная диаграмма. Как показано на рисунок 17, входящие информационные потоки содержат данные:

- об инженерных коммуникациях Управления ООО «Вектор»;
- об организационной структуре предприятия;
- о деятельности предприятия;
- об архитектуре информационной системы.

Результирующие информационные потоки содержат сводную информацию о состоянии информационной безопасности ООО «Вектор». На рисунок 16 приведена диаграмма декомпозиции основного процесса.

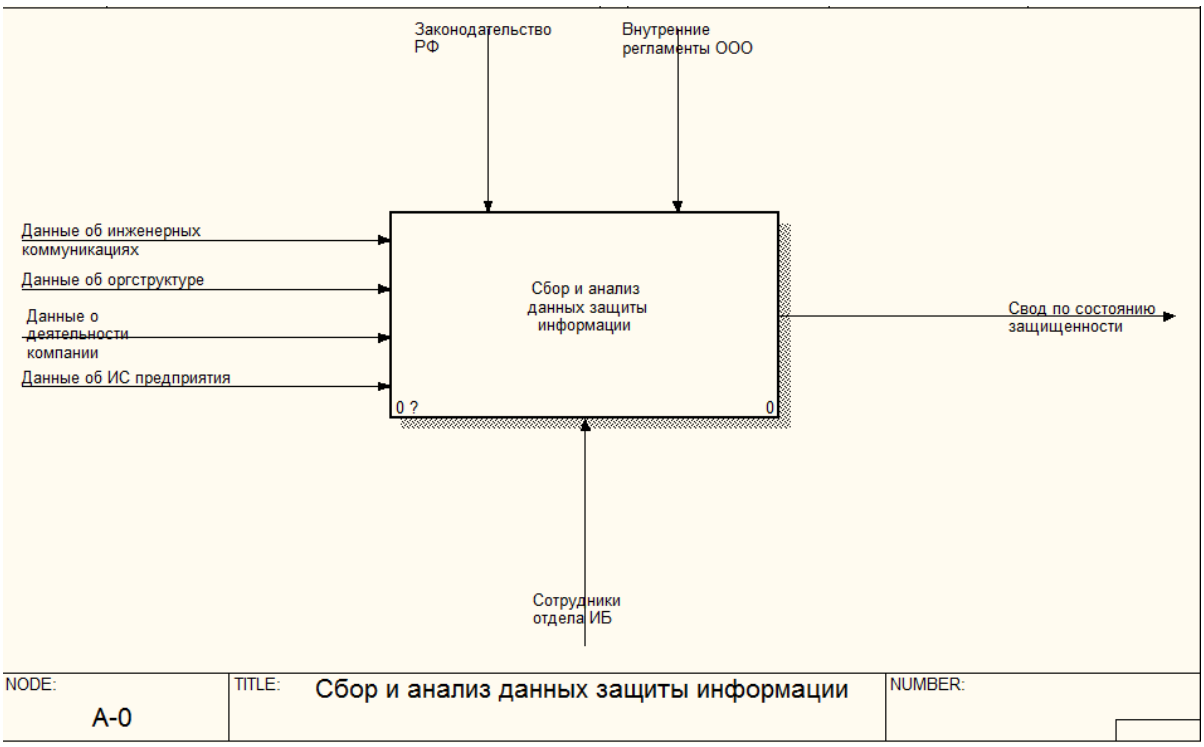

Рисунок 137 - Контекстная диаграмма

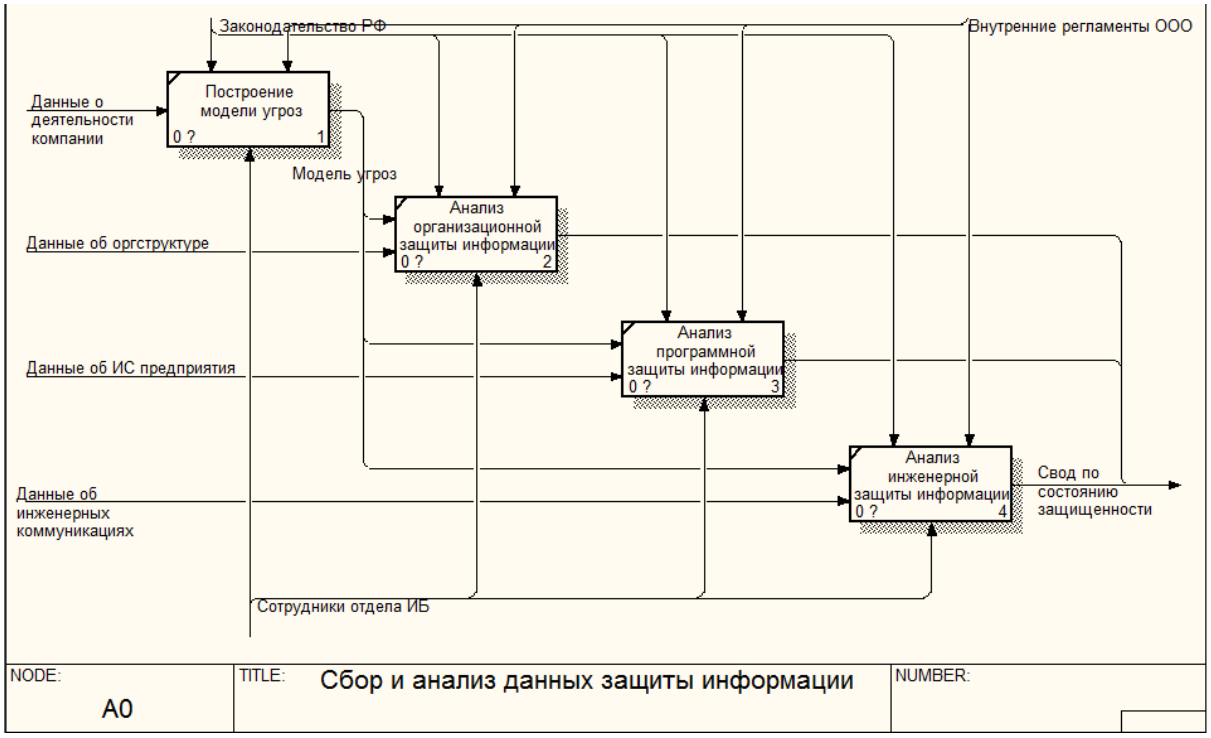

Рисунок 148 - Диаграмма декомпозиции сбора и анализа защиты информации

Как показано на рисунке 18, сбор и анализ состояния информационной безопасности ООО «Вектор» включает следующие виды работ:

- построение модели угроз;

- анализ организационной защиты информации;
- анализ программной защиты информации;
- анализ инженерно-технической защиты информации.

На рисунке 18 приведена диаграмма декомпозиции построения модели угроз, на рисунке 19 – анализа программной защиты информации.

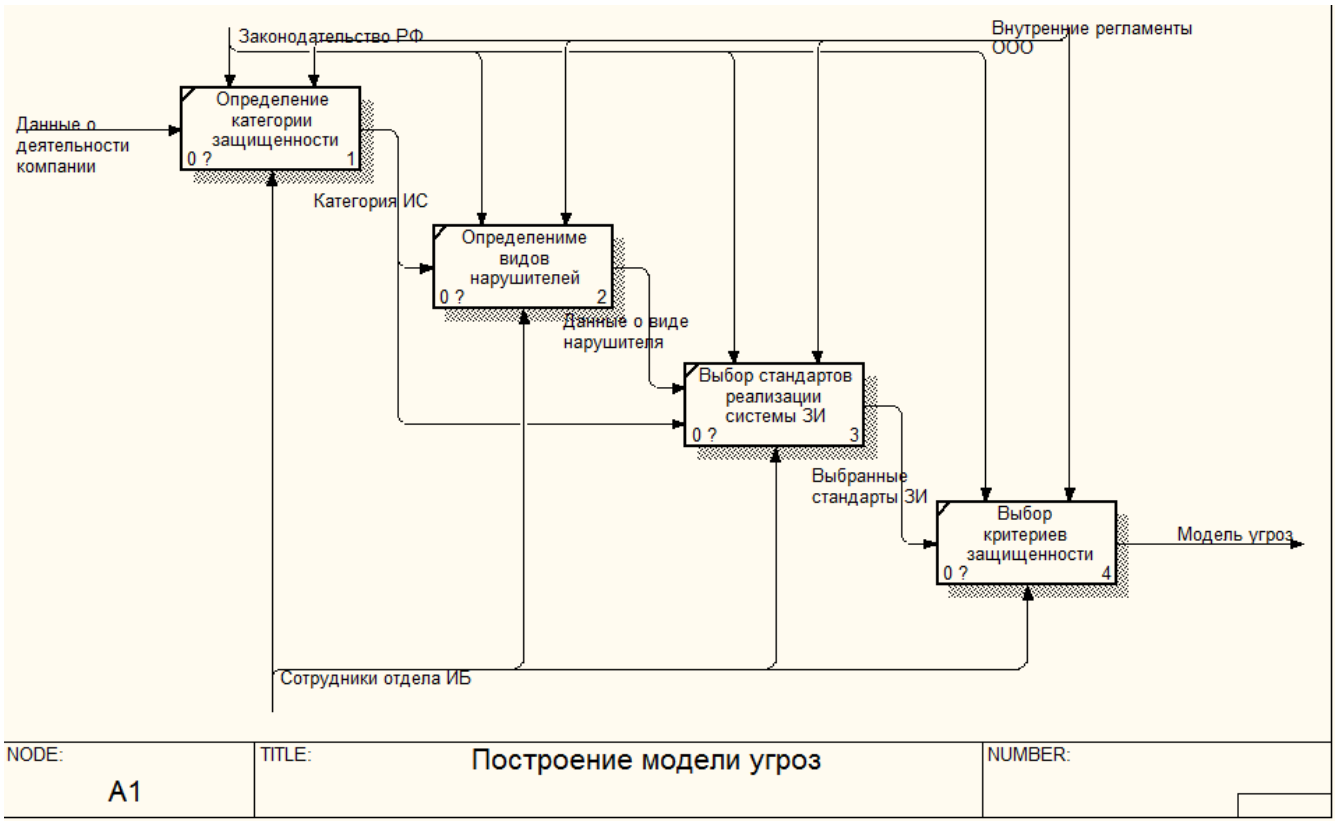

Рисунок 159 - Диаграмма построения модели угроз

Как показано на рисунке 17, для оценки эффективности проводимых работ по защите информации необходимо провести анализ видов обрабатываемой информации в условиях ООО «Вектор», определить категорию обрабатываемых данных. Далее необходимо выбрать стандарт реализации систем защиты информации, соответствующий классу обрабатываемых данных, на основе которого выбираются критерии защищенности системы, по которым проводится дальнейший сбор информации и ее обработка.

На рисунке 20 показаны основные подходы к организации системы защиты информации (анализ организационной структуры предприятия, изучение документации по защите информации, анализ организации системы защиты, оценка качества организации системы защиты).

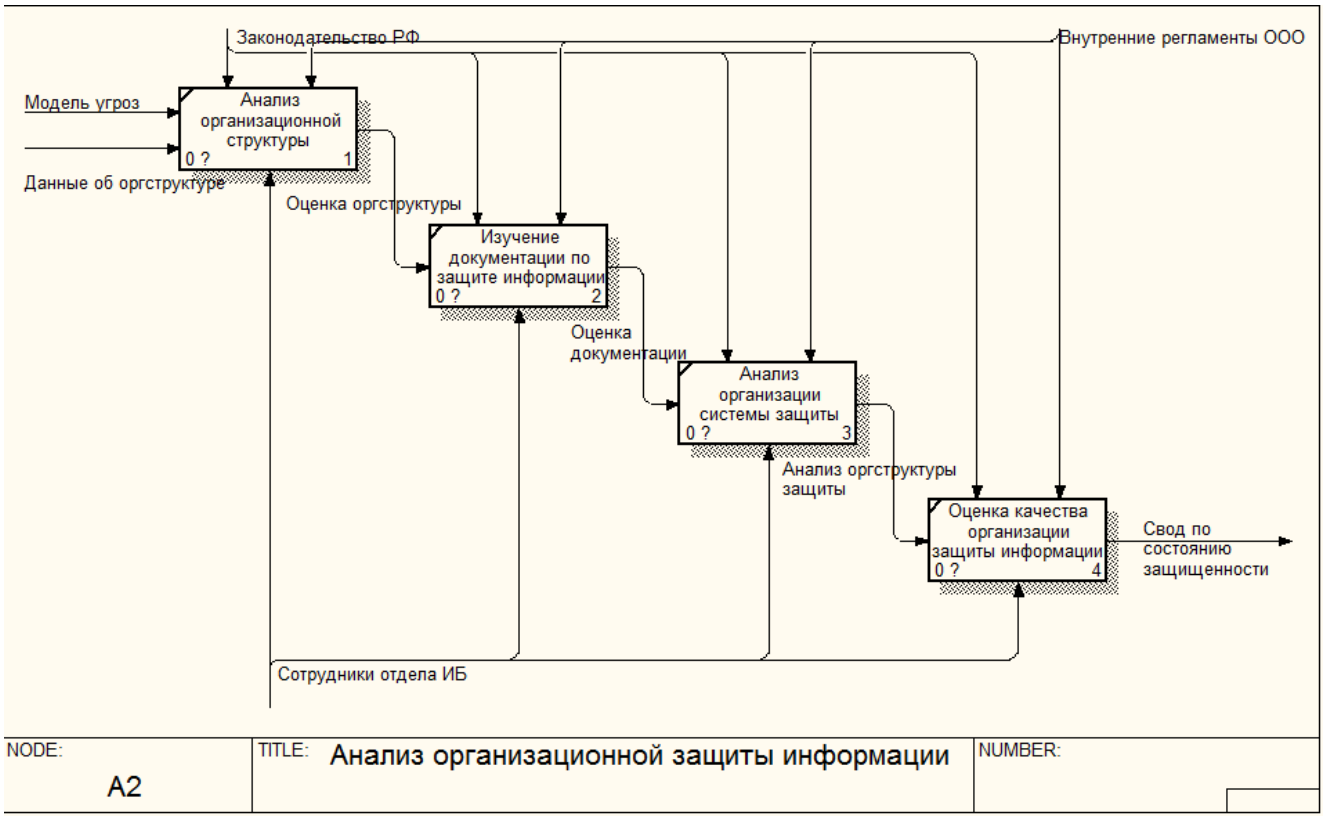

Рисунок 20 - Диаграмма анализа организационной защиты информации

Как показано на рисунке 21, в рамках анализа программной части защиты информации проводится:

- инвентаризация информационных ресурсов ООО «Вектор»;
- определение пользователей и их ролей в контексте их достаточности при выполнении должностных обязанностей;
- оценка эффективности применяемых средств программной защиты информации;
- проведение мониторинга работы программной среды предприятия на предмет соответствия модели угроз.

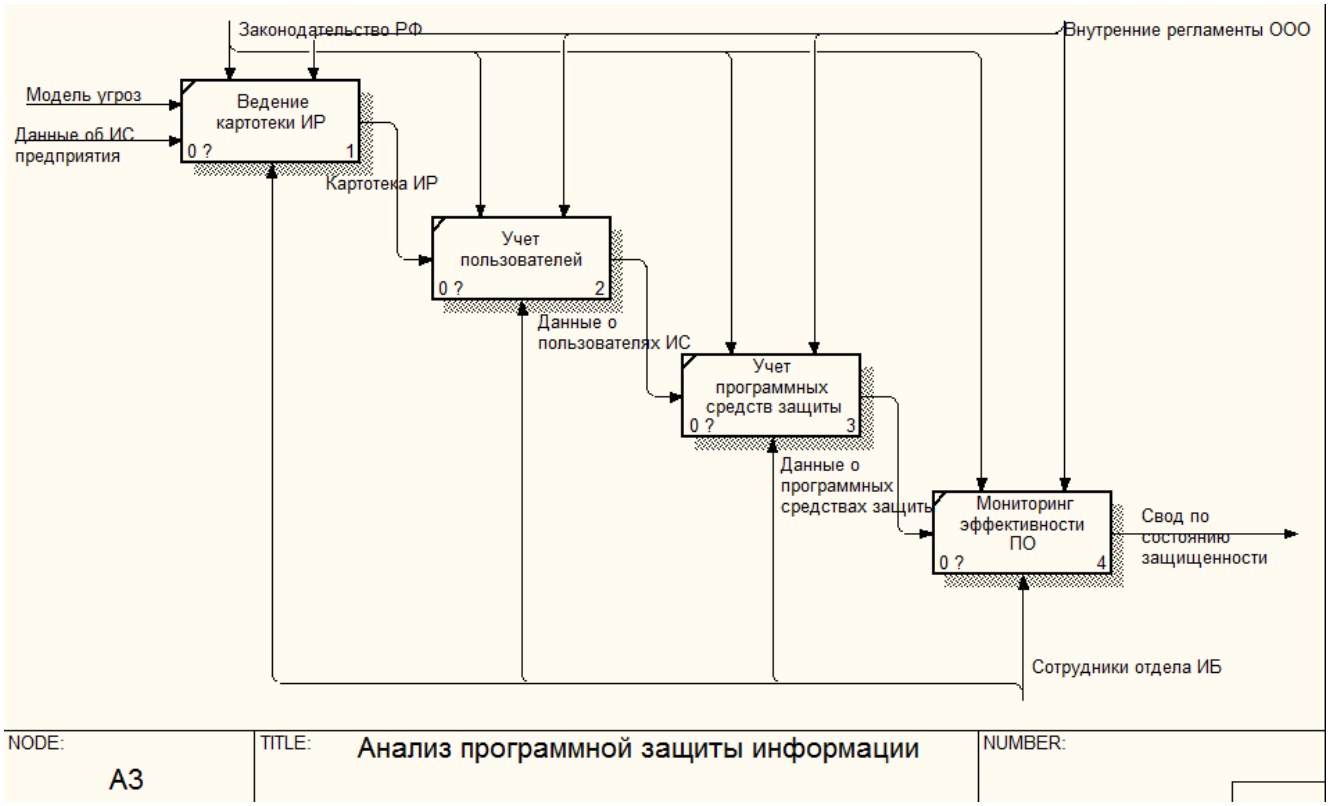

Рисунок 21 - Диаграмма анализа программной защиты информации

Типовыми проблемами в организации сбора информации по защите информации в условиях промышленных предприятий являются:

- отсутствие необходимых программных средств по оценке соответствия документации по защите информации классу информационной системы;
- отсутствие инструментов мониторинга эффективности используемых программных средств и аудита пользовательских учетных записей.

Использование автоматизированной системы для поддержки технологии сбора и анализа данных состояния защищенности информационной системы промышленных предприятий позволит повысить эффективность аудита защищенности. Таким образом, совершенствование бизнес-процесса сбора и анализа данных по защите информации связано с внедрением в работу предприятия программного инструмента, позволяющего решать указанные задачи.

В качестве критериев оценки эффективности функционирования ресурсов распределённой сети ООО «Вектор» и состояния их защиты рассматриваются:

- влияние установленных средств защиты на производительность сетевых приложений;
- эффективность работы систем шифрования трафика (отсутствие коллизий, качество передачи данных, скорость процесса шифрования при передаче данных между узлами распределенной сети);
- производительность работы с Web-приложениями;
- инструкции для работы с сетевыми ресурсами, утверждение которых обязательно на уровне руководства компании, но при этом сотрудники, знакомясь с ними, должны ставить свой автограф;
- наличие выявленных случаев отказа сетевых приложений, вызванных внешними причинами, связанными с информационной безопасностью;
- статистика обнаружения сетевых пакетов, источниками которых не являются установленные сетевые приложения.

Таким образом, совершенствование архитектуры информационной безопасности исследуемой компании связано с использованием сканера безопасности.

В таблице 13 приведена характеристика состояния защищенности информационной системы ООО «Вектор» от основных видов угроз в рамках использования распределенной архитектуры информационной системы.

Таблица 113 - Характеристика состояния защищенности информационной системы ООО «Вектор» от основных видов угроз

Направление защиты информации	Технология	Степень соответствия состоянию защищенности
Антивирусная защита	Kaspersky Security Center	Соответствует
Защита сетевых соединений	VPN	Соответствует
Криптографическая защита	Криптопровайдер ООО «Вектор»	Соответствует
Физическая защита	СКУД Орион	Соответствует
Парольная защита	JaCarta, Indeed-ID	Соответствует
Защита от перехвата информации с использованием специальных средств	Отсутствует	Не соответствует
Защита от действий пользователей, приводящих к инцидентам информационной безопасности	Отсутствует	Не соответствует
Мониторинг активности внешней среды (сканирование уязвимостей)	Отсутствует	Не соответствует
Организационная защита информации	Пакет нормативных документов	Соответствует
Системы резервирования	Acronis	Соответствует
Охранно-пожарная сигнализация	Установлена	Соответствует
Физическая защита помещений	Посты охраны	Соответствует
Использование внешних носителей информации	Регламент использования	Соответствует
Защита от установки нежелательного ПО	Средства мониторинга АВЗ, ограничение прав пользователей, ведение реестра разрешенного ПО	Соответствует
Предоставление доступа к информационным ресурсам	Система документооборота, таблицы управления доступом	Соответствует
Анализ активности учетных записей	Мониторинг активности	Не соответствует

Таким образом, совершенствование архитектуры информационной безопасности ООО «Вектор» необходимо осуществлять в направлениях:

- мониторинга активности внешней среды (сканирование уязвимостей);
- защиты от действий пользователей, приводящих к инцидентам информационной безопасности.

3.4. Использование сканеров безопасности

В рамках практической части работы для аудита защищенности информационной системы ООО «Вектор» предлагается использование сканера уязвимостей Nessus [28].

Сканер уязвимостей Nessus является одним из наиболее распространенных программных продуктов в области поиска уязвимостей в ИС [2].

Ключевой особенностью использования приложения является необходимость подключения плагинов, каждый из которых отвечает за поиск уязвимостей определенного типа. Существуют 42 различных типа подключения внешних модулей: для проведения пентеста возможна активация как отдельных плагинов, так и всех плагинов определенного типа, например, для проведения всех локальных проверок на системах класса Ubuntu. Также пользователями системы, имеющими квалификацию в области работы с системами безопасности, возможно написание собственных модулей сканирования.

Основные возможности системы Nessus Professional включают [3]:

- наличие большого количества режимов анализа защищенности;
- возможность управления настройками сканирования;
- наличие сервиса обновлений программного продукта и базы знаний по уязвимостям;

- возможность создания отчетности об уязвимостях.

В системе поддерживается несколько способов сканирования, включающих удаленное и локальное сканирование активов, сканирование с поддержкой аутентификации, автономный аудит конфигурации сетевых устройств [3]:

- возможности обнаружения и сканирования активов, включающих сетевые устройства, включая брандмауэры, операционные системы, базы данных, веб-приложения, виртуальные и облачные среды;
- сервисы сетевого сканирования. Сканирование протоколов IPv4, IPv6 и гибридных сетей, поддерживается возможность запуска задач по расписанию;
- возможности сканирования с настройкой времени и частоты запуска;
- сканирование сетевых узлов по выборке;
- возможность автоматического анализа результатов сканирования. Выдача рекомендаций по восстановлению и настройке процесса поиска уязвимостей.

В системе имеются возможности автоматической пересылки отчетов ответственным специалистам при обнаружении уязвимостей, с указанием уровня их опасности, формирования отчетности по расписанию, включая отчеты по устранению уязвимостей. Возможность создания отчетности с поддержкой сортировки по видам уязвимостей или хостам, создание аналитического отчета по результатам поиска уязвимостей и состоянию защищенности сети. Поддерживается множество форматов отчетов, включая: встроенные (XML), PDF, CSV и HTML. Возможна настройка рассылки уведомлений об отправке отчета, о получении или обновлении состояния защищенности сети.

Рассмотрим функционал отдельных плагинов системы.

NASL (Nessus Attack Scripting Language).

Данный плагин имеет раздельные серверную и клиентскую части. В последней 4.2 версии агент проводит открытие Web-сервера на 8834 порту, посредством которого возможно управление сканером с использованием интерфейса, реализованного на Flash, с использованием браузера. После установки сканера серверная часть запускается автоматически. При определении типа лицензии система открывает доступные возможности сканирования: по количеству IP-адресов и возможным действия с обнаруженными уязвимостями.

Система администрирования Nessus предлагает создание учетных записей, под которыми выполняются операции сканирование на наличие уязвимостей.

Любой тест на проникновение начинается с создания так называемых Policies – правил, в соответствии с которыми сканер будет проводить анализ уязвимостей системы.

При задании правил необходимо указать [2]:

- виды сканирования портов (TCP Scan, UDP Scan, Syn Scan и т.д.);
- количество одновременных подключений, а также типичные для Nessus настройки, например, Safe Checks. Последняя включает безопасное сканирование, деактивируя плагины, которые могут нанести вред сканируемой системе.

Необходимым шагом при создании правил является подключение необходимых плагинов: возможна активация целых групп, например, Default Unix Accounts, DNS, CISCO, Slackware Local Security Checks, Windows и т.д. Система проверяет признаки большого количества возможных атак и подозрительной активности приложений.

Сканер никогда не будет анализировать активность сервиса только по номеру его порта. При изменении стандартно используемых приложениями портов – сканер обнаруживает изменение и проведет определение наличия подозрительной активности.

Ниже приведен перечень общих настроек, к которым возможно получение доступа [2]:

- Basic: посредством данного параметра возможно определение связанных с безопасностью и организационных аспектов проведения проверки или политики. Данные аспекты будут включать наименование шаблона сканирования, информацию о целях сканирования, в независимости от того является ли данная операция запланированной.
- Discovery: в данной настройке проводится определение сканируемых портов и методов, которые будут использованы при проведении указанного исследования. Настройка содержит несколько разделов.
- Assessment: Данный параметр позволяет определять тип сканирования уязвимостей для выполнения и способы его исполнения. Система проводит проверку уязвимостей веб-приложений к возможным атакам, а также проверку устойчивости других приложений к DDoS-атакам.
- Report: В данной области настройки проводится работа с шаблонами формируемой отчетности по результатам сканирования уязвимостей.

На рисунок 20 приведен режим настройки процесса сканирования уязвимостей, на рисунок 21 – настройки сканирования.

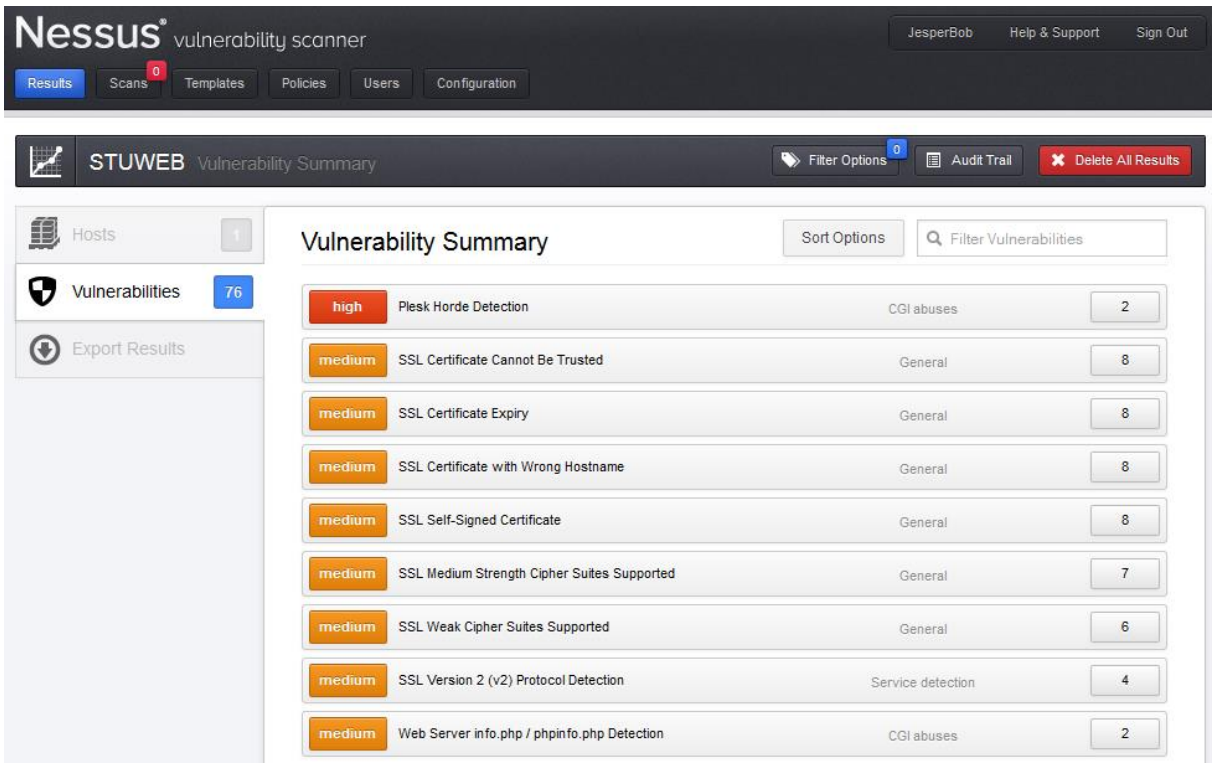

Рисунок 2216. Настройки сканирования уязвимостей

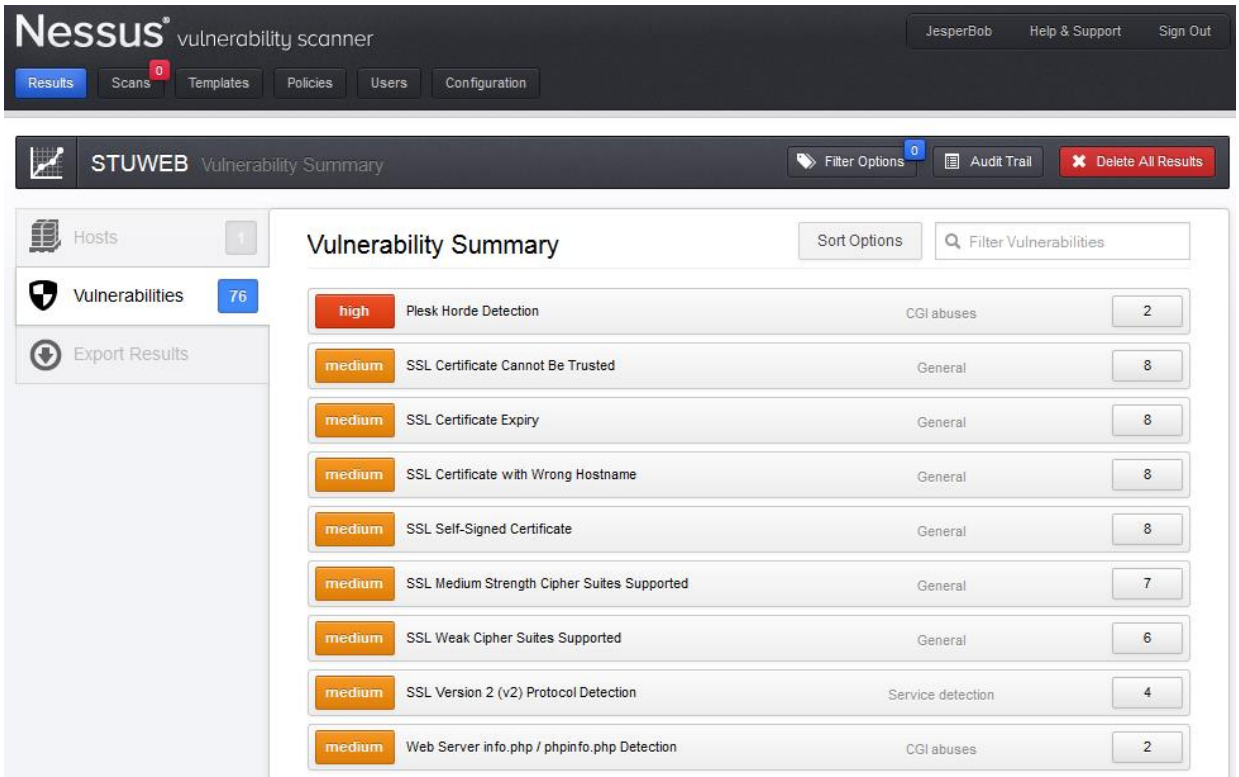

Рисунок 23. Настройки сканирования

В ходе проведения сканирования сети ООО «Вектор» были обнаружены следы инцидентов:

- обнаружение неопознанного потока запросов к базе данных MS SQL Server;
- обнаружены внешние сетевые атаки на серверные ресурсы;
- возможность авторизации в СУБД в автоматическом режиме без ввода пароля;
- обнаружена активность неопознанного приложения на сервере.

Уязвимости в информационной системе ООО «Вектор включают:

- не отключенная учетная запись «администратор» на компьютерах пользователей без пароля;
- пароль Администратора на сервере не соответствует требованиям безопасности;
- пользователям доступен режим самостоятельного отключения и удаления антивирусного ПО;
- пользователи на рабочих станциях имеют права локальных администраторов;
- установлены прикладные программные продукты, использование которых требует административных прав;
- не разграничен доступ к использованию flash-накопителей;
- существуют служебные доменные учетные записи, не имеющие пароля (например, учетная запись для использования сетевого сканера);
- отсутствует система защиты от СПАМа;
- в разделяемых файловых ресурсах всем пользователям доступны режимы записи, изменения и удаления (что является для некоторых ресурсов избыточным), не проводится мониторинг активности учетных записей при работе с ресурсами файлового сервера;
- ошибки в конфигурировании межсетевого экрана.

Устранение указанных уязвимостей возможно при использовании дополнительных программных средств, позволяющих провести анализ состояния системы (например, антивирусного ПО).

Защиту от действий пользователей от инцидентов информационной безопасности предлагается осуществлять с использованием DLP-системы.

Предлагается ко внедрению DLP-система «КИБ СёрчИнформ», которая является более мощной, в отличие от классической DLP. Благодаря тому, что в ней существует значительный комплекс аналитических инструментов, а также с ее помощью можно ориентировать не только на данные, но и на пользователя, система обладает [5]:

- защитной системой и возможностью ликвидации последствий, которые связаны с завладением информации злоумышленниками;
- возможностью упреждения действий мошенников;
- возможностью определения кадровых рисков с составлением прогнозов действий сотрудников;
- системой поддержания трудовой дисциплины с соблюдением регламента.
- возможностью увеличить продуктивность работы как сотрудников компании, так и работу организации в целом.
- управлением лояльностью персонала.

Таблица 14 содержит информацию о режимах работы системы.

Архитектура системы показана на рисунке 24.

Система может использоваться для проведения оперативных оповещений и реагирований при возникновении внутренних и внешних угроз безопасности автоматизированных систем, а также контроля выполнения требований по безопасности информации.

Таблица 124 - Описание режимов работы системы

SearchInform NetworkController	SearchInform EndpointController
Контроль сетевой активности пользователей.	Контроль активности пользователей на рабочих местах.
Зеркалирование трафика на уровне корпоративной сети (коммутатора).	Фиксация действий пользователей с помощью установленных на компьютеры программ-агентов.
Отправка теневых копий на сервер, где проводится их проверка	Данные отправляются на сервер для проверки: сразу, если компьютер находится в офисе. . как только ПК подключается к Интернет, если сотрудник вне офиса (командировка, работа из дома и т.д.).

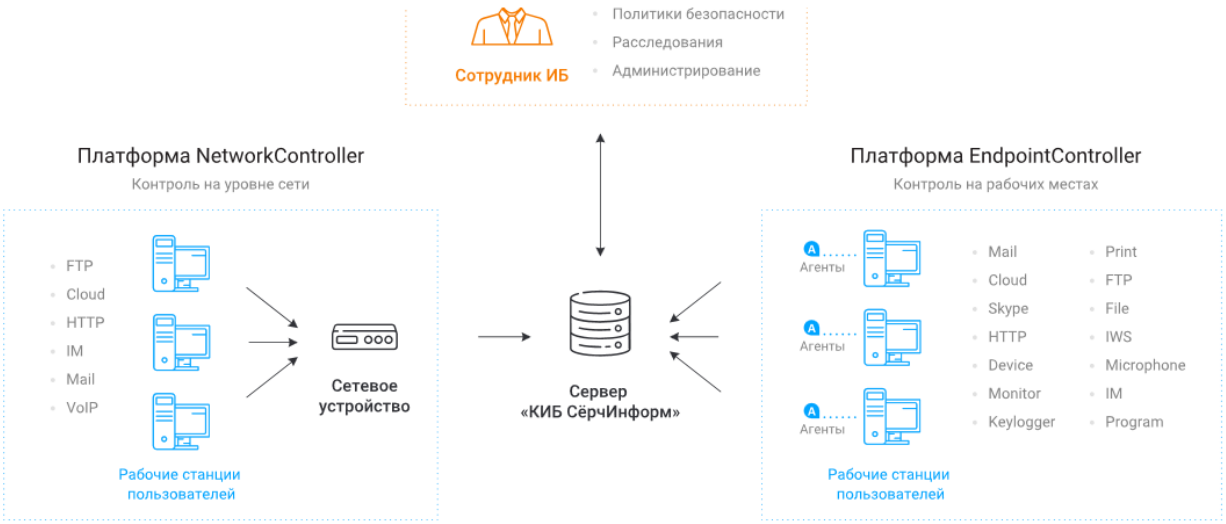

Рисунок 24 - Архитектура системы "КИБ Серчинформ"

Особенности системы [4]:

Сертификация ФСТЭК;

Возможность централизованного сбора и анализа данных журналов событий систем информационной безопасности, рабочих станций, серверного и сетевого оборудования;

Проведение удаленного контроля параметров конфигурации и функционала отслеживаемых объектов;

Возможность оперативного оповещения и реагирования на возникновение внутренних и внешних угроз безопасности автоматизированной системы;

Возможность контроля исполнения заданных требований по защите информации, сбора статистической информации и построения отчетов о состоянии защищенности;

Масштабирование решения и создание системы для проведения мониторинга информационной безопасности в произвольном масштабе;

Возможность взаимодействия с источниками данных о состоянии системы;

Возможность интеграции со следующими отечественными защищенными платформами и системами защиты информации: ОС МСВС, ОС Astra Linux, Сканер-ВС, МЭ и СОВ Рубикон, Xspider.

Дополнительные возможности системы:

- проведение сбора данных из удалённых источников с использованием модуля Splunk Forwarder;
- проведение корреляции сложных событий, охватывающих множество разнородных источников данных в среде.
- проведение масштабирования при сборе и индексации данных в объеме сотни терабайт ежедневно;
- комбинирование информации традиционных реляционных БД и Hadoop и проведение их последующего анализа;
- реализация ролевых моделей доступа к данным;
- создание собственных приложений, панелей (dashboard'ы), из которых формируются собственные Splunk-приложения;
- наличие большого количества готовых инструментов для проведения анализа.

Наличие уникальной инфраструктуры сбора, хранения и анализа сетевого трафика и журналов событий, позволяющей со значительно более высокими скоростями проводить обработку данных для организаций любых масштабов;

Возможность линейной масштабируемости как по параметрам объемов собираемой информации;

Высокая производительность системы корреляции событий, что позволяет проводить анализ огромных потоков событий;

Возможность реконструкции сетевых транзакций и анализа их содержимого;

Анализ и реконструкция сетевых транзакций для произвольных TCP/IP протоколов;

Представление сетевых сессий в унифицированном формате и данных журналов событий.

Таким образом "КИБ Серчинформ" в настоящее время обладает необходимыми компонентами системы информационной безопасности предприятий.

Система КИБ "Серчинформ" позволяет получать данные о состоянии защищенности информационной системы, посредством которых можно проводить оценку уровня принимаемых мер в области информационной безопасности.

В данной главе выпускной квалификационной работы был рассмотрен объект исследования, проанализирована эффективность использования распределенной архитектуры информационной системы, были определены объекты защиты и приведены их примеры, рассмотрена система антивирусной защиты, принятая на предприятии и проведен аудит информационной безопасности с использованием сканера безопасности Nessus.

В рамках проведенного анализа уязвимостей с использованием ПО Nessus информационной системы ООО «Вектор» было показано, что для системы характерно множество актуальных угроз, связанных с:

- обнаружением неопознанного потока запросов к базе данных MS SQL Server;
- обнаружением внешних сетевых атак на серверные ресурсы;
- возможностью авторизации в СУБД в автоматическом режиме без ввода пароля;
- активностью неопознанного приложения на сервере.

Устранение указанных недостатков возможно при проведении мероприятий по оптимизации системы безопасности на уровне баз данных и операционной системы.

4.Совершенствование системы администрирования безопасности распределенной сети ООО «Вектор»

4.1 Администрирование безопасности распределенной сети ООО «Вектор»

Одним из важнейших компонентов обеспечения сетевой безопасности исследуемого предприятия является система антивирусной защиты. Каждый из пользователей информационной системы несет персональную ответственность за выявленные факты заражения вредоносным ПО на своей рабочей станции.

Таким образом, целями антивирусной защиты в ИС предприятия являются:

- противодействие активности вредоносного ПО в ИС предприятия;
- обеспечение работоспособности ИС предприятия и возможностей по ее восстановлению в случае сбоев с минимумом финансовых издержек и временных затрат;

Основными принципами антивирусной защиты в Управлении ООО «Вектор» являются:

- доведение регламентирующих документов в области антивирусной защиты до пользователей информационной системы;
- регламентация использования внешних носителей информации (допускается оборот только учтенных носителей);
- использование в работе только лицензионных программ, включая операционные системы, своевременное их обновление;
- ежедневное обновление сигнатур антивирусных баз, программных модулей АВЗ в автоматическом режиме;
- проверка на наличие вредоносного ПО всех файлов, полученных из внешних источников;

- обучение правилам и нормам АВЗ вновь принятых на работу сотрудников;
- исключение доступа пользователей к настройкам системы антивирусной защиты;
- ограничение доступа пользователей к ресурсам Интернета.

Объектами антивирусной защиты в структуре ИС ООО «Вектор» являются:

- прокси-сервер;
- файловый сервер (ЛВС);
- рабочие станции пользователей, планшетные компьютеры, ноутбуки.

Структура системы антивирусной защиты ООО «Вектор» показана на рисунок 25.

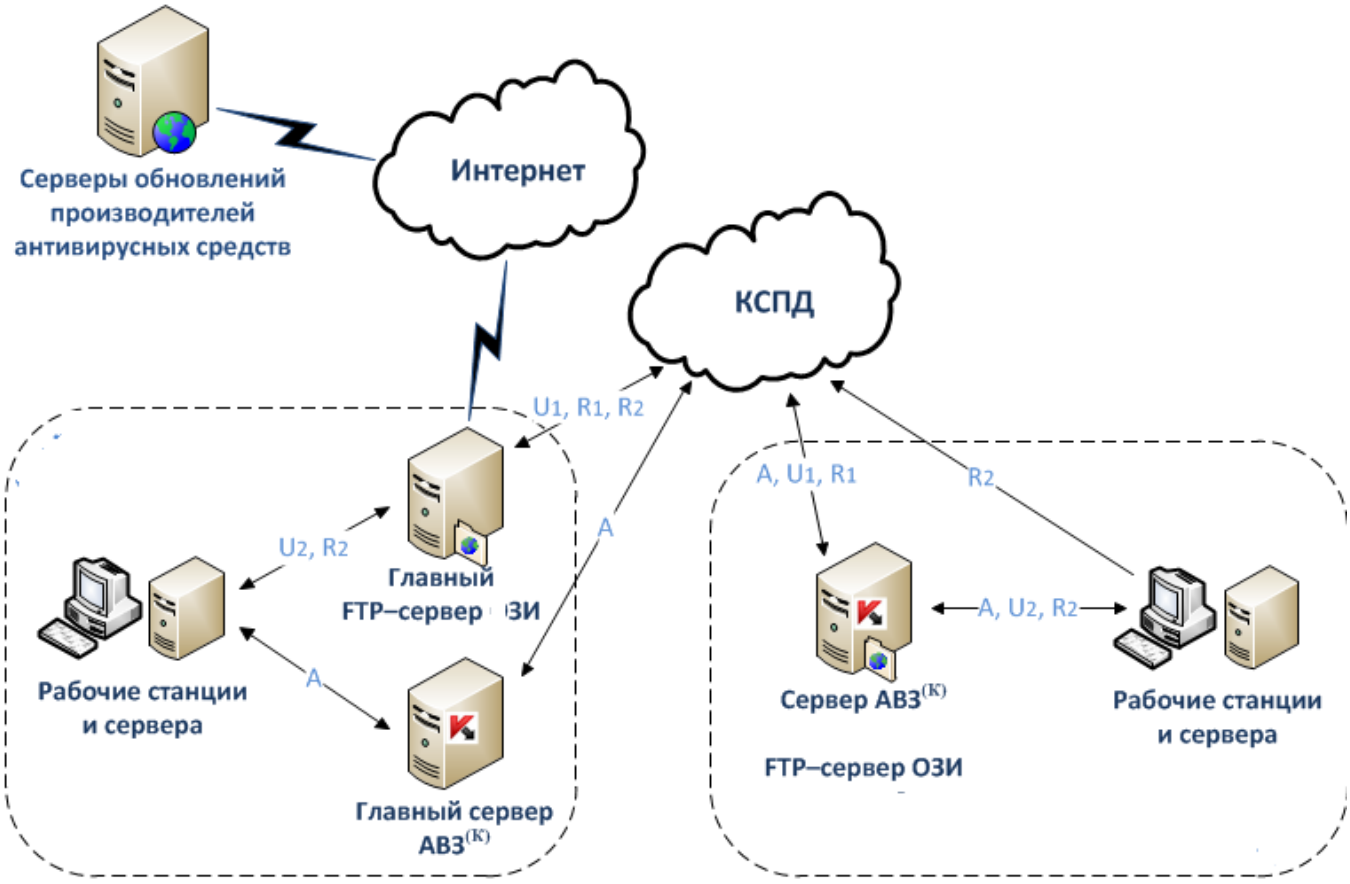

Рисунок 25 - Структура системы антивирусной защиты ООО «Вектор»

В настоящее время используемая версия ПО: Kaspersky End Point Security 10. Автоматическое обновление и администрирование рабочих станций обеспечивается средством Kaspersky Security Center.

В каждом из подразделений Управления ООО «Вектор» приказом назначается ответственный за антивирусную защиту, каждый из которых подчиняется ответственному за АВЗ ИТ-специалисту Управления ООО «Вектор».

Ответственный за АВЗ в подразделениях Управления ООО «Вектор» обязан:

- контролировать выполнение требований антивирусной защиты в своем подразделении;
- администрировать сеть АВЗ в подразделении, поддерживать структуру сети АВЗ;
- своевременно обновлять: антивирусное ПО**,** антивирусные базы, лицензионные ключи на компьютерах входящих в круг ответственности. Поддерживать функционирование антивирусного ПО на компьютерах, входящих в круг ответственности;
- контролировать состояние АВЗ на компьютерах, входящих в круг ответственности;
- доводить до сотрудников в подразделении, в том числе вновь принятых на работу, их права и обязанности по обеспечению АВЗ;
- при получении рекомендаций от ответственного за АВЗ, выполнить указанные действия в указанные сроки;
- предоставлять информацию о состоянии антивирусной защиты по запросу руководства.

Одной из главных задач обеспечения защиты информации является поддержание антивирусных баз в актуальном состоянии, для этого необходимо организовать ежедневное обновление антивирусных баз на

рабочих станциях пользователей и несколько раз в сутки на серверах. Антивирусные базы, будем считать актуальными в течение 3 дней, по истечении данного срока антивирусные базы теряют свою актуальность.

Проведем анализ бизнес-процессов мониторинга состояния информационной безопасности. На рисунок 26 приведена контекстная диаграмма. Как показано на рисунок 26, входящие информационные потоки содержат данные:

- об инженерных коммуникациях Управления ООО «Вектор»;
- об организационной структуре предприятия;
- о деятельности предприятия;
- об архитектуре информационной системы.

Результирующие информационные потоки содержат сводную информацию о состоянии информационной безопасности ООО «Вектор». На рисунок 27 приведена диаграмма декомпозиции основного процесса.

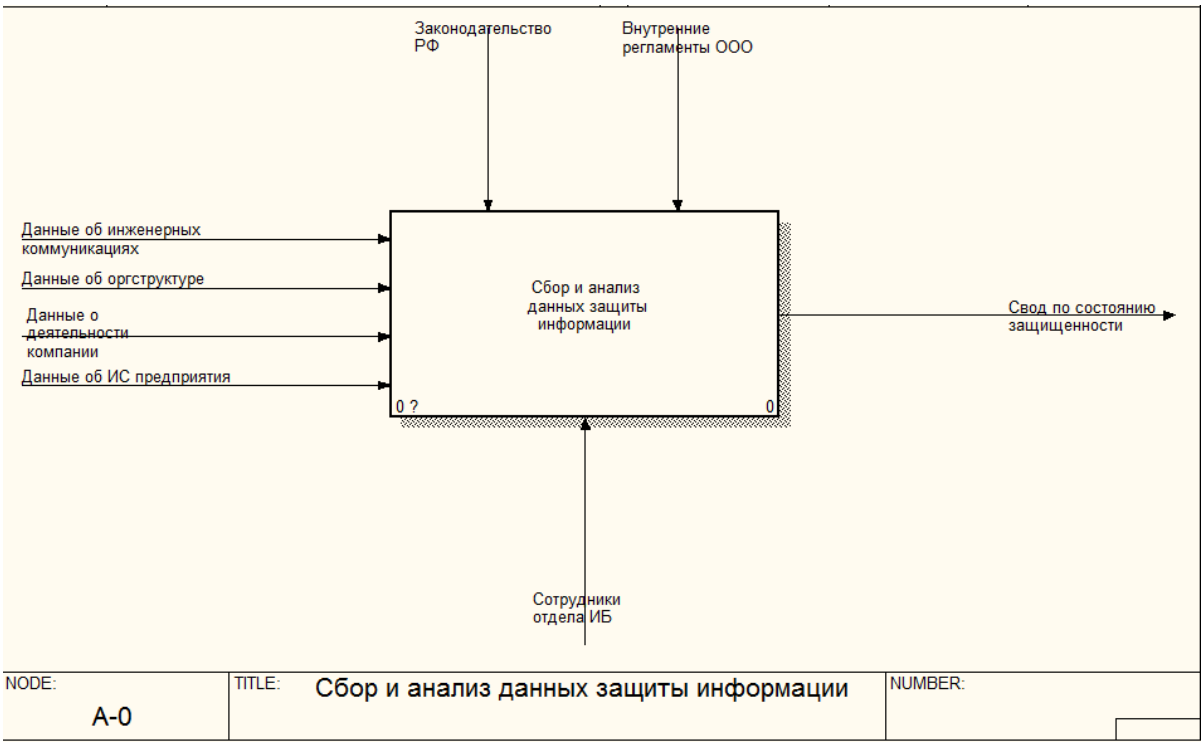

Рисунок 26 - Контекстная диаграмма

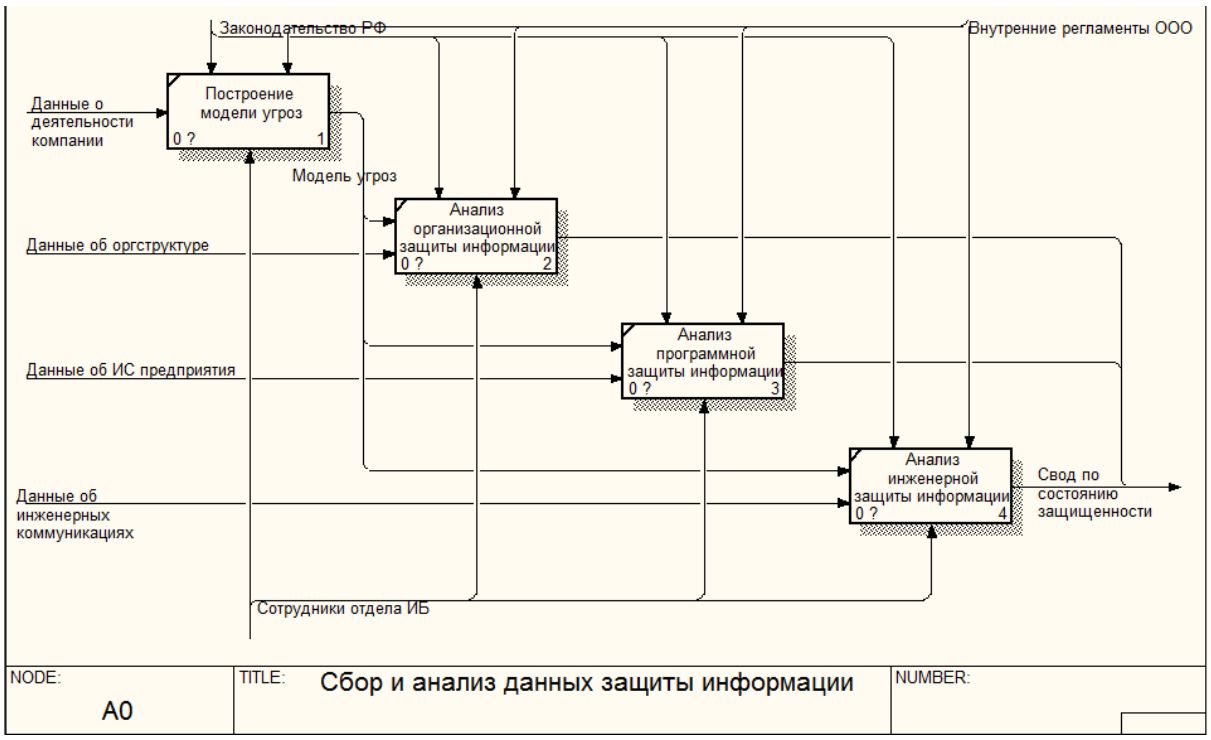

Рисунок 27 - Диаграмма декомпозиции сбора и анализа защиты информации

Как показано на рисунке 26, сбор и анализ состояния информационной безопасности ООО «Вектор» включает следующие виды работ:

- построение модели угроз;
- анализ организационной защиты информации;
- анализ программной защиты информации;
- анализ инженерно-технической защиты информации.

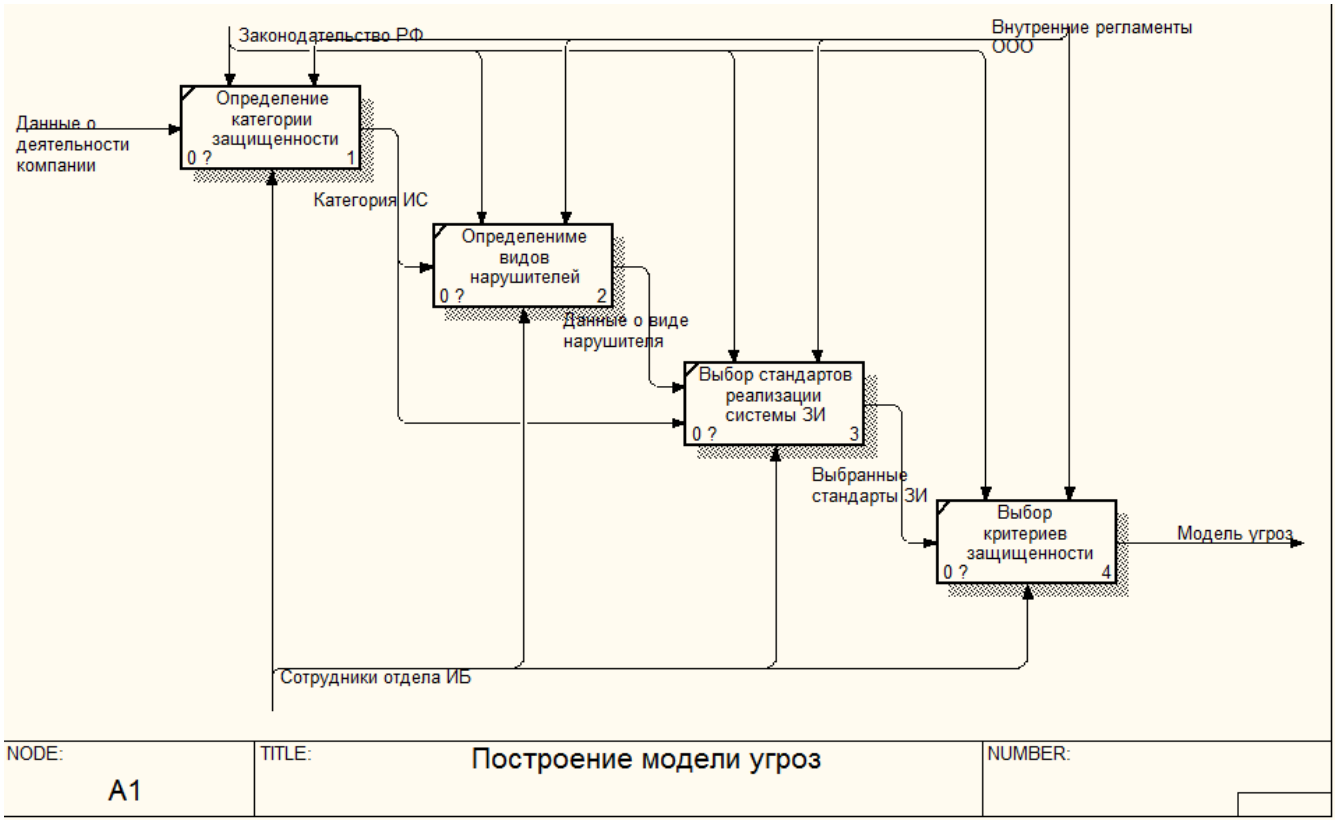

Рисунок 28 - Диаграмма построения модели угроз

Как показано на рисунке 28, для оценки эффективности проводимых работ по защите информации необходимо провести анализ видов обрабатываемой информации в условиях ООО «Вектор», определить категорию обрабатываемых данных. Далее необходимо выбрать стандарт реализации систем защиты информации, соответствующий классу обрабатываемых данных, на основе которого выбираются критерии защищенности системы, по которым проводится дальнейший сбор информации и ее обработка.

На рисунке 29 показаны основные подходы к организации системы защиты информации (анализ организационной структуры предприятия, изучение документации по защите информации, анализ организации системы защиты, оценка качества организации системы защиты).

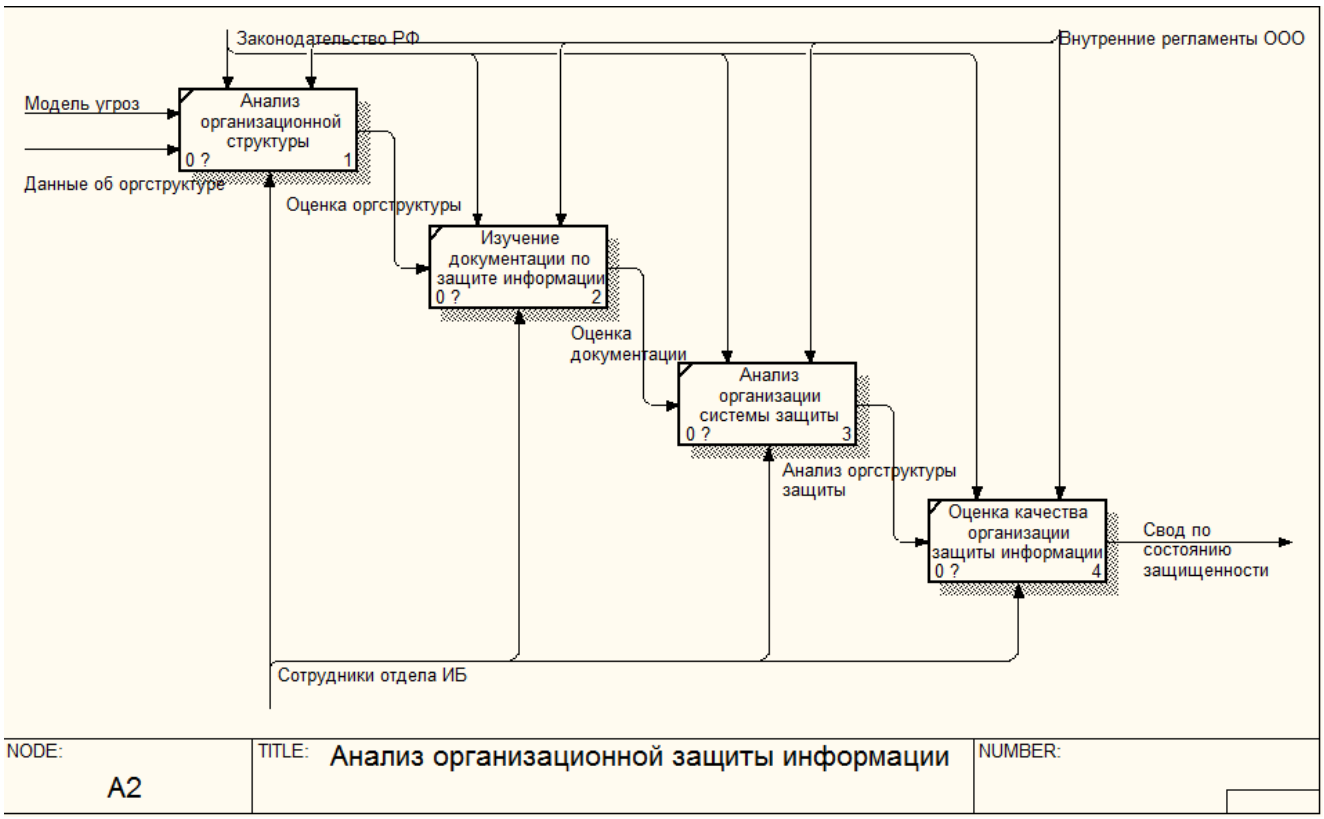

Рисунок 30 - Диаграмма анализа организационной защиты информации

Как показано на рисунке 30, в рамках анализа программной части защиты информации проводится:

- инвентаризация информационных ресурсов ООО «Вектор»;
- определение пользователей и их ролей в контексте их достаточности при выполнении должностных обязанностей;
- оценка эффективности применяемых средств программной защиты информации;
- проведение мониторинга работы программной среды предприятия на предмет соответствия модели угроз.

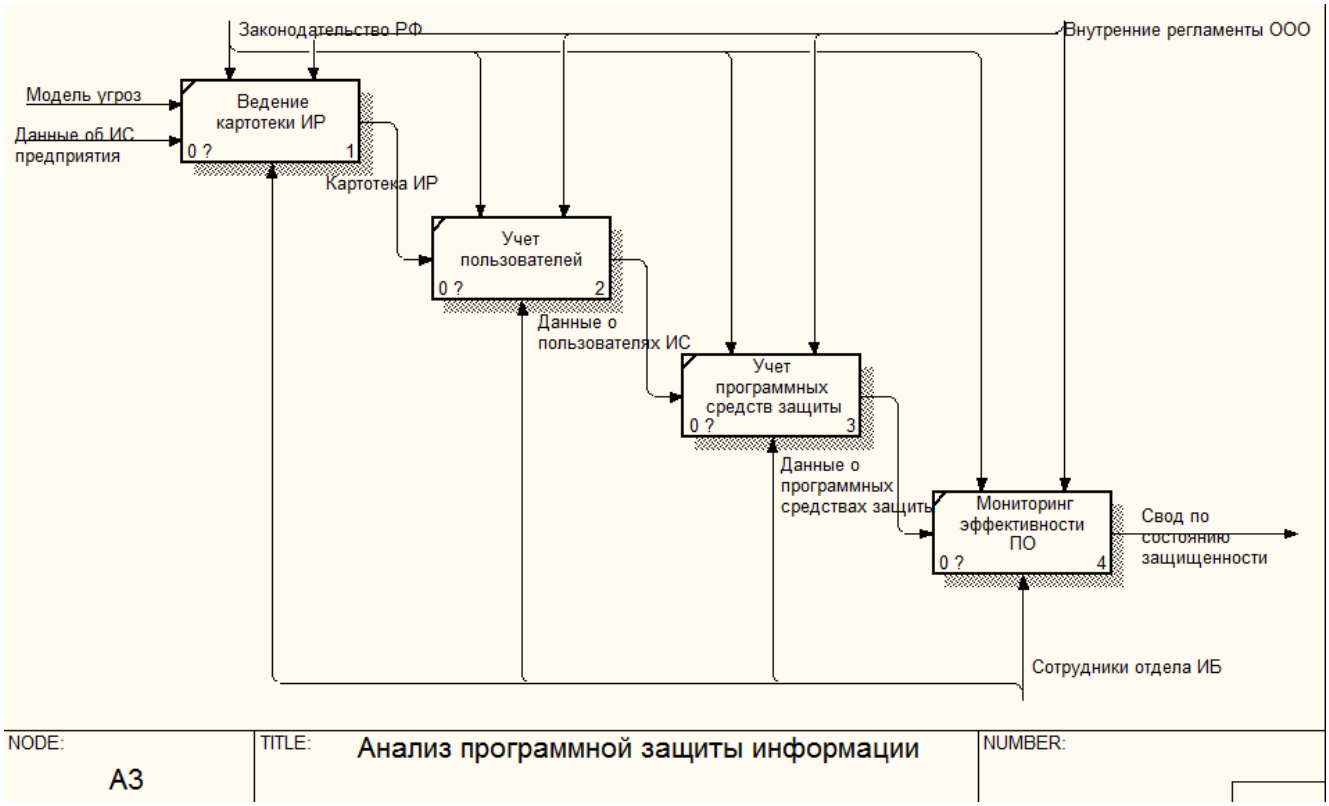

Рисунок 31 - Диаграмма анализа программной защиты информации

Типовыми проблемами в организации сбора информации по защите информации в условиях промышленных предприятий являются:

- отсутствие необходимых программных средств по оценке соответствия документации по защите информации классу информационной системы;
- отсутствие инструментов мониторинга эффективности используемых программных средств и аудита пользовательских учетных записей.

Использование автоматизированной системы для поддержки технологии сбора и анализа данных состояния защищенности информационной системы промышленных предприятий позволит повысить эффективность аудита защищенности. Таким образом, совершенствование бизнес-процесса сбора и анализа данных по защите информации связано с внедрением в работу предприятия программного инструмента, позволяющего решать указанные задачи.

В качестве критериев оценки защищенности локальной сети ООО «Вектор» следует рассматривать следующие:

- скорость работы сетевых приложений (проводится сравнение заявленной производительности сетевых приложений с фактическими);
- использование файрволов, систем шифрования трафика, VPN-систем (анализируется статистика сетевых пакетов);
- стабильность работы Web-сервера компании (анализ скорости работы
  Web-приложений, статистика отказов в обслуживании);
- наличие утвержденных инструкций по работе пользователей с сетевыми ресурсами с доведением их до сотрудников под роспись;
- количество прецедентов в работе сетевых ресурсов, связанных с отказом в обслуживании;
- статистика обнаружения сетевых пакетов, источниками которых не являются установленные сетевые приложения.

Таким образом, совершенствование архитектуры информационной безопасности исследуемой компании связано с использованием сканера безопасности.

В рамках анализа системы защиты информации проводится:

- инвентаризация информационных ресурсов филиала ООО «Вектор»;
- определение пользователей и их ролей в контексте их достаточности при выполнении должностных обязанностей;
- оценка эффективности применяемых средств программной защиты информации;
- проведение мониторинга работы программной среды предприятия на предмет соответствия модели угроз.

В качестве критериев оценки защищенности локальной сети ООО «Вектор» от внешних атак следует рассматривать следующие:

- скорость работы сетевых приложений (проводится сравнение заявленной производительности сетевых приложений с фактическими);
- использование файрволов, систем шифрования трафика, VPN-систем (анализируется статистика сетевых пакетов);
- стабильность работы Web-сервера компании (анализ скорости работы Web-приложений, статистика отказов в обслуживании);
- наличие утвержденных инструкций по работе пользователей с сетевыми ресурсами с доведением их до сотрудников под роспись;
- количество прецедентов в работе сетевых ресурсов, связанных с отказом в обслуживании;
- статистика обнаружения сетевых пакетов, источниками которых не являются установленные сетевые приложения.

В таблице 15 приведена характеристика состояния защищенности информационной системы ООО «Вектор» от основных видов угроз в рамках использования распределенной архитектуры информационной системы.

Таблица 135 - Характеристика состояния защищенности информационной системы ООО «Вектор» от основных видов угроз

Направление защиты информации	Технология	Степень соответствия состоянию защищенности
Антивирусная защита	Kaspersky Security Center	Соответствует
Защита сетевых соединений	VPN	Соответствует
Криптографическая защита	Криптопровайдер ООО «Вектор»	Соответствует
Физическая защита	СКУД Орион	Соответствует
Парольная защита	JaCarta, Indeed-ID	Соответствует
Защита от перехвата информации с использованием специальных средств	Отсутствует	Не соответствует
Защита от действий пользователей, приводящих к инцидентам информационной безопасности	Отсутствует	Не соответствует
Мониторинг активности внешней среды (сканирование уязвимостей)	Отсутствует	Не соответствует
Организационная защита информации	Пакет нормативных документов	Соответствует
Системы резервирования	Acronis	Соответствует
Охранно-пожарная сигнализация	Установлена	Соответствует
Физическая защита помещений	Посты охраны	Соответствует
Использование внешних носителей информации	Регламент использования	Соответствует
Защита от установки нежелательного ПО	Средства мониторинга АВЗ, ограничение прав пользователей, ведение реестра разрешенного ПО	Соответствует
Предоставление доступа к информационным ресурсам	Система документооборота, таблицы управления доступом	Соответствует
Анализ активности учетных записей	Мониторинг активности	Не соответствует

Таким образом, совершенствование архитектуры информационной безопасности ООО «Вектор» необходимо осуществлять в направлениях:

- мониторинга активности внешней среды (сканирование уязвимостей);
- защиты от действий пользователей, приводящих к инцидентам информационной безопасности.

4.2. Оценка экономической эффективности системы

Экономический эффект при внедрении системы достигается за счет сокращения трудозатрат специалистов при выполнении технологических операций.

Оценка эффективности проводится путем сравнения вложенных средств в реализацию проекта с последующим сравнением с полученным выигрышем по трудозатратам специалистов на выполнение автоматизированных операций в денежном выражении. Проект признается эффективным при выявлении превышения полученного эффекта над вложенными затратами [7].

При разработке проекта автоматизации внедрения систем администрирования распределенной сети был составлен календарный план, представленный в таблице 16.

Таблица 146 - Хронологический порядок внедрения программного продукта в технологию работы

Название задачи	Длительность	Начало	Окончание	Предшественники	Ресурсы
Анализ предметной области	5 дней	Чт 10.01.21	Ср 16.01.21		
Изучение функций специалистов	2 дней	Чт 10.01.21	Пт 11.01.21		ИТ-специалист; Специалист по ИБ
Моделирование бизнес-процессов	2 дней	Пн 14.01.21	Вт 15.01.21	2	ИТ-специалист; Специалист по ИБ

Продолжение таблицы 16

Постановка задач автоматизации	1 день	Ср 16.01.21	Ср 16.01.21	3	ИТ-специалист; Специалист по ИБ
Разработка технического задания	3 дней	Чт 17.01.21	Пн 21.01.21	4	ИТ-специалист; Специалист по ИБ
Реализация системы	21 дней	Вт 22.01.21	Вт 19..02.21	5	ИТ-специалист; Специалист по ИБ
Выбор программного решения	3 дней	Вт 22.01.21	Чт 24.01.21		ИТ-специалист; Специалист по ИБ
Установка приложений	7 дней	Пт 25.01.21	Пн 04..02.21	7	ИТ-специалист; Специалист по ИБ
Тестирование приложения	5 дней	Вт 05..02.21	Пн 11..02.21	8	ИТ-специалист; Специалист по ИБ
Развертывание ПО	6 дней	Вт 12..02.21	Вт 19..02.21	9	ИТ-специалист; Специалист по ИБ
Опытная эксплуатация	5 дней	Ср 20..02.21	Вт 26..02.21	10	ИТ-специалист; Специалист по ИБ
Разработка документации	8 дней	Ср 27..02.21	Пт 08..03.21		ИТ-специалист; Специалист по ИБ
Разработка руководства пользователя	4 дней	Ср 27..02.21	Пн 04..03.21	11	ИТ-специалист; Специалист по ИБ
Разработка руководства администратора	2 дней	Вт 05..03.21	Ср 06..03.21	13	ИТ-специалист; Специалист по ИБ
Оформление акта приемки	2 дней	Чт 07..03.21	Пт 08..03.21	14	ИТ-специалист; Специалист по ИБ

Первоначально производится анализ специфики технологии администрирования распределенной сети. На этом этапе задействован ИТ-специалист, а также сотрудники в области информационной безопасности. Документация для разработки проекта предоставляется специалистами компании, другими структурными подразделениями, руководителем компании. Также проводится оценка возможностей внедрения готовых программных решений, либо самостоятельной разработки информационной системы специалистами компании.

В рамках реализации проектной части проводится проектирование физической структуры, рассчитывается стоимость аппаратного комплекса.

Четвертый этап – приобретение программного решения. Задействован специалисты по информационной безопасности.

Следующий этап – опытная эксплуатация – выбранное программное обеспечение устанавливается на тестовые рабочие станции и происходит проверка всего функционала программы с целью выявления ошибок в её работе, соответствия заявленной технологии, определения возможностей усовершенствования. На данном этапе задействованы: руководитель организации, специалист отдела по информационной безопасности, автор данного проекта.

На последнем этапе после исправления неточностей в работе, выявленных в ходе опытной эксплуатации, происходит внедрение программного продукта в промышленную эксплуатацию через развертывание базы данных, установку программы на рабочие станции пользователей. Задействован разработчик данного проекта.

Проведем оценку средств, необходимых для реализации проекта автоматизации [4].

1. Оценка трудовых затрат.

Для реализации проекта привлечены:

- Разработчик программного обеспечения;
- Специалист отдела по работе с клиентами;
- Экономист.

В таблице 17 приведена оценка трудозатрат специалистов, привлеченных к реализации проекта автоматизации технологии работы администратора распределенной сети.

Таблица 17 - Оценка трудозатрат специалистов, привлеченных к реализации проекта автоматизации

№	Специалист	Количество	Часовая заработная плата, руб.	Количество часов	Итого, руб.
1	ИТ-специалист	1	250	80	20000
2	Специалист отдела по информационной безопасности	5	220	30	33000
3	Экономист	2	270	8	4320
	Итого				57320

Расчет сумм страховых взносов (30% фонда заработной платы):

$S_1 = 0.3*57320 = 17196$ руб.

2. Учет оплаты за электроэнергию.

При работе над проектом предполагается использование компьютерной техники, установленной на рабочих местах специалистов.

Количество часов использования компьютерной техники составляет 150. Потребляемая мощность – 0,6кВт. Тариф за 1кВт*ч составляет 4 рубля.

Расходы на электроэнергию составляют:

$S_2 = 0.6*150*5 = 4500$ руб.

Расходы на материалы, включающие бумагу, канцелярские товары, картриджи и др. зарезервированы в размере 10000руб.

Также необходимо приобретение лицензий на программное обеспечение, на необходимое количество рабочих мест на сумму 48000руб.

Таким образом, общая величина затрат на создание программного обеспечения составляет: 57320+17196+3600+10000+48000=136116 руб.

Далее проведем оценку сокращения трудозатрат на выполнение основных технологических операций на рабочих местах специалистов ООО «Вектор» (таблица 18).

Таблица 18 - Оценка сокращения трудозатрат на выполнение основных технологических операций на рабочих местах специалистов

Наименование операции	Количество операций в год	Время выполнения по базовой технологии, час.	Время выполнения по внедряемой технологии, час.	Сокращение временных затрат на одну операцию	Общее снижение трудозатрат
Установка обновлений ПО	700	0.5	0.05	0.45	315
Сканирование состояния сегментов распределенной сети	600	0.5	0.05	0.45	270
Работа с журналом событий	1200	0.5	0.05	0.45	540
Ведение картотеки объектов информационной системы	12	4	0.2	3.8	45.6
Выборки по журналам работы сети	12	4	0.2	3.8	45.6
Формирование сводного отчета	12	4	0.2	3.8	45.6
Итого					1261.8

Таким образом, оценка годового сокращения затрат на реализацию проекта составляет 1262 часа. В денежном выражении (при средней часовой сумме заработной платы специалистов, использующих ПО в 200 руб.) величина экономии составляет 252400руб.

Период окупаемости проекта:

$$T = \frac{136116}{252400} = 0.54\text{года} = 6{,}5\text{мес.}$$

Далее проведем оценку внутренней ставки доходности проекта с использованием функции ВСД, аргументы которой приведены на рисунке 32.

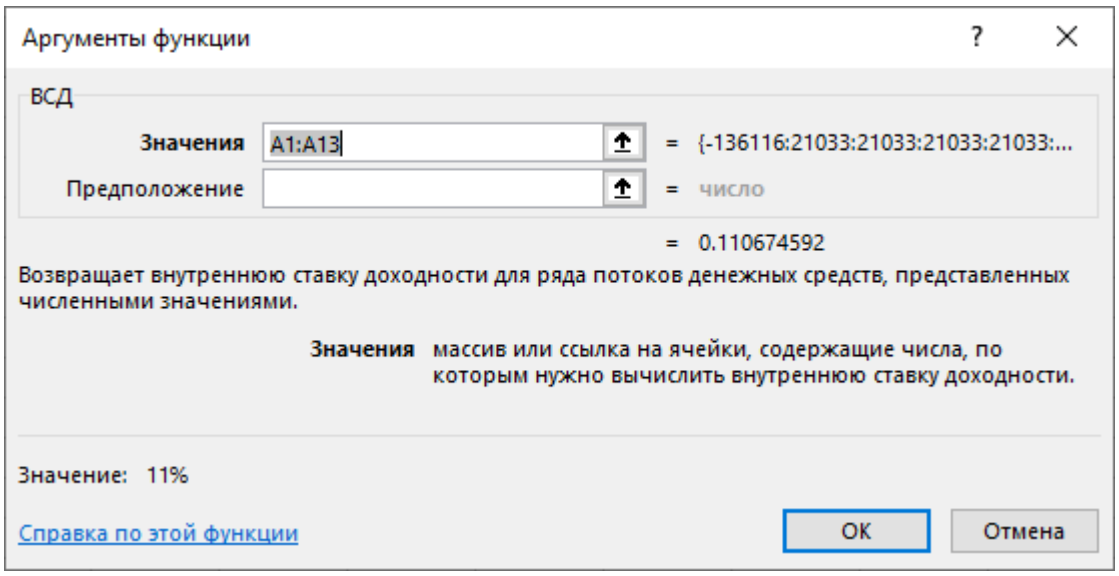

Рисунок 32 – Аргументы функции ВСД

Расчет суммы ВСД показывает величину доходности 11%, что превышает величину ключевой ставки, составляющей 4,25%. таким образом, проект внедрения системы можно признать эффективным [19].

Заключение

Для достижения поставленной цели выпускной квалификационной работы были выполнены определенные задачи, которые раскрываются в рамках данной работы.

Рассмотрены теоретические основы использования распределенной архитектуры информационной системы. Были определены цели, этапы проведения и виды активного аудита информационной безопасности; основные уязвимости информационной безопасности и рассмотрены сканеры уязвимостей MaxPatrol 8 и OpenVAS.

Произведен анализ деятельности ООО «Вектор», в ходе которого были определены объекты защиты ООО «Вектор», к которым относятся базы данных распределенной архитектуры, содержащие конфиденциальные сведения, коммерчески значимая информация, персональные данные и криптографические системы. Обеспечение защиты указанных ресурсов требует применения специальных инструментов мониторинга обеспечения информационной безопасности.

Описана система защиты информации. Рассмотрена система антивирусной защиты, принятая на предприятии, состоящая из Kaspersky End Point Security 10 и Kaspersky Security Center. Рассмотрены цели и принципы АВЗ и описана организационная структура АВЗ.

Проведен в ООО «Вектор» аудит информационной безопасности с использованием сканера безопасности Nessus. В ходе проведенного сканирования информационной системы ООО «Вектор» были обнаружены инциденты информационной безопасности, причинами которых могут являться уязвимости, связанные с ошибками в конфигурировании межсетевых экранов, настройки системы антивирусной защиты, прав доступа к файловым ресурсам, а также управления парольной защитой.

Таким образом, совершенствование системы защиты информации ООО «Вектор» предполагает необходимость проведения ряда мероприятий по настройке антивирусного ПО (в рамках которого также реализована распределенная архитектура), разграничению доступа к информационным ресурсам, использовании систем защиты от СПАМа, ограничение использования flash-накопителей.

Список используемых источников

1. Организация системы аудита информационной безопасности. [Электронный ресурс]. Режим доступа: http://mirznanii.com/a/19714/organizatsiya-audita-informatsionnoy-bezopasnosti-informatsionnoy-sistemy

2. Сканер уязвимостей Nessus. Описание. [Электронный ресурс]. Режим доступа: https://networkguru.ru/tenable-nessus-vulnerability-scanner/

3. Сканирование уязвимостей в ИТ-инфраструктуре. Обзор программных продуктов. [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/tenable-analysis-security-corporate-infrastructure.

4. Сравнение программных продуктов – сканеров уязвимостей. [Электронный ресурс]. Режим доступа: https://www.tiger-optics.ru/resources/tenable-sc-maxpatrol/?yclid=1913900678926858974

5. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова; Минобрнауки России, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования "Ухтинский гос. технический ун-т" (УГТУ). - Ухта : УГТУ, 2016. - 69 с.

6. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки : [учебное пособие] / А. В. Кондратьев. - Москва : Горячая линия - Телеком, 2016. - 304 с.

7. Бабиева Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Бабиева. - Казань: Медицина, 2018. – 127

8. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2015. – 314 с.

9. Блинов А.М. Информационная безопасность. – СПб: СПбГУЭФ, 2015 - 96с.

10. Шалак М. Е. Архивное дело и делопроизводство: учебное пособие / М. Е. Шалак; РОСЖЕЛДОР. - Ростов-на-Дону : ФГБОУ ВО РГУПС, 2017. - 78 с.

11. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишерз, 2015. – 338с.

12. Гришина Н.В. Комплексная система защиты информации на предприятии. – М.: Форум, 2010. – 240 с.

13. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.

14. Емельянов, С.В. Информационные технологии и вычислительные системы: Интернет-технологии. Математическое моделирование. Системы управления. Компьютерная графика / С.В. Емельянов. - М.: Ленанд, 2012. - 96 с.

15. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. – М.: Форум, 2009. – 368 с.

16. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

17. Завгородний В.И. Комплексная защита в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001. - 264 с.

18. Калашян, А.Н. Информационные системы в экономике: В 2-х ч. Ч.2. Практика использования: Учебное пособие / А.Н. Калашян. - М.: Финансы и статистика, 2006. - 240 с.

19. Корнеев И.К, Степанов Е.А. Защита информации в офисе. – М.: ТК Велби, Проспект, 2008. – 336 с.

20. Лопатин Д. В. Программно-аппаратная защита информации: учебное пособие / Лопатин Д. В. - Тамбов: ТГУ, 2014. – 254с.

21. Никифоров С. Н. Защита информации : учебное пособие / С.Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2017. – 76с.

22. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишерз, 2011 – 338с.

23. Ожиганов А.А. Криптография: учебное пособие / А.А. Ожиганов. - Санкт-Петербург : Университет ИТМО, 2016. - 142 с

24. Никифоров С. Н. Защита информации. Шифрование: учебное пособие / С. Н. Никифоров, М. М. Ромаданова. - Санкт-Петербург: СПбГАСУ, 2017. - 129

25. Радько, Н.М. Основы криптографической защиты информации [Электронный ресурс]: учебное пособие / Н. М. Радько, А. Н. Мокроусов; Воронеж. гос. техн. ун-т. - Воронеж : ВГТУ, 2014.

26. Skone S. and de Jong M. The impact of geomagnetic substorms on GPS receiver

27. Zhibo Wen. Estimation of Code and Phase Biases in Satellite Navigation // Master Thesis, Institute for Communications and NavigationTechnische Universif’at M’unchen, 2010.

28. Bainey Kenneth. Integrated IT Performance Management. Auerbach Publications, 2016. 421 p.

29. Castillo F. Managing Information Technology. Springer, 2016. 246 p.

30. Evans A., Martin K., Poatsy M.A. Technology in Action. Complete. 12th Ed., Global Edition. — Pearson, 2016. 628 p.