Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации

Утверждена распоряжением по институту
от «23» сентября 2019 г. № 089-р/12.00
Выполнена по заявке организации (предприятия)

Допущена к защите
« 12 » декабря 2019 г.
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ФОРМИРОВАНИЕ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ

Рецензенты:
Гладских Виктор Николаевич
канд. техн. наук, доцент
директор ИП Гладских В.Н.

Нормоконтролер:
Мандрица Игорь Владимирович
доктор эконом. наук, доцент,
профессор кафедры организации и технологии защиты информации

(*подпись*)

Дата защиты «14» декабря 2019 г.

Оценка

Выполнил (а):
Васильев Василий Андреевич
студент 3 курса, группы ИНБ-м-оз-17-1 направления подготовки 10.04.01 «Информационная безопасность» направленность «Комплексная защита объектов информатизации» очно-заочной формы обучения

(*подпись*)

Руководитель:
Мандрица Игорь Владимирович
доктор экон. наук, профессор,
профессор кафедры организации и технологии защиты информации

(*подпись*)

Ставрополь, 2019 г.

СОДЕРЖАНИЕ

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации
Направление Информационная безопасность
Направленность Комплексная защита объектов информатизации

УТВЕРЖДАЮ
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко
«30» сентября 2019 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ (ДИПЛОМНУЮ РАБОТУ)

Студент Васильев Василий Андреевич группа ИНБ-м-оз-17-1
1. Тема Формирование стратегии информационной безопасности бизнес-процессов организации
Утверждена распоряжением по институту «14» декабря 2019 г. № 089-р/12.00
2. Срок представления работы к защите «12» декабря 2019 г.
3. Исходные данные для выполнения работы Работу выполнить в соответствии с требованиями ФЗ №152-ФЗ «О персональных данных»
4. Содержание ВКР:
4.1 Теоретические основы современных методик информационной безопасности для Бизнес-процессов
4.2 Основы информационной безопасности бизнес-процессов организации
4.3 Описание бизнес-процесса организации для целей создания моделей информационных угроз
4.4 Факторы влияющие на разработку стратегии информационной безопасности
4.5Теоретические основы стратегического моделирования информационной безопасности
4.6 Разработка математической модели для выбора типа стратегии информационной безопасности бизнес-процесса организации
4.7 Методика технико-экономического обоснования выбора стратегии информационной безопасности
Приложение
Дата выдачи задания «30» сентября 2019 г.
Руководитель работы И. В. Мандрица
(*подпись*) (*инициалы, фамилия*)
Консультанты по разделам
(*подпись*) (*инициалы, фамилия*)
(*подпись*) (*инициалы, фамилия*)
(*подпись*) (*инициалы, фамилия*)
Задание к исполнению принял «30» сентября 2019 г. В. А. Васильев

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации
Направление Информационная безопасность
Направленность Комплексная защита объектов информатизации

КАЛЕНДАРНЫЙ ПЛАН

Фамилия, имя, отчество Васильев Василий Андреевич
Тема ВКР Формирование стратегии информационной безопасности бизнес-процессов организации
Руководитель Мандрица И. В.
Консультанты:

№	Наименование этапов выполнения выпускной квалификационной работы	Срок выполнения работы	Примечание
1.	Анализ литературы по теме работы	01.10.2019	
2.	Рассмотрение теоретических основ разработки стратегии информации безопасности и основных проблем теории	02.10.2019	
3.	Теоретические основы современных методик стратегического моделирования информационной безопасности	08.10.2019	
4.	Описание бизнес-процесса организации для целей создания моделей информационных угроз	15.10.2019	
5.	Теоретические основы стратегического моделирования кибербезопасности организации	28.10.2019	
6.	Разработка математической модели выбора типа стратегии для бизнес-процесса организации	05.11.2019	
7.	Представление ВКР руководителю и нормоконтролёру	12.11.2019	
8.	Предварительная защита	07.12.2019	
9.	Рецензирование	09.12.2019	
10.	Представление ВКР заведующему кафедрой	12.12.2019	
11.	Представление ВКР в ГЭК	14.12.2019	

Руководитель И. В. Мандрица
Зав. кафедрой В.И. Петренко

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ВКС – видеоконференцсвязь

ИБ – информационная безопасность

ИСПДн – информационная система персональных данных

ОИ – объект информатизации

ПО – программное обеспечение

СБИС – система бухгалтерского и складского учёта

СКУД – система контроля управления доступом

СМИБ – система менеджмента информационной безопасности

СМК – система менеджмента качества

ССП – сбалансированной системы показателей

СТП – стандарты предприятия

ТЗ – техническое задание

ТС – техническая система

ЭВМ – электронно-вычислительная машина

ВВЕДЕНИЕ

Кибербезопасность представляет одним из высших приоритетов в промышленности, научных кругах и правительствах любой страны, в которой национальная безопасность учитывает киберугрозы.

Обмен информацией об уже имеющихся киберугрозах между различными коммерческими компаниями и государственными организациями может обеспечить максимальное обнаружение уязвимостей при минимальных затратах. Налаженный обмен информацией о киберугрозах имеет ряд преимуществ.

Во-первых, это уменьшает вероятность того, что злоумышленник будет использовать одну и ту же уязвимость для атак в разных организациях. Во-вторых, это снижает вероятность того, что злоумышленник может обойти защиту организацию и собрать данные, которые помогут ему начать атаку на другие организации.

Киберпространство имеет множество взаимосвязей, и владельцы особенно важных инфраструктур зависят друг от друга. Эта известная проблема кибервзаимозависимости усугубляется в общедоступной облачной вычислительной платформе. Совместные усилия коммерческих компаний и государственных организаций по разработке контрмер для кибер-нарушения снижают затраты каждой фирмы на инвестиции в кибер-защиту.

Несмотря на многочисленные преимущества, обмен информацией о киберугрозах сопряжен с определенными издержками и рисками. Когда фирма передаёт в банк угроз свои обнаруженные уязвимости в общее хранилище данных с другими компаниями и организациями, существует риск того, что эта информация будет перехвачена злоумышленниками, что приведет к потере репутации, доли рынка и доходов.

Поэтому, в этой стратегической среде организации, лица обязанные делиться информацией о киберугрозах, могут не делиться правдивой информацией из-за своих собственных интересов.

Кроме того, некоторые эгоистично действующие фирмы могут намеренно ограничивать свои инвестиции в кибербезопасность и полагаться на информацию, которую предоставят другие организации, чтобы защитить себя. Это может привести к недостаточным инвестициям в кибербезопасность, если все участники примут одну и ту же стратегию.

Ущерб, причиняемый кибератаками, становится все больше, шире и серьезнее и включает в себя финансовые и стратегические потери. Некоторые кибератаки, предположительно, являются частью интересов национальных или государственных кампаний.

Российские компании активно инвестируют в защиту от хакерских атак. В 2018 году инвестиции в информационную безопасность в IT-бюджетах увеличились до 22%. Средний IT-бюджет бизнеса в Российской Федерации составил $1,1 млн. В ближайшие три года произойдёт рост ещё на 18% из-за того, что инфраструктура информационных технологий в компаниях развивается, и им необходимы профессиональные знания по кибербезопасности, говорится в проведённом исследовании «Лаборатории Касперского».

Финансовый ущерб российских компаний от утечек данных возрос за последние полгода. Для крупного бизнеса он примерно составил $246 тыс., на 2,5% больше, чем в прошлом году, говорится в исследовании «Лаборатории Касперского». Для среднего – вырос втрое – до $74 тыс.

Однако, рассматривая развитие технологий и навыков злоумышленников, и потенциала других стран, считается, что более важно пересмотреть национальную стратегию по укреплению потенциала кибербезопасности и обеспечить адекватное развитие национального потенциала в ближайшие годы.

В ходе выполнения работы необходимо решить следующие частные задачи:

– анализ развития современного состояния зарубежного опыта и законодательства в области регистрации информационных угроз и кибербезопасности,

– разработка рекомендаций (предложений и мероприятий) по мониторингу, регистрации, идентификации информационных угроз и моделированию стратегии кибербезопасности организации,

– оценка предложенных мероприятий для моделирования эффективной стратегии кибербезопасности организации.

Объектом исследования является действующая система информационной безопасности бизнес-процесса организации.

Предметом исследования является действующий бизнес-процесс и текущая стратегия информационной безопасности организации.

Целью исследования является разработка методики выбора стратегии информационной безопасности бизнес-процесса организации, посредством комбинаторного подбора факторов математической модели минимально-достаточного уровня защищенности информационных активов организации для противостояния угрозам бизнес-процессу в рамках стратегии разноуровневых предложений по восстановлению и противодействию информационным угрозам организации

1 Теоретические основы современных методик регистрации и идентификации информационных угроз

1.1 Основы кибербезопасности и современные проблемы теории

Согласно существующих в информационном пространстве данных, кибербезопасность – это, раздел информационной безопасности, в рамках которого изучают процессы формирования, функционирования и эволюции киберобъектов, для выявления источников киберугроз (киберопасности), образующихся при этом, определение их характеристик, а также их классификацию и формирование нормативных документов, выполнение которых должно гарантировать защиту киберобъектов от всех выявленных и изученных источников киберопасности.

Кибербезопасность – процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных. Системный администратор, как лицо ответственное за кибербезопасность, обеспечивает защиту активов организации, включая данные локальной сети компьютеров, серверов и всех участников (пользователей) сети организации. Кроме того, под охрану берутся непосредственно здания, сооружения, объекты инфраструктуры организации и, самое главное, персонал.

Целью обеспечения кибербезопасности является защита всей информации, циркулирующей в организации (как в процессе передачи и/или обмена, так и находящихся на хранении).

В настоящее время в целях обеспечения безопасности информации могут быть применены контрмеры. Некоторые из этих мер включают (но не ограничиваются) контроль доступа, обучение персонала, аудит и отчётность кибербезопасности, оценку вероятных рисков, анкетирование пользователей, тестирование возможных каналов угроз на проникновение и требование авторизации (аутентификации).

В свою очередь информационная безопасность (англ. Information Security, а также – англ. InfoSec) – это, практика предотвращения

несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная, или, например, физическая).

Основная задача информационной безопасности – сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.

Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками.

В свою очередь согласно методологическим основам кибербезопасности с позиции известной фирмы CISCO , как теоретического задела для настоящего исследования под кибербезопасностью понимается - реализация мер по защите систем, сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний. Принципы в основе кибербезопасности по мнению специалистов фирмы CISCO заложены в успешном подходе в сфере кибербезопасности выражаются в виде многоуровневой защиты, охватывающей компьютеры, сети, программы или данные, которые необходимо обезопасить.

Сотрудники, рабочие процессы и технологии должны дополнять друг друга в организациях, чтобы обеспечить эффективную защиту от кибератак. Пользователи должны понимать и соблюдать основные принципы информационной безопасности, такие как выбор надежных паролей, внимательное отношение к вложениям в электронных письмах и резервное

копирование данных. Дополнительная информация об основных принципах кибербезопасности. Процессы кибербезопасности в организации должны быть разработаны как некий успешный и эффективный набор базовых мер по противодействию предпринимаемым хакерами успешно осуществленным ими атакам извне информационной и электронной среды. В таблице 1 представлены типы современных угроз кибербезопасности.

Допускается руководствоваться одним надежным набором мер. В таком наборе мер должно объясняться, как определять атаки, защищать системы, выявлять угрозы и противодействовать им, а также восстанавливать работоспособность после осуществленных атак.

Технологии кибербезопасности являются важнейшим элементом, предоставляющим организациям и отдельным пользователям инструменты, необходимые для защиты от кибератак.

Основными компонентами, которые подлежат защите, являются оконечные устройства, например, компьютеры, интеллектуальные устройства и маршрутизаторы; сети и облачная среда. К наиболее распространенным технологиям, используемым для защиты перечисленных компонентов, относятся межсетевые экраны нового поколения, фильтрация DNS, защита от вредоносного ПО, антивирусное ПО и решения для защиты электронной почты.

Перекликающиеся понятия: Киберпространство - пространство, где функционируют и взаимодействуют киберобъекты.

Кибербезопасность объекта - свойство последнего, характеризующее его возможность не быть причиной образования ущерба для киберпространства.

Киберзащищенность объекта – свойство последнего, характеризующее его возможность предотвращать образование ущерба от хакерских кибератак или уменьшать величину такого поражения.

Таблица 1– Типы современных угроз кибербезопасности

Тип киберугрозы	Описание
Социоинженерные способы	Рассылка от друзей в социальных сетях (вконтакте, одноклассники и др.), нагло всплывающие фейковые страниц «онлайн проверки системы или обновления ПО» с предложением проверить компьютер на вирусы или обновить программы до последних версий.
Уязвимости нулевого дня	«Нулевой день» обозначает время с момента обнаружения уязвимости разработчиками программного обеспечения. Уязвимость нулевого дня представляет собой баг в системе безопасности программы, который может быть использован в браузере или программе.
Фишинг (фарминг)	Вид интернет-мошенничества, цель которого – получить конфиденциальную информацию пользователей. Сюда можно отнести кражи паролей, номера и данные кредитных карт, банковских счетов и другой конфиденциальной информации. Фишинг представляет собой пришедшие на почту фейковые уведомления или инвойсы от банков, провайдеров, платежных систем и других фирм о том, что по какой-либо причине получателю срочно нужно передать или обновить свои личные данные.
Усовершенствованные постоянные угрозы	Постоянное развитие уже существующих угроз является одним из самых распространённых способов изменения определённого кода в вирусной программе, и тем самым, её не определением у антивируса как угрозы. Разработчики вредоносного ПО тратят меньше усилий на обновление таких угроз.
Мобильные устройства	В связи с тем, что все больше сервисов и рекламы внедряются на мобильные устройства и планшеты, тем самым существенно возрастают случаи всплывания вредоносной рекламы, т. е. практики её навязывания в легальные рекламные онлайн-сети рекламы, привлекающие своё внимание к вредоносному ПО.
Облачные технологии	Облачные вычисления в силу массового использования системных ресурсов требуют надежной защиты пользовательских данных друг от друга. Передаваемая и хранимая в защищённой системе облачных вычислений информация может быть скомпрометирована или фальсифицирована в обход правил и процессов обеспечения безопасности в результате эксплуатации возможных уязвимостей на различных уровнях системы облачных вычислений.
Уязвимости Интернета вещей (IoT)	Удаленный доступ к этим организациям может быть удобен для решения проблем в нерабочее время или критических ситуациях, но также создает большую угрозу уязвимости сети.

Однако согласно мнения авторитетного специалиста в этой области. Касперской директора фирмы InfoWatch на ноябрь 2018 года понятие «кибербезопасность» хотя и является ключевым в современной системе определения угроз, но в стране сложилась довольно парадоксальная ситуация

– с тем, что существуют киберугрозы, но отсутствует понятие кибербезопасности как таковое. Понятие есть, но оно законодательно не определено.

Согласно проектной документации не принятой, но рассмотренной правительством РФ в 2014 году в составе «Концепции стратегии кибербезопасности в РФ» под кибербезопасностью понимается (предлагалось понимать) та совокупность условий, при которой все объекты киберпространства защищены от максимально возможного количества угроз, а также воздействий с нежелательными последствиями.

При этом, когда мы говорим «киберугроза» или «кибербезопасность», все прекрасно понимают, о чем идет речь. Однако законодательно оно не определено.

Существующее понятие «Информационная безопасность» – это совокупность информации, которая должна быть защищена определенными принципами: целостности, конфиденциальности, доступности. К примеру, может существовать вирусная атака, которая не нарушает конфиденциальности информации. Но может быть троянский вирус – который просто внедряется в корпоративное ПО и наблюдает. И с этой точки зрения он не представляет собой препятствия – поскольку вирусы и прочие угрозы, наподобие закладок, должны быть специальным образом определены».

Киберпреступность, по определению, совершает незаконный акт с использованием компьютера или сетевого устройства. Киберпреступники используют сложные методы для получения несанкционированного доступа к информационным системам.

Некоторые из творческих методов, которые могут использовать злоумышленники, – это бэкдор-программы, фишинг-атаки и социальная инженерия. Существует ряд хорошо известных бэкдорных инструментов, которые можно использовать для настройки маршрута, который обходит традиционные механизмы безопасности, позволяя им подключаться к компьютерным системам, например:

– Tini, Netcat,

– Wrappers,

– EXE maker,

– Pretator,

– Restorator и Tetris.

Мотивы хакеров варьируются от кражи конфиденциальной информации работников до прохождения патентов, интеллектуальной собственности и проектов, связанных с защитой (которые имеют гораздо большую ценность, чем кредитные карты).

Защита информационных систем является постоянной экономической проблемой. Стоимость сохранения защиты информации (данных) является дорогостоящей и серьезной. Атаки Киберпреступности ежегодно наносят ущерб в размере 100 миллиардов долларов. Большое количество попыток кибератаки заставляет университеты укреплять свои информационные системы.

Целью информационной безопасности организации является обеспечение конфиденциальности, целостности и доступности формируемых работниками фирмы данных согласно ФЗ-152.

Организация обязаны защищать свои активы, в том числе созданные информационные данные (условные информационные единицы - базы данных), рабочие столы, серверы, здания и, самое главное, работники. Данные могут быть разделены и классифицированы в зависимости от статуса, который необходимо знать. Данные (персональные) работников и руководителей должны быть отделены от общедоступных данных.

Как только данные классифицируются, для обеспечения контроля доступа могут применяться разрешения безопасности.

В настоящее время немногие компании могут функционировать без интернет-ресурсов (электронной почты, онлайн-услуг, корпоративного сайта и т.д.), поэтому блокирование работы организации с помощью DDoS-атаки

может представлять серьезную угрозу для бизнеса, в том числе грозит финансовыми проблемами и утратой доверия клиентов.

Эксперты из «Лаборатории Касперского» рекомендуют компаниям заранее озаботиться безопасностью своих услуг. Выбирая решение для защиты корпоративной ИТ-инфраструктуры от DDoS-атак лучше отдать предпочтение поставщикам, которые имеют прочную позицию на рынке ИТ-безопасности. В результате такой атаки сервера, обслуживающие сайт, вынуждены обрабатывать чрезмерный объём ложных запросов, и сайт становится недоступным для простого пользователя. Популярными жертвами таких атак становятся коммерческие и информационные сайты.

На рисунке 1 представлена динамика данных угроз для и как менялись доли типов угроз информационной безопасности (далее информационной безопасности) в течении 2017 года.

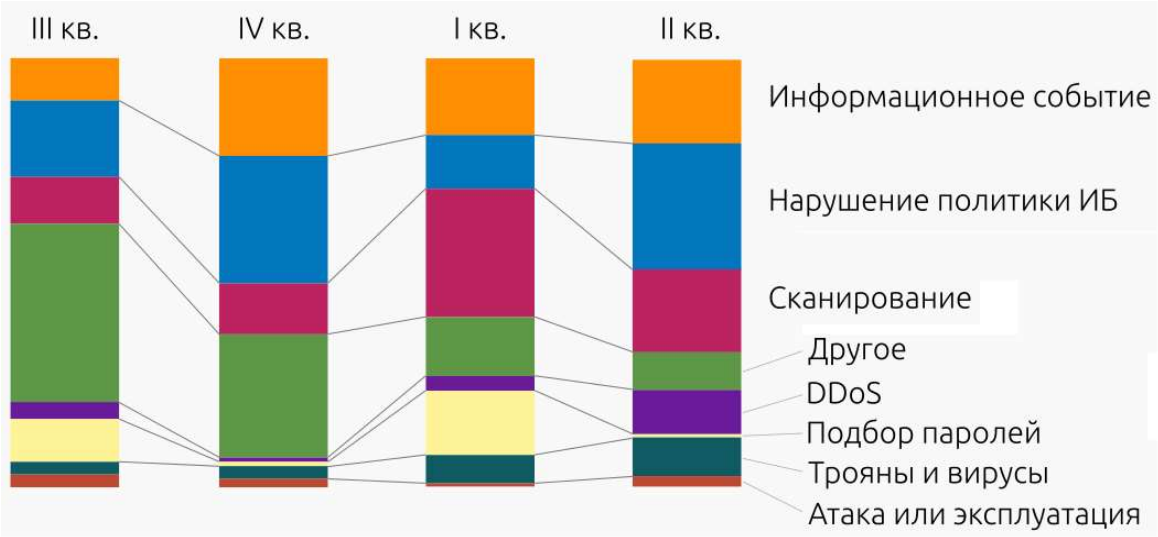

Рисунок 1 – Динамика угроз информационной безопасности в 2017 году на примере нескольких организаций с общим числом подключённых узлов около 15 500 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.)

Хакеры в последнее время используют такой вид атак с целью вымогательства, требуя денег за прекращение атаки, или ведут информационную войну.

В период с 1 апреля по 30 июня 2017 года сотрудники Центра мониторинга контролировали информационные системы нескольких организаций с общим числом подключённых узлов около 15 500 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.).

Компания делает оговорку что, 15 500 узлов это же не только серверы, которые 24 часа на протяжении 365 дней в году генерируют трафик – это еще и пользовательские машины, которые отключаются или бездействуют в выходные/праздники/ночное время, и это сервисы с которыми те же пользователи взаимодействуют в основном только в рабочее время, это виртуальные машины, которые включаются по необходимости.

Не будем забывать про то, что у многих сенсоров есть «трешхолды» агрегирующие множественные события в одно, чтобы избежать флуда.

1.2 Описание бизнес-процесса организации для целей создания моделей информационных угроз

Существует несколько наиболее распространенных причин, по которым руководство (собственники) организации приходят к идее о том, что им нужно описать свои бизнес-процессы. На начальной стадии самого процесса бизнес описания процессов это соответствует всем нормам корпоративного бизнес-планирования и развитого управления данной организацией.

Однако именно неверная организация работ по описанию, оптимизации и внедрению ранее измененных бизнес-процессов, в итоге может принести компанию, затеявшей такую работу, либо к положительным результатам, либо, либо к финансовым проблемам получения доходов от деятельности, а также морально-нравственным потерям в управлении коллективом работками фирмы, и соответственно приостановке самого бизнес-процесса организации.

На сегодня сами проблемы такого подхода полного структурно-логического описания бизнес-процессов делятся на три группы.

Первую группу проблем топ-менеджеры организации описывают в примерно так: «Наш бизнес за последнее время сильно разросся (увеличился), но что-то

в нем стало происходить не так, как было обычно». В качестве финансово-экономических проблем обычно называют следующие:

– возросло количество организационных и межличностных конфликтов, которые можно разрешить только с привлечением собственников (топ-менеджеров),

– непропорционально росту бизнеса возросли операционные затраты (издержки), но совершенно не понятна причина этого,

– возросло количество технических проблем связанных с производством и обслуживанием клиентов, таких как срыв сроков, брак, равнодушие, хамство персонала фронт-офиса,

– организация начинает проигрывать своим более мелким конкурентам в качестве, быстроте оказанных услуг и продуктов на рынке.

Вторая группа проблем применения бизнес-описания процессов описывается топ-менеджерами следующим образом: «Очень сложно понять, кто, за что в компании отвечает, на что мотивирован, в случае кризисов внутри компании совершенно нельзя понять, кто виноват и что надо сделать, чтобы впредь этого не повторялось. Нам надо поднять управляемость и прозрачность бизнеса». Третья группа проблем использования уже созданных (описанных) бизнес-процессов описывается так: «Мы решили существенно улучшить нашу информационную систему (внедрить новую), именно это должно дать существенный импульс развитию нашего бизнеса».

По мере внедрения бизнес-процесса в организацию, она сталкивается с другими не менее значимыми вопросами, а именно какую конкретно бизнес-задачу ставить перед конкретным исполнителем. Суть сложности заключена в самой постановке задачи для которой есть несколько «слабых» информационных моментов, которые могут привести к неприятным последствиям.

Прежде всего, описание бизнес-процессов рассматривается в большинстве случаев самой организацией как простое для понимания подчиненных описание бизнес-процессов в виде программы оперативно-

хозяйственных действий, или комплексного подхода в управлении организацией.

Тут же на передний план управления выходит проблема в приведенных выше постановках оперативно-технических и производственных задач является отсутствие в них бизнес-задачи. Зачем что-то менять, если компания работает, приносит некоторую прибыль, которая всех устраивает. Топ-менеджмент считает, что да, есть некоторые сложности в коммуникациях, решении проблем, но они являются просто рабочими моментами. Описание же бизнес-процессов потребует инвестиций (и, зачастую, гораздо больших, чем кажется в начале) в программное обеспечение, обучение специалистов, проведение работ, отвлечение сотрудников компании. Если при этом компания не ставит перед собой цели увеличения бизнес-показателей — то этот проект только снизит эффективность компании (только увеличатся издержки).

И параллельно с вышеназванными местами управления организацией на сегодня проблемой является бескомпромиссность применения программ MRP, ERP, CRM, SCM, BPM, DFM и т. д., которые (со слов ее создателей-продавцов) являются неиссякаемым источником эффективных результатов от их внедрения. И вера топ-менеджеров в то, что бизнес нашей организации сам изменится в «правильную» сторону. Увеличатся доходы, будут выбраны правильные сегменты рынка, сократятся издержки и конфликты между сотрудниками. Но, как говорят сами продавцы «волшебных» программ, для того, чтобы ее внедрить, надо правильно описать процессы.

В теории бизнес-процессов переход на новые (оптимизированные) процессы скорее всего, приведет к тому, что в компании нужно будет что-то изменить в рамках уже действующего оперативно-производственного механизма выполнения хозяйственного процесса. Изменения коснутся либо самого сложившегося уклада производственно-хозяйственной деятельности сотрудников, их взаимоотношений, порядка общения, либо выбора ассортимента продукты/услуги, либо действующей ниши рынки, либо

изменения политики клиентов компании, а скорее всего в некоей пропорции все из описанного.

Для топ-менеджмента и всех прочих управленцев это становится неприятной новостью. Описанные бизнес-процессы сами по себе не работают. А сам заказчик, сотрудники компании, и, тем более, менеджеры компании не готовы и не стремятся к тому, что-то еще надо сделать. Из практики внедрения бизнес-процессов известно, ведь плохо или хорошо, но компания работает, что-то зарабатывает, а что будет, если все поменять - никто уверенно не знает.

А это усугубляет то, что первоначальная задача «просто описание бизнес-процессов» точно не включает в себя разработку программы по переходу на новые процессы, программы управления бизнес-процессами в дальнейшем. Бытует упрощенное мнение: «примем одним приказом по компании новые регламенты с первого числа, и все заработает».

Важность эффективного управления человеческими ресурсами находит отражение в международных стандартах и современных подходах к вопросам менеджмента организации – так, например [2, 3]:

В соответствии с понятиями Системы Менеджмента Качества (СМК) деятельность, использующая ресурсы и управляемая в целях преобразования входов в выходы, может рассматриваться как процесс. При этом основными группами процессов СМК являются следующие:

– жизненного цикла продукции,

– правления ресурсами (включая человеческие),

– правления (ответственности руководства),

– измерения, анализа и улучшения.

Непосредственно методология функционального моделирования (IDEF0) выделяет в качестве основных элементов модели бизнес-процесса [13]:

– вход,

– выход,

– управление,

–механизм (ресурсы, включая человеческие).

Общая модель Сбалансированной Системы Показателей (ССП) включает следующие стратегические аспекты (перспективы):

– финансы,

– клиенты,

– процессы,

– персонал (обучение и развитие).

С целью учета отраслевой специфики и особенностей деятельности предприятия разрабатывают и внедряют внутренние стандарты — Стандарты предприятия (СТП) [6].

Система стандартов предприятия представляет собой документированную совокупность норм и требований, разрабатываемых и утверждаемых предприятием самостоятельно, исходя из необходимости их применения в целях совершенствования организации и управления производством.

Стандарты предприятий могут разрабатываться в следующих случаях:
Для обеспечения применения на предприятии государственных стандартов, стандартов отраслей, международных, региональных и национальных стандартов других стран, стандартов научно-технических, инженерных обществ и других общественных объединений;

На создаваемые и применяемые на данном предприятии продукцию, процессы и услуги, в том числе:

– составные части продукции, технологическую оснастку и инструмент,

– технологические процессы, а также общие технологические нормы и требования к ним, с учетом обеспечения безопасности для окружающей среды, жизни и здоровья,

– услуги, оказываемые внутри предприятия,

– процессы организации и управления производством.

Деятельность предприятия, представляющего собой совокупность процессов, оценивается показателями результативности и эффективности (процессов, продуктов и удовлетворенности потребителей).

Для эффективного управления процессами предприятия необходимо:

– идентифицировать процессы,

– определить назначение организации (потребителей и их требований),

– определить политику и цели предприятия,

– определить процессы предприятия,

–определить последовательность и взаимодействие процессов,

–определить Владельца (хозяина) процесса (ответственность и полномочия),

– определить документацию процесса (регламенты, процедуры, спецификации).

Запланировать процесс:

– определить виды деятельности в рамках процесса (процедуры и требования к входам и выходам),

– определить требования к мониторингу и измерению (периодичность регистрации показателей процесса),

– определить необходимые ресурсы (требования к ресурсам),

– проверить процесс на соответствие запланированным целям (верификация требований).

Таким образом, владельцу (Руководителю подразделения) необходимо обладать системой информации по содержанию и окружению (взаимодействию) процесса. Подготовка и поддержание в актуальном состоянии описания бизнес-процессов достигается применением современных программных систем, выбор которых основан на оценке следующих характеристик:

– удобство и наглядность интерфейса (наличие набора типовых нотаций описания бизнес-процессов и поддержка их обновления),

– интеграция с Базами Данных и другими прикладными системами автоматизации видов деятельности предприятия,

– возможность формирования стандартных (принятые в деловой практике) отчетных документов и настройки отчетов с учетом специфики решения текущих управленческих задач,

– стоимость приобретения и сопровождения.

Основными документами кадрового менеджмента (управления человеческими ресурсами) являются:

– «Положение о подразделении» — это документ, который определяет: порядок создания подразделения; правовое положение подразделения в структуре предприятия; организационную структура подразделения; задачи, функции, права и ответственность подразделения; порядок взаимодействия вновь созданного подразделения с иными структурами предприятия,

– «Должностная инструкция» — это документ, разъясняющий порядок взаимоотношений работника и работодателя. Содержит полный перечень квалификационных требований, права, обязанности работника, а также определяет меру его ответственности за те или иные действия (совершенные или несовершенные). При этом, «Положение о подразделении» в основном предназначено для Руководителя подразделения, а «Должностная инструкция» — для его сотрудников.

Типовое содержание «Положения о подразделении» включает следующие разделы:

– общие положения,

– основные задачи,

– функции,

– права и обязанности,

– ответственность,

– взаимоотношения.

Повышение надежности процессов управления персоналом (ключевым ресурсом процессов предприятия) обуславливает необходимость

информационного обеспечения деятельности Руководителя подразделения (особенно в период замещения по болезни, отпуска или увольнения).

С этой целью предлагается модифицировать содержание документа «Положение о подразделении» следующим образом:

– добавляется раздел «Карта целевых показателей» деятельности подразделения – это позволит связать цели подразделения и стратегию развития предприятия, а также определить показатели мотивации сотрудников подразделения,

– добавляется раздел «Циклограмма событий» процессов подразделения – это позволит своевременно планировать и контролировать наличие необходимых ресурсов для выполнения операций с целью исключения риска срыва или снижения качества выполнения функций подразделения,

– раздел «Функции» дополняется пооперационной структурой бизнес-процесса (-ов) подразделения — это позволит осуществить сравнительный анализ трудоемкости и распределение ответственности в интересах развития и мотивации сотрудников подразделения, а также определить целевые нормы трудозатрат на выполнение типовых операций для поддержания квалификационной производительности труда,

– добавляется раздел «Внешние участники» процессов подразделения – это позволит своевременно обеспечить необходимые коммуникации с внутренними и внешними «поставщиками и клиентами» процессов подразделения для поддержания «обратной связи с внешней средой» и обеспечения благоприятных условий реализации процессов.

Далее нами на примере системы «Business Studio» далее описан алгоритм настройки соответствующего Отчета – Реализация проекта на рисунке 1.

На сегодня определяющим в вопросе выбора методологии и программного обеспечения для описания и оптимизации бизнес-процессов являются правильно определенные цели, которые определил для себя бизнес.

Есть две диаметральных формулировки задачи, которые определяют то, какая методология описания процессов наиболее приемлема.

Постановка задачи звучит как-то так: «для решения поставленных задач необходимо одним из этапов создать функциональную (процессную) модель компании, отображающую структуру, взаимосвязи и функции системы, а также потоки информации и материальных объектов, связывающих эти функции». В этом случае делается упор на создание описания системы, выделение и описание объектов управления, на отслеживание иерархий управления, на обязательность отслеживания связей между процессами.

По-другому возможна несколько иная постановка задачи, которая может звучать как-то так: «необходимы описания алгоритмов (сценариев) выполнения процессов. Прежде всего, нужно выявить причинно-следственные связи и временную последовательность выполнения действий, упорядоченную комбинацию событий и функций». В этом случае упор делается на описание последовательностей действий, определение начальных и конечных событий, выявление участников, исполнителей, материальных и документальных потоков.

Отметим, что, эти постановки задач не являются взаимоисключающими, возможны ситуации, когда есть необходимость решить и ту, и другую задачи, но в этом случае, стоит идти от общего к частному: сначала моделировать бизнес компании, а затем использовать эту модель для дальнейшего описания отдельных алгоритмов.

Существующие подходы по описанию бизнес-процессов, как и существующее программное обеспечение, за редким исключением, специализированы и плохо подходят для решения тех задач, для которых они не были предназначены изначально [14]. Например, организация (компания) решила повысить свою эффективность, и для этого собирается создать взаимосвязанную непротиворечивую модель бизнеса всей компании, описав систему бизнес-процессов, каждый из которых связан друг с другом результатами работы, каждый участник процесса имеет показатели KPI,

каждое подразделение компании имеет планы и бюджеты, нацеленные на достижение единых стратегических целей.

В этом случае решение использовать методологии и программное обеспечение, разработанные, прежде всего, для описания алгоритмов и взаимосвязей операционного уровня будет для компании чрезвычайно сложно, дорого и долго. И поэтому, отдав решение этого вопроса на откуп узким (техническим) специалистам, компания рискует получить в итоге ситуацию не очень приятную: потрачены значительные финансовые ресурсы, время, усилия, а полученный формальный результат не дает ожидаемого эффекта.

Поверхностный анализ производителей ПО по бизнес-процессам и Интернета показывает, что данная тема (выбор методологии и инструментария) недостаточно освещена (анализ META Group мало того, что больше ориентирован на IT-решения, так еще и практически не учитывает особенностей Российского рынка, рассматривает только типичных представителей сложившегося западного рынка). Наиболее часто встречаются методики сравнения методологий ARIS и IDEF. Другой наиболее распространенной темой является перечисление сильных и слабых сторон (обычно методологий) без учета того, применительно к какой задаче эти качества анализируются. Приведем ниже таблицу с описанием и общей характеристикой продуктов (ПО) в свете описанных выше задач.

Таблица 1 – Действующее ПО в области описания бизнес-процессов

№ пп	Наименование ПО	Возможности/недостатки
1	CA ERwin Data Modeler (ранее называвшийся AllFusion Data Modeler, BPwin).	В данном ПО наиболее удачно реализована возможность описания взаимосвязанных сложных моделей, задачи описания алгоритмов и последовательности действий реализованы заметно слабее. Простые (лаконичные) нотации

		описания. Сложно, либо вообще никак не реализуются дополнительные задачи (увязка целей и процессов, создание дерева показателей, проведение имитационного моделирования).
2	ARIS (набор программных обеспечений, модулей компании IDS Scheer)	Само название (Architecture of Integrated Information Systems) говорит о том, что данное ПО изначально было ориентировано на решение задачи описания алгоритмов и последовательности производственно-хозяйственных действий. Для описания бизнес-процессов придётся использовать большое количество моделей (в ARIS их более 80, и количество их растет) достаточно сложной семантики. Без большого опыта и существенного переосмысления основ методологии реализовать сложные описания взаимосвязанных моделей непросто
3	Corporate Modeler (Casewise Systems)	Являестя аналогом ARIS — не по методологии и решениям, но по самим идеям1 ПО. Также ориентировано на помощь в описании бизнес-процессов для последующей разработки программного обеспечения. Но стоит оно в среднем дешевле.
4	iGrafx Enterprise Central (подразделение Corel Inc)	Менее известное в России, но очень интересное решение из Канады. Включает в себя целый набор модулей по описанию, моделированию процессов, приложения по планированию и управлению качеством управлением рисками. Существенным ее минусом является ее нераспространённость.

5	Business Studio (ГК «Современные технологии управления»)	Российское ПО. Наиболее известная российская разработка из семейства рассматриваемого ПО. Пожалуй (на наш частный взгляд), удачно совмещает (насколько это возможно) некоторые наиболее полезные возможности BPwin и ARIS, чем-то напоминая по своему решению iGrafx (но не по стоимости). Если для заказчика важно соотношение цена/возможности, наверное, это оптимальный выбор для российских предприятий. Имеет один недостаток, так как очень плотно интегрирована с MS Office (Word, Excel, Visio), а поэтому все шероховатости этих решений автоматически переносятся и на Business Studio.

Ниже представим детальное описание бизнес-задач по субъектам бизнес-процесса на примере условной организации.

Бизнес-задача - А4.2 Реализация проекта (описанный в ПО - Business Studio (ГК «Современные технологии управления»)

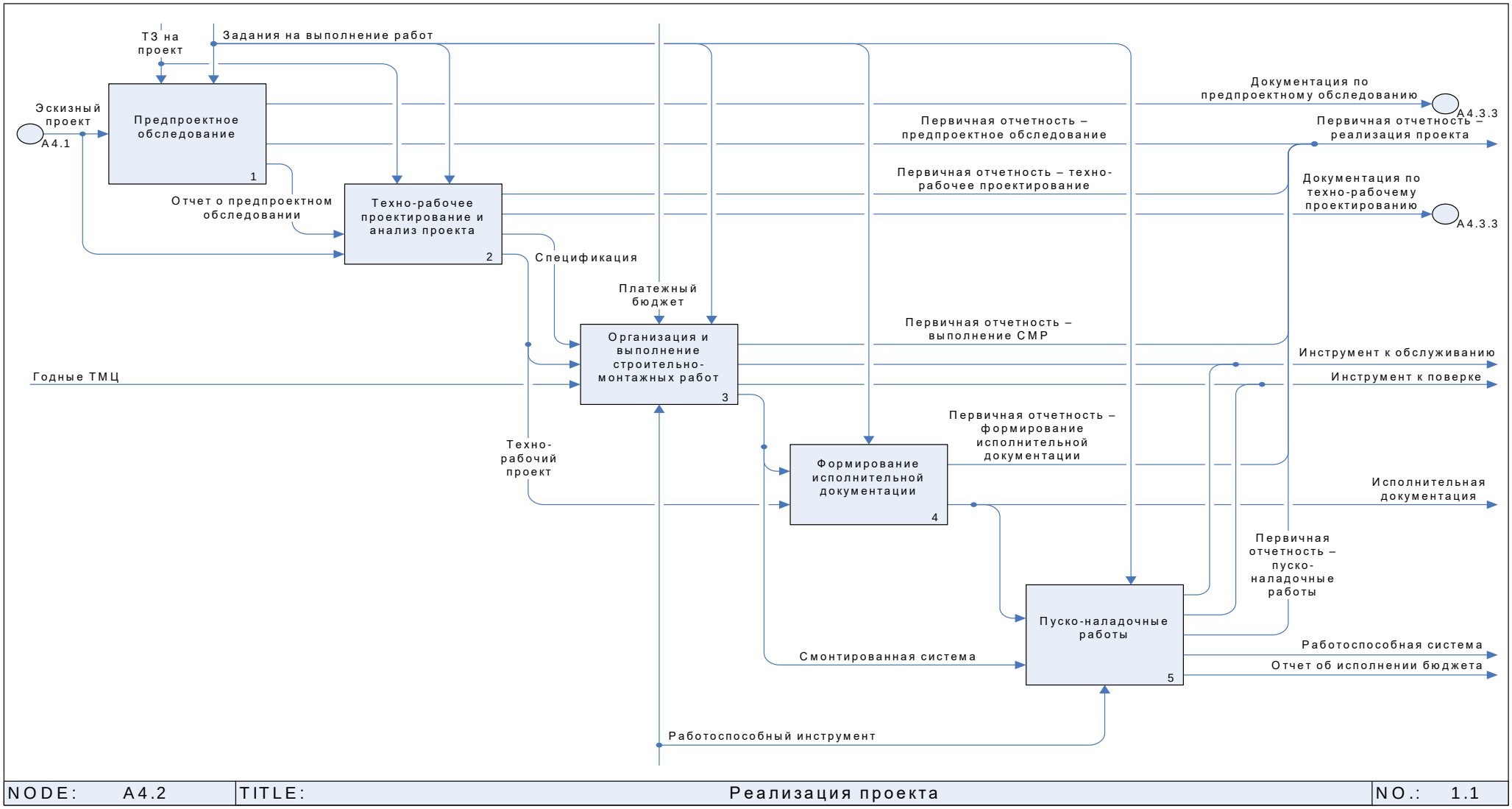

Рисунок 1 – Бизнес-процесс для задачи «Реализация проекта»

Содержанием деятельности по процессу «А4.2 Реализация проекта» является реализация проекта в соответствии с разработанным техническим заданием и планом проекта в заданные сроки.

Владелец процесса:

- Заместитель директора по производству организации.

Исполнители процесса:

- ведущий инженер – в отношении предмета деятельности «Проектная документация»,
- мастер – в отношении предмета деятельности «Монтажные работы»,
- монтажник (Монтажный участок) – в отношении предмета деятельности «Монтажные работы»,
- начальник монтажного участка (Монтажный участок) – в отношении предмета деятельности «Монтажные работы»,
- руководитель проекта – в отношении предмета деятельности «Управление проектом».

Результат выполнения: работоспособная система, смонтированная и запущенная в эксплуатацию в соответствии с техническим заданием на проект в заданные сроки.

Нормативно-методическая и плановая документация:

- задания на выполнение работ,
- план проекта,
- платежный бюджет,
- ТЗ на проект.

Таблица 2 – Входы бизнес-процесса

№	Вход	Объекты	Поступает от	
			Исполнитель	Процесс/Внешняя среда
1.	Годные ТМЦ	ТМЦ	Кладовщик	А6.5 Хранение и выдача ТМЦ
2.	Эскизный проект	Эскизный проект	Инженер-проектировщик	А4.1.3 Эскизное проектирование

Таблица 3 – Выходы бизнес-процесса

№	Выход	Объекты	Передается	
			Получатель	Процесс/Внешняя среда
1.	Документация по предпроектному обследованию	Акт выполненных работ Отчет о предпроектном обследовании	Руководитель проекта	А4.3.3 Закрытие проекта
2.	Документация по техно-рабочему проектированию	Акт выполненных работ Техно-рабочий проект	Руководитель проекта	А4.3.3 Закрытие проекта
3.	Инструмент к обслуживанию	Инструмент	Инженерно-технический отдел	А5.2 Выполнение ремонтно-восстановительных работ
4.	Инструмент к поверке	Инструмент	Инженерно-технический отдел	А5.3 Поверка и калибровка инструмента
5.	Информация о ходе работ по проекту		Инженер-проектировщик	А4.1.3 Эскизное проектирование
			Руководитель проекта	А4.1.4 Формирование и корректировка плана проекта
6.	Исполнительная документация	Исполнительная документация	Ведущий инженер	А4.3.1 Ввод системы в эксплуатацию
7.	Отчет об исполнении бюджета	Отчет об исполнении бюджета	Руководитель проекта	А4.3.3 Закрытие проекта
			Директор	
8.	Первичная отчетность – реализация проекта	Акт выполненных работ и счет-фактура Акт выполненных работ по пуско-наладке Акт приемки площадки Акт сдачи площадки Исполнительная документация Отчет о выполненных СМР Отчет о предпроектном обследовании Отчет о пуско-наладочных работах Техно-рабочий проект	Бухгалтерия	А7.6 Подготовка отчетности
9.	Работоспособная система	Система	Бухгалтер	А4.3.1 Ввод системы в эксплуатацию
			Лица, выполняющие приемо-сдаточные работы	

Таблица 4 – Управление бизнес-процессом

№	Вход	Объекты	Поступает от	
			Исполнитель	Процесс/Внешняя среда
1.	Задания на выполнение работ	Задания на выполнение работ	Руководитель проекта	А4.1.6 Формирование и выдача заданий на выполнение работ
2.	План проекта	План проекта	Руководитель проекта	А4.1.4 Формирование и корректировка плана проекта
3.	Платежный бюджет	Платежный бюджет	Бухгалтерия	А7.4 Формирование платежного бюджета
4.	ТЗ на проект	ТЗ на проект	Ведущий инженер Руководитель проекта	А4.1.2 Разработка ТЗ

Таблица 5 – Механизмы процесса

№	Вход	Объекты	Поступает от	
			Исполнитель	Процесс/Внешняя среда
1.	Работоспособный инструмент	Инструмент	Инженерно-технический отдел	А5.4 Хранение и выдача инструмента

Таблица 6 – Описание под процессов

№	Процесс	Владелец	Исполнители	Входы			Выходы	
				Тип	Название	Объекты	Название	Объекты
1.	А4.2.1 Предпроектное обследование	Руководитель проекта	Ведущий инженер	Вход	Эскизный проект	Эскизный проект	Документация по предпроектному обследованию	Акт выполненных работ Отчет о предпроектном обследовании
				Управление	Задания на выполнение работ	Задания на выполнение работ	Отчет о предпроектном обследовании	Отчет о предпроектном обследовании
					ТЗ на проект	ТЗ на проект	Первичная отчетность – предпрое	Акт выполненных работ и

№	Процесс	Владелец	Исполнители	Входы			Выходы	
				Тип	Название	Объекты	Название	Объекты
							ктное обследование	счет-фактура Отчет о предпроектном обследовании
2.	А4.2.2 Техно-рабочее проектирование и анализ проекта	Заместитель директора по производству	Ведущий инженер Руководитель проекта	Вход	Отчет о предпроектном обследовании	Отчет о предпроектном обследовании	Документация по техно-рабочему проектированию	Акт выполненных работ Техно-рабочий проект
					Эскизный проект	Эскизный проект	Первичная отчетность – техно-рабочее проектирование	Акт выполненных работ и счет-фактура Техно-рабочий проект
				Управление	Задания на выполнение работ	Задания на выполнение работ	Спецификация	Спецификация
					ТЗ на проект	ТЗ на проект	Техно-рабочий проект	Техно-рабочий проект
3.	А4.2.3 Организация и выполнение строительно-монтажных работ	Руководитель проекта	Команда проекта	Вход	Годные ТМЦ	ТМЦ	Инструмент к обслуживанию	Инструмент
					Спецификация	Спецификация	Инструмент к поверке	Инструмент
					Техно-рабочий проект	Техно-рабочий проект	Обязательства перед субподрядчиком	Договор
				Управление	Задания на выполнение работ	Задания на выполнение работ	Первичная отчетность – выполнение СМР	Акт выполненных работ и счет-фактура Акт приемки площадки Акт сдачи

№	Процесс	Владелец	Исполнители	Входы			Выходы	
				Тип	Название	Объекты	Название	Объекты
								площадки Отчет о выполненных СМР
					Платежный бюджет	Платежный бюджет	Смонтированная система	Система
				Механизм	Работоспособный инструмент	Инструмент		
4.	А4.2.4 Формирование исполнительной документации	Руководитель проекта	Ведущий инженер	Вход	Смонтированная система	Система	Исполнительная документация	Исполнительная документация
					Техно-рабочий проект	Техно-рабочий проект	Исполнительная документация в папку проекта	Акт выполненных работ Исполнительная документация
				Управление	Задания на выполнение работ	Задания на выполнение работ	Первичная отчетность – формирование исполнительной документации	Акт выполненных работ и счет-фактура Исполнительная документация
5.	А4.2.5 Пуско-наладочные работы	Руководитель проекта	Мастер	Вход	Исполнительная документация	Исполнительная документация	Документация по пуско-наладочным работам	Акт выполненных работ по пуско-наладке Отчет о пуско-наладочных работах
					Смонтированная система	Система	Инструмент к обслуживанию	Инструмент
				Управление	Задания на выполнение работ	Задания на выполнение работ	Инструмент к поверке	Инструмент

№	Процесс	Владелец	Исполнители	Входы			Выходы	
				Тип	Название	Объекты	Название	Объекты
				Механизм	Работоспособный инструмент	Инструмент	Отчет об исполнении бюджета	Отчет об исполнении бюджета
							Первичная отчетность – пуско-наладочные работы	Акт выполненных работ по пуско-наладке Отчет о пуско-наладочных работах
							Работоспособная система	Система

1.3 Факторы влияющие на разработку стратегии кибербезопасности в организации

Согласно результатам опроса, недавно опубликованным Barracuda Networks (USA) в сентябре 2018 года, организации, внедряющие программные решения для глобальных сетей (SD-WAN), сообщается, что повышение сетевой безопасности является основным достижением стратегии кибербезопасности для таких систем противостояния кибеугрозам коей является SD-WAN.

Кибербезопасность в организациях США была главной темой всего доклада, под названием «Проблемы и возможности SD-WAN» за 2017 год и на основе опроса, проведенного от имени Barracuda, Вансон Борн, который опросил более 900 мировых ИТ-лидеров и сетевых специалистов и специалистов по безопасности было выявлено следующее.

Barracuda описывает себя как «поставщик облачных решений для обеспечения безопасности и защиты данных». В ходе опроса 92% опрошенных согласились (полностью или частично) с утверждением: «безопасность должна быть приоритетом номер один при рассмотрении решения SD-WAN».

На современном этапе размещение внешнего и внутреннего Exchange серверов в физически или логически разделенных зонах безопасности это лучший отображён на рисунке 2.

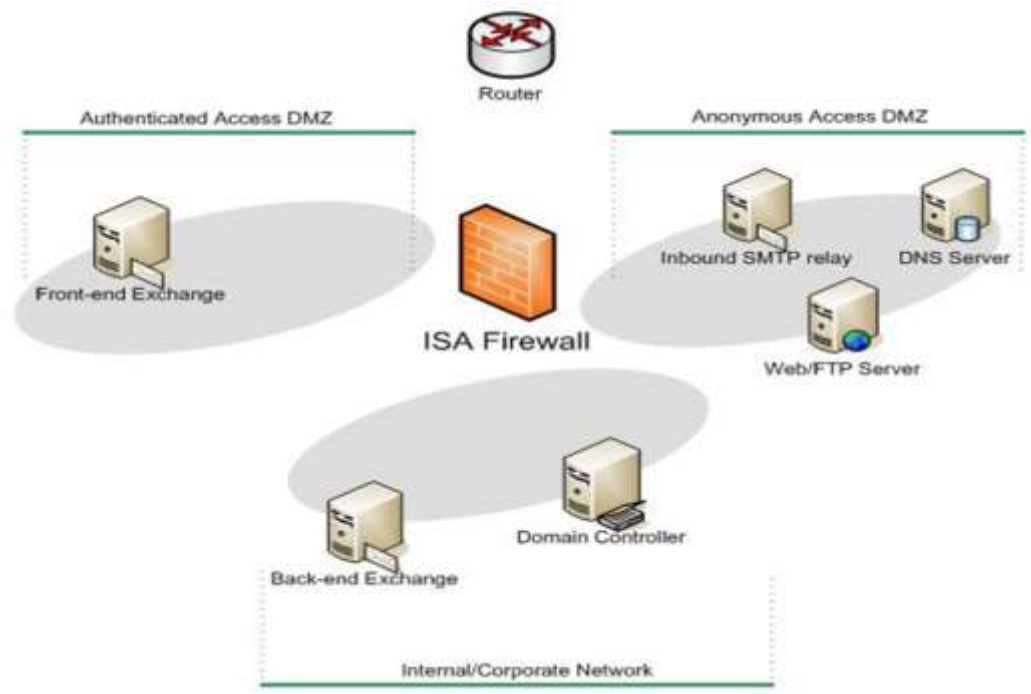

Рисунок 2 – Построение DMZ периметра сети для защиты

На современном этапе развития теории информационной безопасности часто используют категорию DMZ, что означает демилитаризованную зону периметра сети организации. Ее техническое решение о построении зон и периметра сегодня позволяет организациям построить достаточно недорогую, но все же затратную схему защиты организации.

На следующем рисунке 3 отразим локализацию угроз в рамках демилитаризованных зон (далее DMZ) периметра сети организации.

Остальные вопросы построения DMZ в том, как можно создать лучшую схему параметризации не только для внешнего и внутреннего Exchange серверов, но и для всех ресурсов, так или иначе соприкасающихся с Интернетом.

Ключевой момент организации построения информационной безопасности для в том, что не все сети .NET одинаково «не доверенные». Некоторые не доверенные сети считаются более надежными, чем другие.

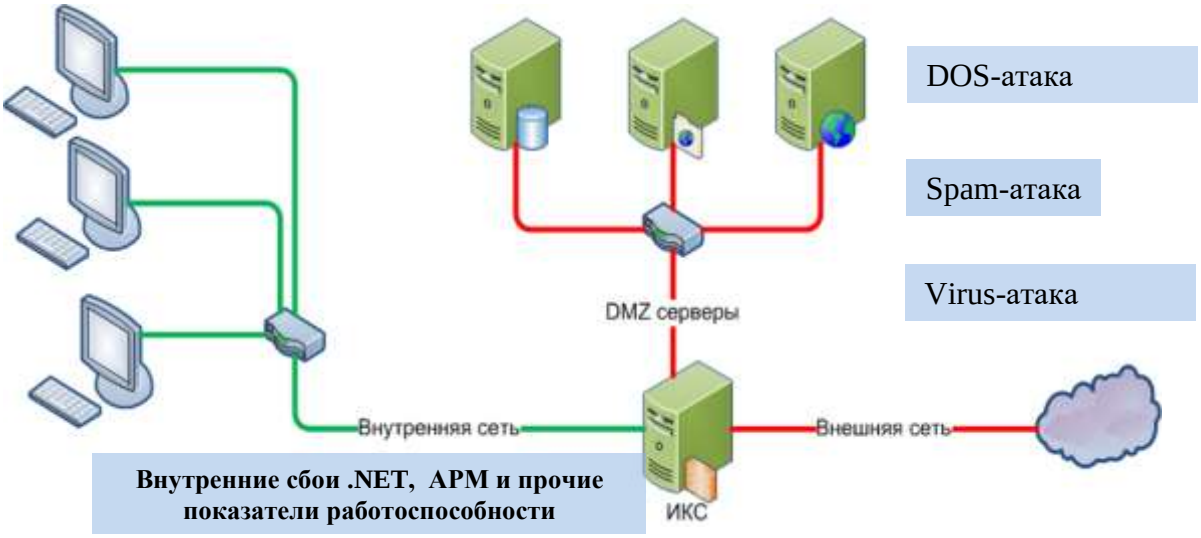

Рисунок 3 – Атака DMZ периметра сети на малой организации

В свою очередь, список разных зон безопасности по убыванию степени надежности, следующий:

– сегмент сетевых служб,

– сегмент разработчиков,

– сегмент для всех пользователей,

– DMZ с авторизованным доступом,

– сегмент анонимных клиентов беспроводной ЛВС,

– DMZ с неавторизованным доступом.

На рисунке 4 и 5 представим варианты возможной атаки DMZ средней и крупной по размеру организации.

С учетом целеполагания экономической составляющей нашей задачи мы получим следующее вербальное математическое формулирование целей поиска рациональности защиты организации на рисунке 4.

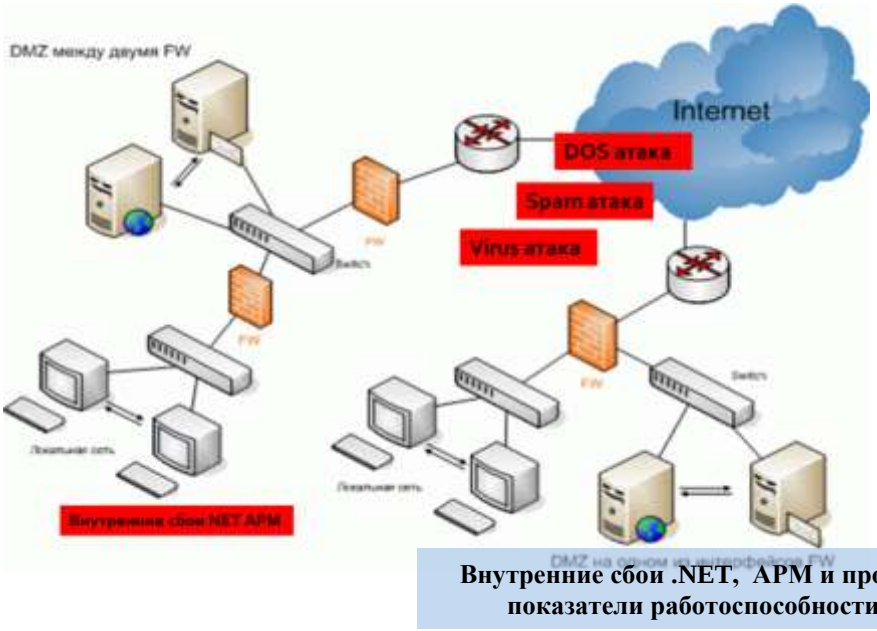

Рисунок 4 – Вариант атаки DMZ периметра сети на средней по размерам организации

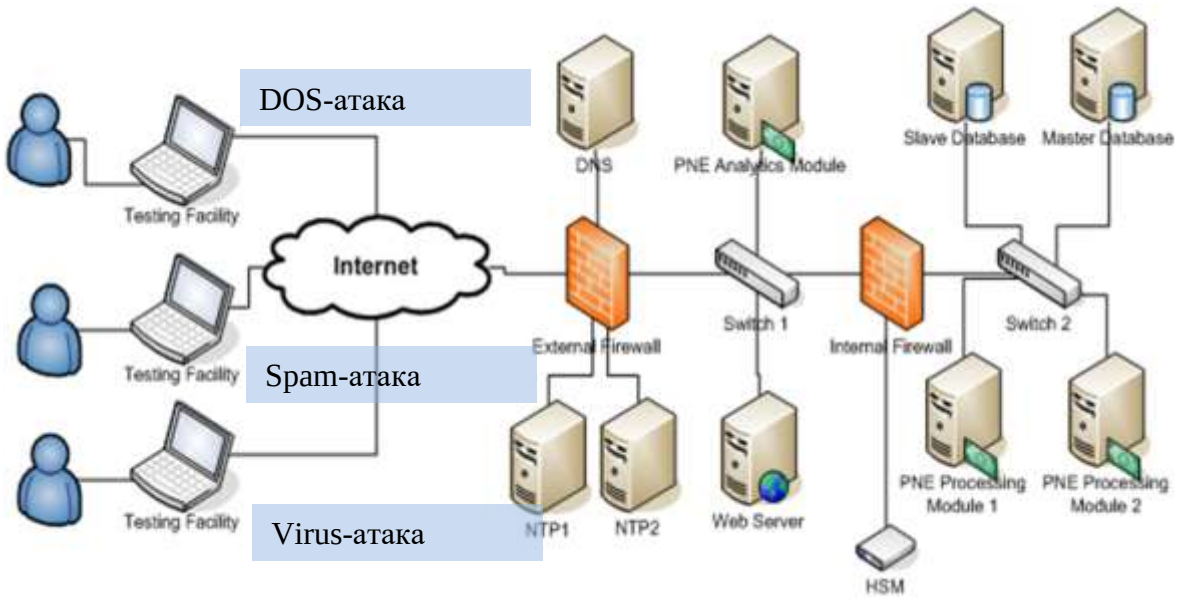

Рисунок 5 – Вариант атаки DMZ периметра сети на крупной организации

Однако в рамках теории защиты информации оговоримся, что автором поддерживается критерий максимум бюджетозащищенности организации, на текущий момент наиболее адекватно отражающем цель задачи выработки стратегии кибербезопасности организации по целевой функции.

1.4 Выводы по разделу

В данном разделе рассмотрены:

– основы кибербезопасности и современные проблемы теории,

– цель обеспечения кибербезопасности,

– методологические основы кибербезопасности,

– типы современных угроз кибербезопасности,

– компоненты, подлежащие защите кибербезопасности.

Так же проведено описание бизнес-процесса организации для целей создания моделей информационных угроз. Представлена динамика угроз информационной безопасности в 2018 году на примере нескольких организаций, которая включила в себя всевозможное оборудование, которое контактирует с сетью. Более подробно рассмотрены факторы влияющие на разработку стратегии кибербезопасности в организации. Приведены наглядные примеры факторов, влияющих на разработку стратегии кибербезопасности для организаций.

2 Теоретические основы стратегического моделирования кибербезопасности организации

2.1 Разработка модели угроз для бизнес-процесса организации

Согласно действующим на текущий момент времени в РФ стандартам информационной безопасности принятыми ФСТЭК РФ, такими как:

– ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационные технологии - Методы безопасности - Критерии оценки ИТ-безопасности - Часть 1: Введение и общая модель (IDT)» [2],

– ГОСТ Р ИСО/МЭК 27007 – 2014 идентичный международному стандарту ИСО/МЭК 27007:2011 «Информационная технология. Методы обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»,

– ISO/IEC 27002:2013 (E) «Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью».

Нами предлагается модернизированный вариант известной модели угроз по известному приказу ФСТЭК РФ от 11 февраля 2013 г. N 17, в котором защита персональных данных и рассматриваемый нами бизнес-процесс, имеет те-же особенности, что и при составлении модели угроз применительно к бизнес-процессу. К таковым особенностям (в корреляции с международным стандартом ISO/IEC 27002:2013) можно отнести: зона вероятных угроз, вид информационного актива, который будет подвержен угрозе, вид воздействующего фактора угрозы и показатели бизнес-процесса организации, которые будут подвержены угрозе. Согласно данного стандарта (не имеющего российского аналога) организации всех типов и размеров (включая государственный и частный сектор, коммерческие и некоммерческие) накапливают, обрабатывают, сохраняют и передают информацию в различных формах, включая электронную, физическую и устную (например, собеседования и презентации). Ценность информации не только в

документированных словах, числах и изображениях: знания, понятия, идеи и бренды – вот примеры нематериальных форм информации. В мире, где все взаимосвязано, информация и соответствующие процессы, системы, сети и персонал, осуществляющий их эксплуатацию, обработку и защиту – все это активы, которые, подобно другим важным деловым активам, представляют ценность для бизнеса организации и, следовательно, нуждаются или требуют защиты от различных угроз.

Рассмотрим перечисленные угрозы и сведем их в модернизированную модель угроз для бизнес-процесса организации (на примере ООО «Информационные Кронвел» г. Ставрополь) основные из них, с позиции анализа вероятных угроз бизнес-процессу на примере конкретной организации в рамках используемой ею модели бизнес-процесса составленного и описанного в параграфе 1.3 настоящего исследования.

Так в бизнес-процессе каждой организации есть блок-звено известное как «расчетно-кассовое обслуживание» или время простоя получения аванса или итога дохода. С позиции информационных киберугроз на текущий момент 01.11.2019 года, любой target вирус, проникший в системы компании по точкам входа, а именно любое оборудование компании может быть потенциально уязвимым, может вызвать как отказы в обслуживании кассовых систем, так и нелегитимный перевод средств на «лже-счета» злоумышленника. В тоже время известный в бизнес-процессе любой организации этап как согласование дизайн-макета проекта заказчика и любой target вирус, проникший в системы компании по точкам входа, приведет к времени простоя для калькулирования и утверждения старта монтажных работ по данному клиентскому договору, а причиной будет - отказы в обслуживании после локальной target атаки на информационную систему компании, позволяющие подменить легитимный проект на ложный.

Также известный этап «калькулирование» заказа клиента после локальной target атаки на информационную систему компании, повлечет неисполнение договора на заказ, в виде времени простоя на этапах монтажа,

установки оборудования, для калькулирования и утверждения старта монтажных работ. Здесь не менее важна информационная безопасность от атаки на компании-посредники или на поставщиков, через внедрение в информационную систему организации «лже»-договоров в бизнес-процесс организации. Необходимо выделить также возможные вынужденные производственные простои от третьих лиц (электроснабжение, отсутствие комплектующих и прочее) при вводе в эксплуатацию заказа клиента, путем локальных DDoS-атак на IP-телефони. Также вероятно будет отсутствие доступа к базе данных комплектующих, изменение ее содержимого или внезапный отказ обеспечения комплектующими, и как следствие задержка старта монтажа или ввода в эксплуатацию заказа.

Известными угрозами для бизнес-процесса организации являются - срыв поставки комплектующих для исполнения заказа. Надо упомянуть также возможный технический отказ (сбой) установленного после монтажа оборудования заказа клиента (время демонтажа, последующие переделки и ожидание поставки новых комплектующих). К наиболее вероятным угрозам можно отнести заражение всех информационных активов компании и уничтожение данных (включая все существующие проекты, документы, отчетности и прочие этапы, и ключевые факторы бизнес-процесса).

К наименее вероятным информационным угрозам, но вполне осуществимыми в условиях конкурентной борьбы организации за нишу рынка будет полное нарушение информационной целостности ПО или АО оборудования организации, по известному примеру Tailored Access Operations, с возможностью перехвата управления или уничтожения данных. К совсем нереальным, но все-таки учитываемым информационным угрозам надо отнести создание клона заказчика (целевая атака на длительное время с последующим уничтожением компании.

Отразим данные факторы вероятных информационных угроз в модернизированной модели угроз в таблице 7.

Таблица 7 – Модернизированная модель угроз для бизнес-процесса организации (по стандарту ISO/IEC 27001:2013 (E))

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
1	Отдел бухгалтерского учета	Сбой или отсутствие расчетно-кассового обслуживания всей организации, в виде отказов в обслуживании кассовых систем, или также нелегитимный перевод средств на «лже»-счета злоумышленника или дополнительные расходы при покупке, настройки, обслуживании вышедшего из строя оборудования.	База данных учета операций бизнес-процесса 1С: Бухгалтерия	Время простоя получения аванса от заказчика или недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование отдела бухгалтерского учета которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Microsoft Windows Server 2016 Standard 64-bit Russian 1pk DSP OEI DVD 16 Core ~70000 руб.)
2	Отдел дизайна	Сбой в процессе согласования дизайн-макета проекта с заказчиком (время простоя для калькулирования и утверждения старта	База данных учета и хранения эскизов макет-дизайнов для заказчика Adope Photoshop	Время простоя получения аванса от заказчика или недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
		монтажных работ); (отказы в обслуживании, target атаки на системы компании, позволяющие подменить легитимный проект на ложный)			любое оборудование отдела дизайна которое потенциально уязвимо.		
3	Отдел продаж, Офис-менеджер организации	Сбой в процессе исполнения клиентского договора, в виде времени простоя на этапах монтажа, установки оборудования, для калькулирования и утверждения старта монтажных работ; а также параллельные атаки на компании-посредники или на поставщиков, подмена договоров на лже-договоры.	База данных контрактов с клиентами и посредниками "Электронный документооборот"	Время простоя получения итогового дохода (выручки) от заказчика или недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование отдела монтажа которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
4	Отдел бухгалтерского учета, Склад организации	Сбой в процессе доступа или отсутствие такого доступа к базе данных комплектующих, изменение ее содержимого или внезапный отказ обеспечения комплектующими (задержка старта монтажа или ввода в эксплуатацию.	База данных учета операций бизнес-процесса 1С: Склад	Время простоя общего времени монтажа и исполнения клиентского договора влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
5	Отдел смет и мат-технического сопровождения	Сбой или отсутствие доступа к базе данных смет и комплектующих, изменение их содержимого или внезапный отказ обеспечения комплектующими (задержка старта монтажа или ввода в эксплуатацию);	База данных учета операций бизнес-процесса 1С: Сметы	Время простоя до подписания и начала старта исполнения клиентского договора влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
					потенциально уязвимо.		
6	Отдел бухгалтерского учета, Склад организации	Сбой или полный срыв поставки комплектующих для исполнения заказа по уже заключенным договорам с клиентами	База данных учета операций бизнес-процесса 1С: Склад	Время простоя при исполнении клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
7	Производственный отдел (монтаж, инженерия)	Сбой или технический отказ уже установленного по договору с клиентом смонтированного оборудования (время демонтажа, последующие переделки и ожидание поставки	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время простоя общего времени по окончании монтажа по клиентскому договору влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад	Затраты отдела монтажа организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
		новых комплектующих);			которое потенциально уязвимо.		
8	Все отделы организации	Сбой бизнес-процесса или вынужденные производственные простои от третьих лиц (э/снабжение, отсутствие комплектующих и прочее) при вводе в эксплуатацию системы инф безопасности; (DDoS-атаки на IP-телефонию, противодействие - контроль доступа и политика аудита)	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время простоя при исполнении клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любая DDoS-атака на систему Network организации - любое оборудование всей организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
9	Все отделы организации	Уничтожение информационного актива путем заражения всех информационных активов компании и уничтожение	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Потеря информационного актива организации	Любая DDoS-атака или вирус -атака на периметр сети - Network организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности.

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
		данных (включая все существующие проекты, документы, отчетности и прочие факторы бизнес-процесса.					Создание модели угроз.
10	Все отделы организации	Сбой, отказ в доступе или полное нарушение информационной целостности ПО или АО оборудования (как пример Tailored Access Operations) с возможностью перехвата управления или уничтожения данных	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время простоя при исполнении клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любая DDoS-атака на систему Network организации - любое оборудование всей организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
11	Все отделы организации	Потеря времени - "холостой" бизнес-процесс от создания злоумышленниками клона заказчика-клиента (целевая атака на длительное время с последующим уничтожением компании)	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время "холостого" обслуживания при исполнении "лже"-клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любая DDoS-атака на систему Network организации - оборудование всей организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

Активы организации подвержены как преднамеренным, так и случайным угрозам, при этом связанные с ними процессы, системы, сети и люди имеют присущие им уязвимости. Изменения бизнес-процессов и систем или другие внешние изменения (такие как новые законы и регламенты) могут создать новые риски для информационной безопасности. Поэтому, учитывая множество способов, которыми угрозы, используя уязвимости, могут нанести вред организации, можно утверждать, что риски информационной безопасности всегда присутствуют. Результативная защита информации уменьшает эти риски, страхуя организацию от угроз и уязвимостей и, тем самым, уменьшая воздействие на ее активы.

Информационная безопасность достигается внедрением соответствующего набора средств, включая политики, процессы, процедуры, организационные структуры, а также программного и аппаратного обеспечения соответствующего назначения. Эти средства должны быть разработаны и внедрены, а результаты их работы должны отслеживаться, анализироваться и улучшаться там, где это необходимо, чтобы гарантировать достижение конкретных целей организации, как относящихся к безопасности, так и бизнесу в целом.

Система менеджмента информационной безопасности (сокращенно СМИБ), как это определено в ISO/IEC 27001 [10], дает целостное, согласованное представление о рисках организации в сфере информационной безопасности в целях осуществления всестороннего комплекса мер по обеспечению информационной безопасности в рамках целостной системы менеджмента.

Многие информационные системы были разработаны без учета требований к безопасности в контексте ISO/IEC 27001 [10] и этого стандарта. Безопасность, обеспечиваемая только техническими средствами, носит ограниченный характер и должна быть дополнена соответствующим менеджментом и процедурами. Определение, какие средства использовать в конкретном случае, требует тщательного планирования и внимания к деталям.

Для успешного функционирования СМИБ требуется ее поддержка всеми сотрудниками организации. Это может также потребовать участия акционеров, поставщиков или других внешних сторон. Также могут потребоваться советы привлекаемых извне специалистов.

В более общем смысле результативная защита информации дает уверенность менеджменту и другим заинтересованным лицам в том, что активам организации обеспечена достаточная безопасность и защита от вреда, что выступает как позитивный бизнес-фактор.

Таким образом, мы можем приступить к разработке адекватной стратегии информационной безопасности в рамках предложенной модели угроз для объекта исследования.

2.2 Методы регистрации инцидентов и их последствия воздействия на информационную безопасность

Для регистрации инцидентов используются специальные форм бланки, которые заполняются оператором ЭВМ в ручную или полуавтоматическом виде.

Таблица 8 – Технические характеристики организации

Общее количество настольных компьютеров	20
Общее количество переносных компьютеров	15
Число физических серверов	3
Общее количество коммуникационных узлов (маршрутизаторы, коммутаторы)	1,2
Использование защищенных каналов передачи данных (VPN)	отсутствует
Использование виртуальных машин	локально
Наличие зон безопасности (серверная, аттестованное помещение для переговоров)	отсутствует
Наличие поста охраны	имеется
Наличие систем инженерной защиты	имеется
В том числе: видеонаблюдение	имеется
В том числе: охранная (пожарная) сигнализация	имеется
В том числе: система контроля управления доступом	имеется
Другие характеристики	–

Технические характеристики организации необходимы для составления и анализа полного перечня оборудования для регистрации и выявления инцидентов в режиме реального времени ответственным лицом или в автоматическом виде.

Для тщательного анализа необходимо знать полный состав ПО в организации, указанный в таблице 9.

Таблица 9 – Используемое программное обеспечение в организации

Тип программного обеспечения	Описание использования
Системное ПО	Windows 10 Pro Windows Server 2008
Программные средства защиты:	
Средства аутентификации	Active Directory
Средства мониторинга и аудита	Журналы ОС, ISA Server 2006
Сканеры защищенности	–
Средства разграничения доступа	Active Directory, ISA Server 2006
Антивирусные программы	Microsoft Antivirus Avast
Антиспамовые программы	AntiSpam Sniper Pro, Microsoft Security Essentials
Межсетевой экран	Межсетевой экран Microsoft ISA Server 2006
Инструментальное ПО:	
Средства разработки программного обеспечения	1С Склад, бухгалтерия
Системы управления базами данных (СУБД)	MS SQL server 2008 express
Офисные приложения	MS Office 2010, 2016, ABBYY FineReader 12, Acrobat Reader DC, 7zip
Корпоративные информационные системы	СБИС, 1С, Консультант Плюс; Юридически значимый документооборот сайтом «Гос-услуги»
Клиенты для доступа к интернет-сервисам	Mozilla Firefox, Google Chrome
Мультимедиа	Media Player Classic
Прочие системы	–

Указать виды важной информации, обрабатываемой организации:

– персональные данные клиентов,

– персональные данные сотрудников,

– коммерческая тайна,

– для служебного пользования.

Указать имеются ли в организации записи, которые не могут быть предоставлены для рассмотрения аудиторской группой, так как содержат конфиденциальную или секретную информацию:

– информация о клиентах,

– информация о сотрудниках,

– информация о финансовых операциях,

– информация об операция в сфере контрактной службы,

– информация о структуре УЦ,

– информация о средствах физической охраны,

– информация о структуре локальной вычислительной сети и о средствах защиты информации.

Описать, (если это имеет место), какое ПО (собственной разработки или приобретенное) используется в процессе управления Вашей организации и оказании услуг:

– система контроля доступа СКУД на стадии разработки собственной разработки,

– программа по контролю работы сотрудников – в процессе приобретения,

– 1С бухгалтерия – приобретенное,

– абонентское оборудование ГЛОНАСС и аренда сервиса для контроля служебного авто транспорта – приобретенное.

Передача информации в сторонние организации через стороннее ПО:

– СБИС отчеты в ПФР, Росстат, ФНС по защищенному каналу связи,

– сайт bus.gov.ru паспорт учреждения, план финансово хозяйственной деятельности, отчеты бухгалтерии и экономического отдела по защищенному каналу связи,

– сайт zakupki.gov.ru осуществление контрактной деятельности по защищенному каналу связи,

– программа для ВКС с филиалами по краю и центральным офисом по защищенной сети.

В последние три-четыре года утечки данных происходили главным образом из-за того, что компании оставляли открытые в Интернете серверы MongoDB или AWS без пароля. Но в последние годы данных инцидентов стало на много меньше.

Таблица 10 – Описание технических средств и мер в организации

Техническая мера	Средства и методы использования
Как и с помощью каких средств осуществляется разграничение прав доступа к информационной системе и установление полномочий?	С помощью штатных средств серверной ОС Microsoft AD
Способы авторизации в программах, содержащих конфиденциальную информацию (по логину и паролю, по учетной записи Windows, токен и т.д.)	по доменному логину и паролю Windows по локальному логину и паролю Windows по учетной записи Windows по логину и паролю СУБД по ip и mac адресам токен
Используемые средства резервного копирования	автоматический бэкап средствами СУБД SQL ручное копирование файлов БД SQL средствами ОС автоматический бэкап (скрипт) файлов 1С
Компоненты виртуальной инфраструктуры, облачные компоненты, и применяемые в них средства защиты информации.	VMware ESX Server., СЗ: штатные средства ОС W8k, антивирусное ПО, облачные компоненты - отсутствуют
Средства защиты от несанкционированного вскрытия корпуса ЭВМ (датчики вскрытия, система контроля, пломбирование корпусов ЭВМ)	отсутствуют
Защита BIOS от несанкционированного изменения настроек (наличие пароля для входа в BIOS, специальное ПО и т.д.).	частично
Развернут ли контроллер домена, действуют ли политики.	да, политики действуют
Применяемые меры защиты от сбоев электроснабжения	ИБП в коммутационных шкафах, частично на ПК, частично для серверов
Применяются ли средства удаленного управления объектами внутренней ЛВС извне (AmiAdmin, Radmin или др) и применяемые средства защиты используемых для этого удаленных соединений (VPN).	ПО TeamViewer 11.0. - VPN не защищено

В то время как некоторые утечки данных будут происходить в последствии хакерской атаки, большое количество также произойдет, потому что на сервере не установлен пароль или он имеет легко подбирающий вид.

Регистрация всех типов параметров очень важно для дальнейшего анализа проникновения угрозы в информационную систему организации, тк её отсутствие ставит в тупик деятельность организации и её финансовый отдел, в таком случае фирмы просто банкротятся.

2.3 Методика обоснования оптимальной политики информационной безопасности (методом оптимального программирования)

Линейное программирование – это направление математического программирования, изучающее методы решения экстремальных задач, которые характеризуются линейной зависимостью между переменными и линейным критерием, что также применимо к задачам поиска оптимальной стратегии информационной безопасности.

Необходимым условием постановки задачи линейного программирования являются ограничения на наличие ресурсов (финансовых) организации реализующей стратегию информационной безопасности, которые могут воздействовать на величину спроса услуг данной организации, его производственную мощность и другие производственные факторы (производительность труда, компетенции кадров, качество производства и пр.).

В случае с информационной безопасностью организации от внешних угроз, возникающих по причине - трех типов угроз: DDoS- атаки, вирус -атаки и прочих видов угроз, к которым можно отнести и спам воздействие мы можем вербально подойти к разработке математической модели информационной безопасности. На рисунке 6 отразим как формируются факторы модели и искомые решения.

Сущность линейного программирования поиска оптимальной стратегии информационной безопасности состоит в нахождении точек (решений) наибольшего или наименьшего значения некоторой функции (защищенность информационных активов организации) при определенном наборе ограничений (финансовые ресурсы на защиту информационных активов от видов и вероятности возможных типов угроз), налагаемых на аргументы и образующих систему ограничений, которая имеет, как правило, бесконечное множество решений.

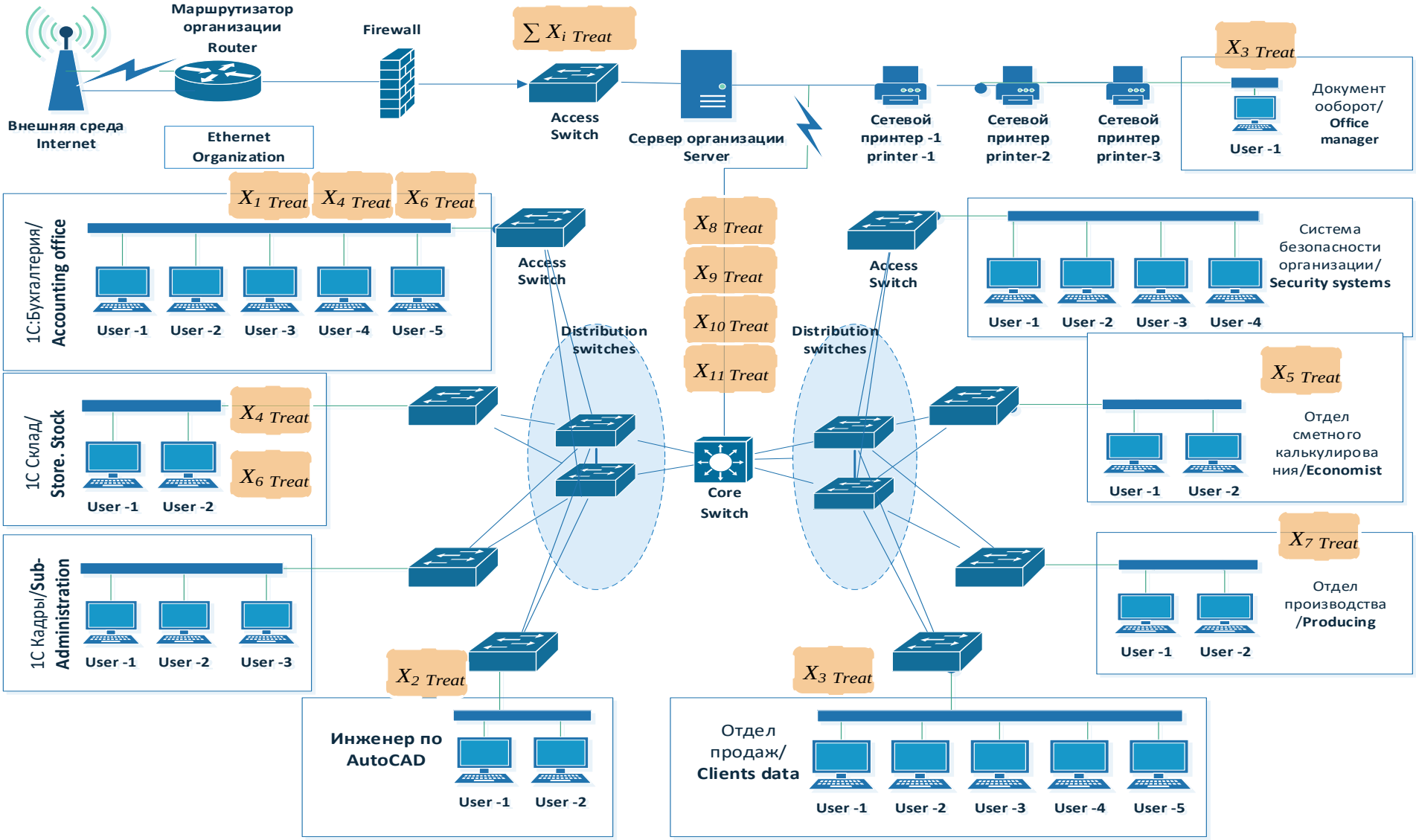

Рисунок 6 – Вербальное наполнение факторами будущей стратегии информационной безопасности организации

На рисунке 6 мы видим основные факторы математической задачи для поиска оптимального варианта стратегии информационной безопасности (далее ИБ), а именно:

– $\sum X_i Treats$ - сумма всех вероятных информационных угроз посредством атак извне организации,

– $\rho_j * X_i Treat$ - тип угрозы и ее вероятность,

– $T_{XiTreat}$ - время простоя организации (ее звеньев бизнес-процесса) от каждого вероятного типа угрозы,

– $\sum T_x = T_{1X_1Treat} + T_{2X_2Treat} \dots T_{nX_nTreat}$ - общее время потерь бизнес-процесса организации от всех типов информационных угроз за календарное время (месяц, квартал, год).

Примерные ранги угроз ИБ для исследуемой организации (по рисунку 6) и по результатам проведенного аудита информационных угроз будет выглядеть следующей иерархией (рангами) угроз. При этом иерархия предусматривает и вероятность возникновения угроз ИБ:

– 0-й уровень (высокая опасность угроз ИБ) $\rho_0 = 0,76 \div 0,99,$

– 1-й уровень (средневысокая опасность угроз ИБ) - $\rho_0 = 0,51 \div 0,75,$

– 2-й уровень (средняя опасность угроз ИБ) - $\rho_0 = 0,26 \div 0,51,$

– 3-й уровень (низкая опасность угроз ИБ) - $\rho_0 = 0,03 \div 0,25.$

Рассмотрим данные уровни по источникам возникновения угроз ИБ.

0-й уровень (высокая опасность угроз ИБ):

– ИБ в компании никто не занимается, руководство компании не осознает важности проблем ИБ,

– финансирование ИБ отсутствует,

– ИБ реализуется штатными сотрудниками не имеющих высшего образования в области ИБ и средствами операционных систем, СУБД и приложений (парольная защита начального уровня знаний, и равное ему разграничение доступа к ресурсам и сервисам организации).

1-й уровень (средневысокая опасность угроз ИБ):

– ИБ рассматривается руководством как чисто «техническая» проблема, отсутствует единая программа (концепция ИБ, политика) развития системы обеспечения ИБ компании, однако в штате организации есть работник с высшим образованием по ИБ,

– финансирование ведётся в рамках общего ИТ – бюджета,

– ИБ реализуется работником среднего качества знаний ИБ, но средствами нулевого уровня плюс средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN (построения виртуальных частных сетей), т.е. традиционные средства защиты.

2-й уровень (средняя опасность угроз ИБ):

–ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для бизнес-процессов, есть утверждённая руководством программа развития системы обеспечения ИБ компании,

– финансирование ведётся в рамках отдельного бюджета ИБ;

– ИБ реализуется работниками высшего и среднего качества знаний ИБ, а также средствами усиленной аутентификации, средствами анализа почтовых сообщений и web-контента, системы обнаружения вторжений (IDS), средствами анализа защищённости, средства однократной аутентификации (SSO), наличием инфраструктуры открытых ключей (PKI) и внедрены необходимые организационные меры (внутренний и внешний аудит, анализ рисков, политика ИБ, положения, процедуры, регламенты и руководства).

3-й уровень (низкая опасность угроз ИБ):

– ИБ является частью корпоративной культуры, назначен старший администратор по вопросам обеспечения информационной безопасности (CISA),

– финансирование ведётся в рамках отдельного бюджета ИБ с тенденцией роста из года в год,

– ИБ реализуется работниками высшего качества знаний ИБ, а также средствами второго уровня ИБ плюс система управления ИБ, группа

реагирования на инциденты нарушения ИБ (CSIRT), и сопровождается соглашением об уровне сервиса (SLA).

По результатам аудита исследуемой организации, у её сервера есть роли: хранилища (SMB/cifs), почтового сервера, веб-сервера (сайт организации), а также условные информационные единицы 1С:Предприятие (куда входят Бухгалтерия, Склад, Кадры, ПО AutoCad, Corel и прочее).

Среди потенциальных проблем угроз ИБ, могут быть с внешнего периметра (интернета), следующие по устройствам сети:

– корневой маршрутизатор организации:

1) DDoS атака (вывод из строя),

2) отравление таблицы маршрутизации (перенаправление рабочего трафика сотрудников на серверы злоумышленника),

– сервер организации:

1) DDoS атаки на серверные службы,

2) DDoS атака на почтовый сервер,

3) спам (замусоривание сервера),

4) ложные клиентские письма (контракты),

– DDoS атака на сайт организации,

– DDoS атака на службы удаленного управления (невозможность ликвидации простоев),

1) получение незаконного доступа к серверу:

2) методом подбора паролей к службам удаленного управления,

3) методом уязвимостей и эксплоитов,

4) фишинг с помощью поддельных писем,

– уничтожение рабочих данных, включая:

1) договоры, счета, выписки и т.д.,

2) файлы проектов AutoCad, Adobe Photoshop,

3) базы данных 1С: Предприятие, 1С: Склад, Документооброт,

– клиентские компьютеры в организации:

1) через почту,

2) фишинговые письма,

3) письма с зараженными вложениями (с эксплоитами),

– через самих пользователей:

1) отсутствие контроля за подключаемыми съемными носителями,

2) отсутствие политики ограниченного запуска программ из доверенных источников или с доверенными цифровыми подписями,

– отсутствие разграничений прав доступа.

Потенциальные проблемы с внутреннего периметра (интернет):

– отсутствие контроля доступа сотрудников к сети и к ее ресурсам,

– доступ сотрудников к файлам проектам других сотрудников организации без явной на это необходимости (нет разграничения прав на основе бизнес-роли).

Сведем результаты проведенного аудита ИБ в таблицу 11, где представлен перечень возможных (наиболее вероятных) угроз организации по звеньям бизнес-процесса. Тогда целевая функция Z – поиска оптимально-безопасной стратегии организации М, должна стремиться к минимуму временных потерь (простоев Т) её бизнес-процесса от воздействия Х возможных (внешних и внутренних) угроз ИБ, и будет иметь вид (1).

$$f\left(Z_m\right) \rightarrow \min \sum T_m \bullet \max \sum X_i Treats \tag{1}$$

При этом максимальной сумме вероятных временных простоев Т бизнес-процесса организации от угроз Х, должна противостоять стратегия ИБ (мероприятия по противодействию угрозам) которая имеет набор переменных в виде (2) и в общем итоге равной минимальному времени Т для восстановления бизнес-процесса организации:

$$\begin{cases} \sum X_i Treats = \rho_1 \bullet X_1 + \rho_2 \bullet X_2 \ldots \rho_n \bullet X_n = \max \sum T_i \\ \sum T_m = M_1 + M_2 + M_n = \min \sum T_m \end{cases} \tag{2}$$

Где: Ti – максимальное время простоя бизнес-процесса:

Тм - минимальное время на восстановление информационных активов бизнес-процесса.

Таким образом, ставится задача: найти экстремум (максимум или минимум) целевой функции f(x) при условии, что переменные x принадлежат некоторой области *G* (решений), при которых время потерь для бизнес-процесса организации будут минимальны, если организация применит мероприятия для повышения информационной безопасности *M*.

Далее, задача будет сводится к поиску такого набора мероприятий M_k по восстановлению бизнес-процесса организации (3):

$$\min M_n \to \max f\left(Z_m\right) \tag{3}$$

В итоге канонически двойственная формула задачи выбора оптимальной стратегии ИБ будет выглядеть следующим образом (4).

$$f\left(Z_m\right) \to \left(\max C_{xi}\right) - \left(\min C_m\right) = \pm \Delta M_z \tag{4}$$

При этом - максимальной сумме вероятностных ущербов Cxi - (от временных простоев) бизнес-процесса организации, должен противостоять (возместить) такой тип стратегии Mz (- набор мероприятий по противодействию угрозам Xi), которая равна минимальной стоимости восстановления Cm информационных активов, что и составляет задачу поиска функции Zм – типы стратегий защищенности информационных активов.

При ограничениях (5):

$$\begin{cases} \sum_{i=1}^{n} \rho_i * X_i Treat \le T_m (m = \overline{1, treat_1}) \\ \sum_{i=1}^{n} \rho_i * X_i Treat = T_m (m = \overline{treat_1 + 1, treat_2}) \\ \sum_{i=1}^{n} \rho_i * X_i Treat \ge T_m (m = \overline{treat_2 + 1, treat}) \\ Xi_{Treat} \ge 0 (i = \overline{1, n_1}) \\ X_{i^{Treat}} - (i = \overline{n_1 + 1, n_1}) \end{cases} \tag{5}$$

В результате диапазон $\pm\Delta M_z$, обозначает тип стратегии ИБ, где, (+) стратегия защищает информационные активы бизнес-процесса, а (-) стратегия не защищает информационные активы от вероятных атак.

При этом мероприятия информационной безопасности для соответствующих информационных угроз состоят из следующих переменных (6):

$$\sum M_z = M_1 restore + M_2 restore + M_3 restore \quad (6)$$

В таблице 11 представим возможный спектр угроз X информационной безопасности для соответствующих информационных угроз согласно построения информационной системы сети организации и описанного нами бизнес-процесса в таблице 11.

В таблице 11 представим возможный спектр мероприятий по восстановлению информационной безопасности для соответствующих информационных угроз согласно рисунку 6.

Таблица 11 – Потенциальные угрозы X_i для выбора мероприятий противодействия M_z в рамках проектируемой (оптимальной) стратегии ИБ организации

№ пп	Звено бизнес-процесса	Фактор угрозы для звена бизнес-процесса	Вид возможного ущерба	Вид угрозы	Вероятность реализации данной угрозы	
					максимум	минимум
1	2	3	4	5	6	7
1	Отдел бухгалтерского учета	Сбой или отсутствие расчетно-кассового обслуживания всей организации	Время простоя до получения аванса от заказчика	X1	0,6	0,3
2	Отдел дизайна	Сбой в процессе согласования дизайн-макета проекта с заказчиком)	Время простоя до получения аванса от заказчика	X2	0,5	0,25
3	Отдел продаж, Офис-менеджер организации	Сбой в процессе исполнения клиентского договора	Время простоя до получения итогового дохода (выручки) от заказчика	X3	0,6	0,3
4	Отдел бухгалтерского учета, Склад организации	Сбой в процессе доступа или отсутствие такого доступа к базе данных комплектующих, изменение ее содержимого	Время простоя общего времени монтажа и исполнения клиентского договора	X4	0,6	0,3

№ пп	Звено бизнес-процесса	Фактор угрозы для звена бизнес-процесса	Вид возможного ущерба	Вид угрозы	Вероятность реализации данной угрозы	
					максимум	минимум
1	2	3	4	5	6	7
5	Отдел смет и мат-технического сопровождения	Сбой или отсутствие доступа к базе данных смет и комплектующих, изменение их содержимого	Время простоя до подписания и начала старта исполнения клиентского договора	X5	0,4	0,3
6	Отдел бухгалтерского учета, Склад организации	Сбой или полный срыв поставки комплектующих для исполнения заказа по уже заключенным договорам с клиентами	Время простоя при исполнении клиентского договора	X6	0,5	0,25
7	Производственный отдел (монтаж, инженерия)	Сбой или технический отказ уже установленного по договору с клиентом смонтированного оборудования	Время простоя общего времени по окончании монтажа	X7	0,4	0,2
8	Все отделы организации	Сбой бизнес-процесса или вынужденные производственные простои от третьих лиц	Время простоя при исполнении клиентского договора	X8	0,01	0,001

№ пп	Звено бизнес-процесса	Фактор угрозы для звена бизнес-процесса	Вид возможного ущерба	Вид угрозы	Вероятность реализации данной угрозы	
					максимум	минимум
1	2	3	4	5	6	7
9	Все отделы организации	Уничтожение информационного актива путем заражения всех информационных активов компании	Потеря информационного актива организации	X9	0,01	0,001
10	Все отделы организации	Сбой, отказ в доступе или полное нарушение информационной целостности ПО или АО оборудования организации	Время простоя всего бизнес-процесса	X10	0,01	0,001
11	Все отделы организации	Потеря времени бизнес-процесса - "холостой" бизнес-процесс	Время "холостого" обслуживания при исполнении "лже"-клиентского договора	X11	0,01	0,001

В таблице 11 представлены на наш взгляд, наиболее реальные после проведения аудита угроз на конкретном примере организации 11-ть типологий угроз для бизнес-процесса исследуемой организации, которые необходимо преобразовать (упростить, объединить) для решения математической задачи известным -методом.

Отразим в таблице 12 исходный бизнес-процесс организации (на примере ООО «Кронвел» г. Ставрополь) в виде «маршрутной карты» бизнес-процесса для одного заказа на информационную услуг по монтажу системы видеонаблюдения для заказчика, для упрощения (объединения) факторов угроз до значения трех - X – таблица 12.

Таблица 12 –Стандартная маршрутная карта для бизнес-процесса для проекта заказа (на примере организации)

№пп	Название этапа бизнес-процесса	Начало этапа бизнес-процесса	Окончание этапа бизнес-процесса	Длительность этапа бизнес-процесса	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса
1	2	3	4	5	6	7
1	Приём заявки	Чт 11.04.19	Чт 11.04.19	1 ч	Иванова Татьяна	400,00 ₽
2	Замер объекта	Чт 11.04.19	Пт 12.04.19	10 ч	Менеджер проекта	3 800,00 ₽
3	Проект оборудования	Пт 12.04.19	Вт 16.04.19	16 ч	Начальник отдела проектирования	6 400,00 ₽
4	Проект монтажа	Пт 12.04.19	Пн 15.04.19	12 ч	Начальник отдела проектирования	6 800,00 ₽
5	Составление сметы на оборудования	Пн 15.04.19	Вт 16.04.19	18 ч	Сметчик	13 360,00 ₽
6	Составление сметы на монтаж; Excel	Пн 15.04.19	Пт 19.04.19	40 ч	Сметчик	13 400,00 ₽
7	Построение проекта монтажа в AUTOCad	Пт 12.04.19	Пт 19.04.19	40 ч	Автокадчик Алексей	12 200,00 ₽
8	Построение сметы монтажа	Пт 19.04.19	Вт 23.04.19	16 ч	Сметчик	3 367,00 ₽

№пп	Название этапа бизнес-процесса	Начало этапа бизнес-процесса	Окончание этапа бизнес-процесса	Длительность этапа бизнес-процесса	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса
1	2	3	4	5	6	7
9	Согласование с заказчиком	Пн 22.04.19	Вт 23.04.19	16 ч	зам. Дир. Бережнов	3 600,00 ₽
10	Заключение договора на КСЗИ	Чт 25.04.19	Пн 29.04.19	16 ч	Менеджер проекта	5 600,00 ₽
11	Создание и выставление счет-фактуры на монтаж	Пн 29.04.19	Вт 30.04.19	8 ч	Бухгалтер Иванова	19 760,00 ₽
12	Создание и выставление счет-фактуры на оборудование	Пн 29.04.19	Пн 29.04.19	8 ч	Бухгалтер Иванова	19 760,00 ₽
13	Получение предоплаты	Пн 29.04.19	Чт 02.05.19	24 ч	заказчик	- ₽
14	Закупка по Смете на закупку линейной части	Пн 29.04.19	Чт 02.05.19	24 ч	Материалы для линейной части	35 700,00 ₽
15	Закупка по Смете на оборудование	Пн 29.04.19	Чт 02.05.19	24 ч	Оборудование	411 755,00 ₽

№пп	Название этапа бизнес-процесса	Начало этапа бизнес-процесса	Окончание этапа бизнес-процесса	Длительность этапа бизнес-процесса	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса
1	2	3	4	5	6	7
16	Перфорация отверстий	Пн 06.05.19	Пн 13.05.19	48 ч	помощник Андрей	1 000,00 ₽
17	Прокладка соединительных линий	Пн 13.05.19	Пн 20.05.19	48 ч	помощник Андрей	500,00 ₽
18	затяжка проводов в трубы	Пн 20.05.19	Вт 21.05.19	8 ч	Слесарь Антон; Автокадчик Алексей	2 840,00 ₽
19	Тестирование линейной части	Пн 20.05.19	Ср 22.05.19	16 ч	Программист Святослав	4 000,00 ₽
20	Сдача по Акту линейной части	Пт 24.05.19	Вт 28.05.19	16 ч	Бухгалтер Иванова	3 520,00 ₽
21	Монтаж турникета	Пт 24.05.19	Пн 27.05.19	12 ч	Слесарь Антон; помощник Андрей;	2 860,00 ₽
22	Монтаж считывателя карт	Пт 24.05.19	Ср 29.05.19	24 ч	Программист Святослав; Слесарь Антон;	9 720,00 ₽
23	Монтаж ЦПУ и прочего оборудования	Пн 27.05.19	Пт 31.05.19	32 ч	помощник Андрей; Программист Святослав; Слесарь Антон	12 000,00 ₽

№пп	Название этапа бизнес-процесса	Начало этапа бизнес-процесса	Окончание этапа бизнес-процесса	Длительность этапа бизнес-процесса	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса
1	2	3	4	5	6	7
24	Настройка СКУД	Пн 03.06.19	Ср 05.06.19	20 ч	Программист Святослав; помощник Андрей; Слесарь Антон;	9 100,00 ₽
25	Тестирование системы	Чт 06.06.19	Пн 10.06.19	16 ч	Программист Святослав; помощник Андрей; Слесарь Антон;	6 480,00 ₽
26	Сдача объекта	Пн 10.06.19	Вт 11.06.19	12 ч	Иванова Татьяна; Перфораторщик Андрей; помощник Андрей; Программист Святослав; Слесарь Антон; зам. директора Бережнов	7 800,00 ₽
27	Окончательный расчет за СКУД	Пн 10.06.19	Чт 13.06.19	24 ч	заказчик	
			Итого	549 ч		615 722,00 ₽

Таблица 13 – Результат упрощения (объединения) факторов угроз для реализации поиска оптимальной стратегии ИБ

№п п	Название этапа бизнес-процесса	Длительность этапа бизнес-процесса, часах	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса	Декомпозиция факторов угроз X
1	2	3	4	5	6
1	Приём заявки	1	Иванова Татьяна	400,00 ₽	X1
2	Замер объекта	10	Менеджер проекта	3 800,00 ₽	X1
3	Проект оборудования	16	Начальник отдела проектирования	6 400,00 ₽	X2
4	Проект монтажа	12	Начальник отдела проектирования	6 800,00 ₽	X2
5	Составление сметы на оборудования	18	Сметчик	13 360,00 ₽	X2
6	Составление сметы на монтаж; Excel	40	Сметчик	13 400,00 ₽	X2
7	Построение проекта монтажа в AUTOCad	40	Автокадчик Алексей	12 200,00 ₽	X2
8	Построение сметы монтажа	16	Сметчик	3 367,00 ₽	X2
9	Согласование с заказчиком	16	зам. Дир. Бережнов	3 600,00 ₽	X1
10	Заключение договора на КСЗИ	16	Менеджер проекта	5 600,00 ₽	X1
11	Создание и выставление счет-фактуры на монтаж	8	Бухгалтер Иванова	19 760,00 ₽	X2
12	Создание и выставление счет-фактуры на оборудование	8	Бухгалтер Иванова	19 760,00 ₽	X2

№пп	Название этапа бизнес-процесса	Длительность этапа бизнес-процесса, часах	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса	Декомпозиция факторов угроз X
1	2	3	4	5	6
14	Закупка по Смете на закупку линейной части	24	Материалы для линейной части	35 700,00 ₽	X3
15	Закупка по Смете на оборудование	24	Оборудование	411 755,00 ₽	X3
16	Перфорация отверстий	48	помощник Андрей	1 000,00 ₽	X3
17	Прокладка соединительных линий	48	помощник Андрей	500,00 ₽	X3
18	затяжка проводов в трубы	8	Слесарь Антон; Автокадчик Алексей	2 840,00 ₽	X3
19	Тестирование линейной части	16	Программист Святослав	4 000,00 ₽	X1
20	Сдача по Акту линейной части	16	Бухгалтер Иванова	3 520,00 ₽	X2
21	Монтаж турникета	12	Слесарь Антон; помощник Андрей;	2 860,00 ₽	X3
22	Монтаж считывателя карт	24	Программист Святослав; Слесарь Антон;	9 720,00 ₽	X3
23	Монтаж ЦПУ и прочего оборудования	32	помощник Андрей; Программист Святослав; Слесарь Антон	12 000,00 ₽	X3
24	Настройка СКУД	20	Программист Святослав; помощник Андрей; Слесарь Антон;	9 100,00 ₽	X3

№пп	Название этапа бизнес-процесса	Длительность этапа бизнес-процесса, часах	Название ресурсов, используемых на этапе бизнес-процесса	Затраты на этап бизнес-процесса	Декомпозиция факторов угроз X
1	2	3	4	5	6
25	Тестирование системы	16	Программист Святослав; помощник Андрей; Слесарь Антон;	6 480,00 ₽	X3
26	Сдача объекта	12	Иванова Татьяна; Перфораторщик Андрей; помощник Андрей; Программист Святослав; Слесарь Антон; зам.	7 800,00 ₽	X1

В результате преобразований мы получим следующие факторы угроз бизнес-процессу организации и их значения:

– $\sum X_1 Treats = 87$ на сумму возможного ущерба 31680 рублей,

– $\sum X_2 Treats = 174$ на сумму возможного ущерба 98567 рублей,

– $\sum X_3 Treats = 240$ на сумму возможного ущерба 485475 рублей.

Соответственно, средняя тяжесть воздействия угроз по каждому из предложенных факторов различна (без учета вероятности):

$X_1 = 364{,}14$ рублей,

$X_2 = 566{,}48$ рублей,

$X_3 = 2022{,}81$ рублей.

И если учесть вероятности воздействия согласно данным таблицы 11, то получим следующие итоговые веса факторов, объединенных по зонам воздействия их на бизнес-процесс, таблица 14.

Таблица 14 - Итоговые значения факторов угроз X для бизнес-процесса

Вид угрозы	Зона воздействия на бизнес-процесс	Возможный ущерб (простой бизнес-процесса) согласно аудиту вероятности реализации данной угрозы (час)			Возможный ущерб согласно аудиту вероятности реализации данной угрозы (руб./1 час)	
1	2	3	4	5	6	7
$\sum X_i Treats$	Организация	максимум	средний	минимум	максимум	минимум
$X_1 =$	Сбыт и сервис	60,9	39,15	26,1	163,86	109,24
$X_2 =$	Учет	121,8	104,4	69,6	339,89	226,59
$X_3 =$	Производство	168	48	24	404,56	202,28
	Итого: T	350,7	191,55	119,7		

В следующей таблице 15 приводятся мероприятия для противодействия угрозам бизнес-процесса и среди них такая категория – настройка политики безопасности и восстановление информационных активов организации. Для реализации математической задачи – поиска оптимальной стратегии информационной безопасности (далее ИБ) также упростим (объединим) возможные стратегии из мероприятий по трем направлениям:

– $\sum M_1 restore$ - максимально-долгая настройка и восстановление предыдущего информационного актива (информационной единицы) звена бизнес-процесса,

– $\sum M_2 restore$ - средняя по времени настройка и создание политики безопасности организации с учетом актуальных угроз компьютерных систем на основе ролей и функций в бизнес-процессе,

– $\sum M_3 restore$ - минимальная по времени настройка политики информационной безопасности всего бизнес-процесса организации.

Необходимо уточнить данное понятие: политика безопасности организации в области ИБ - это совокупность документируемых решений в виде программных, аппаратных, организационных, административных,

юридических, физических мер, методов, средств, правил и инструкций, чётко регламентирующих все аспекты деятельности организации в области безопасности ИБ.

Основная цель политики безопасности – информирование пользователей, сотрудников и руководства о наложенных на них обязательных требованиях по защите технологии и информационных ресурсов.

Среди наиболее важных мероприятий на сегодня специалисты выделяют мероприятия по противодействию атакам:

– своевременное применение обновлений безопасности (все устройства),

– DDoS атаки – настройка маршрутизаторов на защиту от DDoS, услуги сетей доставки контента (Content Delivery Network),

– применение антивирусной защиты,

– применение системы предотвращения вторжений,

– ведение журналов активности, периодическая их проверка,

– парольная политика, разрешающая только стойкие пароли,

– периодический аудит (тестирование на проникновение).

Все документально оформленные решения, формирующие политику безопасности ИБ, должны быть утверждены руководством и опубликованы. Все сотрудники организации должны быть ознакомлены с политикой безопасности ИБ. Концептуальные вопросы политики безопасности организации целесообразно изложить в «Концепции обеспечения безопасности в автоматизированной системе организации».

Для исследуемой организации в таблице 15 приведены основные мероприятия по восстановлению и переформатированию политики ИБ и объединены в три следующие группы М для разных уровней атак и угроз.

В свою очередь на время восстановления ИБ, основными составляющими временных затрат, будут вопросы:

– определение целей политики безопасности,

– определение принципов обеспечения и границ применяемости политики безопасности,

– краткое разъяснение (дайджест) политики безопасности,

– соответствие законодательным актам и стандартам,

– определение правил приобретения информационных технологий, которые отвечают требованиям безопасности,

– определение политики обеспечения непрерывности работы и восстановления АС,

– определение политики конфиденциальности стандартных сервисов (электронная почта (ЭП), Интернет, VPN, мобильные пользователи),

– определение политики аутентификации (пароли, рекомендации по аутентификации удалённых субъектов и использованию аутентифицирующих устройств),

Таблица 15 – Результат упрощения (объединения) мероприятий ИБ для выбора стратегии информационной безопасности организации

№ пп	Мероприятие для противодействия угрозам бизнес-процесса организации	Время восстановления (часах) если атака агрессивная	Время восстановления (часах) если атака умеренная	Время восстановления (часах) если атака слабая	Фактор модели
1	2	3	4	5	6
1	Настройка и восстановление предыдущего информационного актива (информационной единицы) звена, в том числе:	476	333,2	142,8	M_1
	а) базы 1С:Бухгалтерия	112	78,4	33,6	
	б) базы 1С:Склад	72	50,4	21,6	
	в) проекты AdobePhotoshop	48	33,6	14,4	
	г) базы Microsoft Excel (калькуляции)	36	25,2	10,8	

№ пп	Мероприятие для противодействия угрозам бизнес-процесса организации	Время восстановления (часах) если атака агрессивная	Время восстановления (часах) если атака умеренная	Время восстановления (часах) если атака слабая	Фактор модели
1	2	3	4	5	6
	д) базы договоров с поставщиками	160	112	48	
	е) базы договоров с заказчиками	48	33,6	14,4	
2	Настройка политики инф. безопасности (в том числе):	89	62,3	26,7	M_2
	а) перенастройка оборудования в соответствии с созданной политикой безопасности	24	16,8	7,2	
	б) замена оборудования, которое невозможно настроить в соответствии с созданной политикой	25	17,5	7,5	
	в) настройка системы контроля доступа (TACACS/RADIUS/AD)	11	7,7	3,3	
	г) настройка политики безопасности на клиентских машинах организации (доменные политики AD, политики ограниченного распространения программ)	5	3,5	1,5	
	д) политика минимального доступа для пользователей к звеньям бизнес-процесса	5	3,5	1,5	
	е) настройка коммутационного оборудования на основе политики безопасности	16	11,2	4,8	

№ пп	Мероприятие для противодействия угрозам бизнес-процесса организации	Время восстановления (часах) если атака агрессивная	Время восстановления (часах) если атака умеренная	Время восстановления (часах) если атака слабая	Фактор модели
1	2	3	4	5	6
	ж) настройка доступа к сетевым ресурсам на основе политики безопасности и ролей подразделений организации	3	2,1	0,9	
3	Создание политики безопасности организации с учетом актуальных угроз компьютерных систем на основе ролей и функций в бизнес-процессе	40	28	12	M_3
	Итого Т на восстановление:	605	423,5	181,5	

Мероприятия ИБ для выбора стратегии информационной безопасности организации:

– определение политики разграничения доступа и привилегии для различных категорий сотрудников (пользователей, системных администраторов, администраторов безопасности, руководителей),

– обнаружение и блокирование вирусов и других вредоносных программ,

– определение порядка разработки и сопровождения АС,

– обучение персонала по вопросам безопасности ИБ,

– защита от не декларированных возможностей ПО,

– ликвидация последствий нарушения политики безопасности и ответственность нарушителей,

– ссылки на более детальные документы по безопасности ИБ (положения, инструкции),

– аудит и обновление политики безопасности.

К сожалению, на практике после внедрения в организациях систем обеспечения ИБ могут быть недостатки, среди которых можно выделить типовые:

– отсутствие необходимой организационной основы, обеспечивающей согласованные действия подразделений организации по выработке и реализации единой политики безопасности ИБ,

– отсутствие в организационно-штатной структуре организации специального подразделения, непосредственно ответственного за решение вопросов обеспечения безопасности ИБ в организации, за разработку и внедрение в организации единой технологии управления безопасностью ИБ,

– неполнота и противоречивость нормативно-правовой базы организации по вопросам обеспечения безопасности ИБ, слабая увязка существующих организационно-распорядительных документов с реальными потребностями и требованиями законодательства Российской Федерации,

– отсутствие системного подхода к обеспечению безопасности ИБ организации, при котором была бы обеспечена комплексная защита информации на всех этапах жизненного цикла АС и технологических циклов её обработки и передачи.

Среди таких методик можно назвать Infrastructure Maturity Model (Gartner Group), Architecture Maturity Model (MTI), Infrastructure Optimization Model (Microsoft) и ряд других. Набор сервисов в моделях зрелости часто называют уровнем зрелости.

2.4 Выводы по разделу

В данном разделе разработана модель угроз для бизнес-процесса организации. Представлен рисунок вербального наполнения факторами будущей стратегии информационной безопасности организации. Расписана иерархия, которая предусматривает вероятность возникновения угроз ИБ.

Определены потенциальные проблемы угроз ИБ, которые могут быть с внешнего периметра (интернета), по устройствам сети.

Представлена канонически двойственная формула задачи выбора оптимальной стратегии ИБ.

Представлен исходный бизнес-процесс организации (на примере ООО «Кронвел» г. Ставрополь) в виде «маршрутной карты» бизнес-процесса для одного заказа на информационную услуг по монтажу системы видеонаблюдения для заказчика, для упрощения (объединения) факторов угроз до значения трех - X.

3 Методические рекомендации по выбору условно-оптимальной стратегии информационной безопасности организации

3.1 Расчет итоговых значений комбинаторики стратегии информационной безопасности организации

Согласно исходным данным изложенным ранее в параграфе 2.3 настоящего исследования, мы условно различаем одновременно и зоны вероятных атак бизнес-процесса для исследуемой организации, и типы возможных мер противодействия для последующего выбора стратегий информационной безопасности, позволяющих в той или иной мере противостоять организации возможным угрозам.

Поэтому результатом такого выбора может быть условно-оптимальная стратегия, поскольку присутствуют условные факторы (элементы теории игр) выбора. Непосредственно на сам выбор стратегии ИБ, будет влиять следующие факторы:

1. вероятность атак исследуемой организации со стороны «внешних» злоумышленников;
2. потенциал злоумышленника, по градации приказа ФСТЭК;
3. уровень оплаты труда специалиста по ИБ (руб./час) – как фактор самого выбора администрацией стратегии по противостоянию внешним информационным угрозам.

В таблице 3.1 представлены и сгруппированы данные факторы, а в следующей за ней таблице 3.2 представлены результаты расчетов величин возможных экономических ущербов от потери информационных активов исследуемой организации на примере ее бизнес-процесса.

В таблице 3.1 параметрами комбинаторики выбора стратегии ИБ будут 2 строка- фактор «Вероятность атак по данным фирмы InfoWatch (лаборатория Касперского)» и 4-ая строка – фактор «Уровень оплаты труда специалиста по ИБ».

Таблица 3.1 – Исходные факторы выбора стратегии ИБ

№ пп	Факторы выбора	Тип возможных атак		
		агрессивная	умеренная	минимальная
1	2	3	4	5
1	Вероятность атак = (Потенциал нарушителя *фактические случаи)	0,99	0,25	0,03
2	По данным InfoWatch	1	0,5	0,2
		высокий (Н6)	средний (Н5-Н4)	низкий(Н1-Н3)
3	Потенциал нарушителя по ФСТЭК	0,99	0,5	0,15
4	Уровень оплаты труда специалиста по ИБ (руб./час)	2000	900	200
5	Зарплата специалиста ИБ в месяц (на 01.11.2019 г.)	320 000*	144 000*	32 000*
	где -*(регион оплаты)	зарубежье	г. Москва	г. Ставрополь

Такая комбинация наиболее реально на сегодня отвечает требованиям механизма функционирования (менеджмента) исследуемой организации и соответствует «пониманию» ее руководства как принять решение о выборе стратегии парасостояния информационным угрозам.

Так при оплате труда специалиста по информационной безопасности в размере 200 руб./час., администрация исследуемой организации увидит, согласно расчетам математической модели от какого реального экономического ущерба будут защищены ее информационные активы по зонам бизнес-процесса, но при условной вероятности и уровне «потенциала» возможной атаки на организацию.

Однако, среди возможных типов стратегий, каждая из которых будет условно-оптимальной поскольку присутствует условная вероятность возникновения атак нарушителя, мы произведем комбинаторику (набор вариаций) возможных стратегий защищенности информационных активов организации, участвующих в ее бизнес-процессе по этапам: нулевая защищенность, защищенность – зоны БП «сервис офиса», защищенность – зоны БП «учет офиса» и защищенность – зоны БП «производство».

Администрация должна обладать знаниями о ближайших «конкурентах», действующих на ее сегменте рынка бизнеса, знать основные экономические особенности функционирования механизма ее бизнес-процесса и оценивать зоны возможных и потенциальных угроз.

Произведем расчеты для варианта полного отсутствия стратегии ИБ, когда нет специалиста по ИБ. В таблице 3.2 и рисунке 3.1 отразим такой тип стратегии. Такой тип стратегии условно назовем – нулевая.

Таблица 3.2 – Результат «нулевой» стратегии ИБ для БП организации

№ пп	Информационные активы организации	Зоны БП	Сверхзащищенность ИА (+) / Незащищенность ИА (-) информационных активов организации по зонам БП		
	Зоны БП	Угрозы по зонам БП	высокий (Н6)	средний (Н5-Н4)	низкий(Н1-Н3)
		Тип стратегии по зонам БП	X1	X2	X3
1	Учет офиса	M1=t1	-97581,3	-24641,8	-2957,0
2	Производство	M2=M1+t2	-494757,5	-124938,8	-14992,7
3	Сервис офиса	M3=M1+M2+t3	-31363,2	-7920,0	-950,4
4	Весь БП		-623702,0	-157500,5	-18900,1

Как видно, из значений таблицы 3.2 для «нулевой» стратегии ИБ максимально-возможный ущерб составит 623,7 тыс. рублей, что и равно стоимости всего бизнес-процесса согласно таблице 2.2 настоящего исследования. Также мы видим величину возможных экономических ущербов для информационных активов по зонам бизнес-процесса, так для:

- зона «Учет офиса» = -97,58 тыс. рублей;
- зона «Производство» = - 494,75 тыс. рублей;
- зона «Сервис офиса» = -31,36 тыс. рублей.

Далее на рисунке 3.1, отразим графически как выглядит защищенность информационных активов организации по зонам бизнес-процесса.

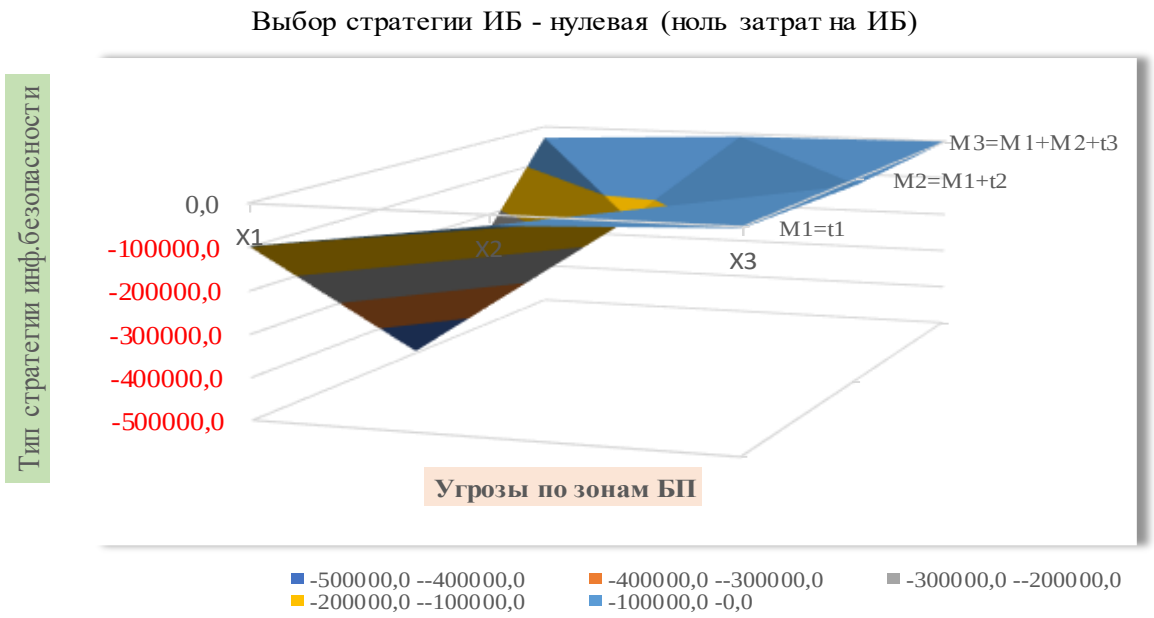

Рисунок 3.1 – Выбор «нулевой» стратегии защищенности информационных активов участвующих в бизнес-процессе организации

Как видно из рисунка 3.1 максимальная незащищенность (или возможный ущерб) на сумму -623,7 тыс. руб., возникнет в случае атаки всех зон бизнес-процесса, далее по зонам ущербы составят – для зоны X1 (производство) =-494,75, для зоны X2 (производство) =-124,9, и для зоны X3 (производство) =-14,99 тыс. руб.

Таким образом- самым незащищенной зоной бизнес-процесса, в случае если вообще не будут произведены затраты на информационную стратегию (или 0 рублей) будет производство.

Произведем расчеты для варианта, когда на работу приняты специалисты по информационной безопасности, и когда при реализации информационной политики по ИБ – будет достигнут ноль суммы ущербов по одной из любых зон бизнес-процесса. При этом затраты на оплату труда специалистов применим для всех типов атак, подразумевая что специалист будет пытаться защитить бизнес-процесс организации от всех типов нарушителей. Данный факт будет иметь исходный вид в таблице 3.3.

Таблица 3.3 – Исходные данные для модели выбора «минимальной» стратегии защищенности организации

№ пп	Факторы выбора	Тип возможных атак		
		агрессивная	умеренная	минимальная
1	2	3	4	5
1	Вероятность атак = (Потенциал нарушителя *фактические случаи)	0,99	0,25	0,03
2	По данным InfoWatch	1	0,5	0,2
		высокий (Н6)	средний (Н5-Н4)	низкий(Н1-Н3)
3	Потенциал нарушителя по ФСТЭК	0,99	0,5	0,15
4	Уровень оплаты труда специалиста по ИБ (руб./час)	210,335	210,335	210,335
5	Зарплата специалиста ИБ в месяц (на 01.11.2019 г.)	33653,6	33653,6	33653,6
	где -*(регион оплаты)	зарубежье	г. Москва	г. Ставрополь

Как видно из таблицы уровень оплаты труда специалистов для достижения «минимальной» стратегии защищенности бизнес-процесса должен составлять 210, 335 рублей/час, или 33653,6 рублей зарплаты в месяц. Далее в таблице 3.4 и рисунке 3.2 отразим расчетные значения защищённости информационных активов бизнес-процесса для такого типа стратегии.

Такой тип стратегии условно мы предложили назвать – «минимальная» защищенность.

Как видно, из значений таблицы 3.4 для «минимальной» стратегии ИБ максимально-возможный ущерб составит 310,9 тыс. рублей, что вдвое меньше «нулевой» стратегии и равно части стоимости бизнес-процесса согласно таблице 2.2 настоящего исследования.

Также мы видим величину возможных экономических ущербов или их отсутствия для информационных активов по зонам бизнес-процесса, так для:

- зона «Учет офиса» = защищенность полностью восстановлена;
- зона «Производство» = - 382,27 тыс. рублей;
- зона «Сервис офиса» = защищенность полностью восстановлена.

Таблица 3.4 – Результат «минимальной» стратегии ИБ для БП организации

№ пп	Информационные активы организации	Зоны БП	Сверхзащищенность ИА (+) / Незащищенность ИА (-) информационных активов организации по зонам БП		
	Зоны БП	Угрозы по зонам БП	высокий (Н6)	средний (Н5-Н4)	низкий(Н1-Н3)
		Тип стратегии по зонам БП	X1	X2	X3
1	Учет офиса	M1=t1	17779,0	28665,6	8704,0
2	Производство	M2=M1+t2	-382728,8	-66633,9	0,0
3	Сервис офиса	M3=M1+M2+t3	54011,8	43721,4	15708,1
4	Весь БП		-310938,0	5753,1	24412,1

На рисунке 3.2 отразим стратегию ИБ «минимальную» защищенность.

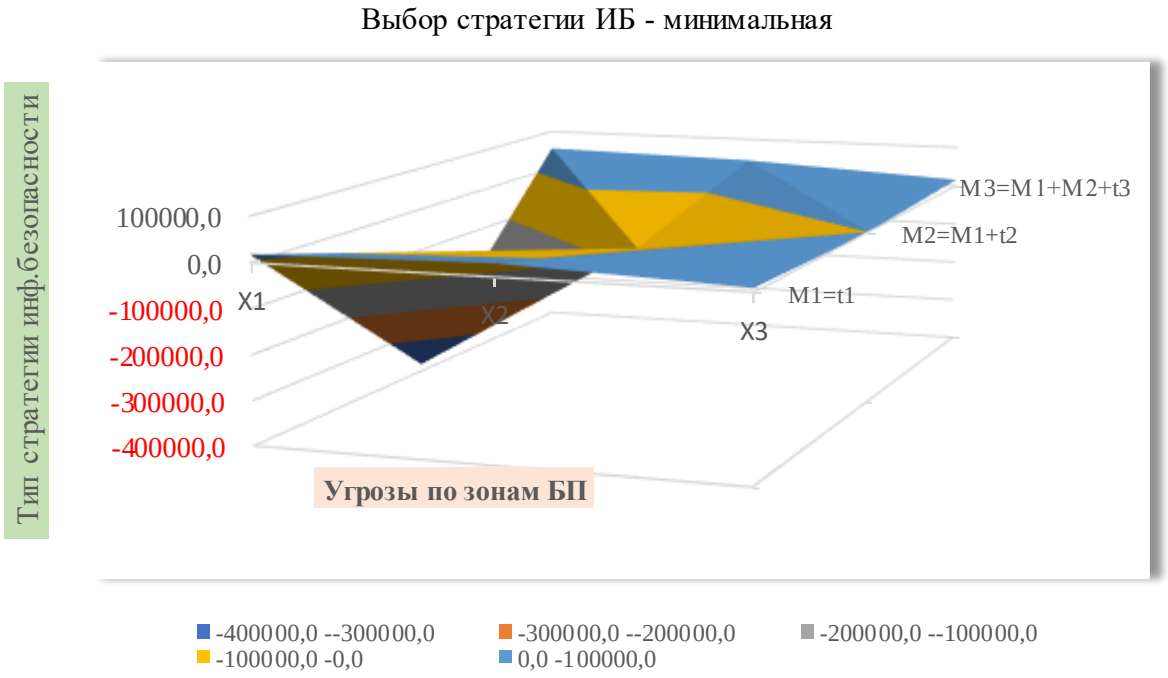

Рисунок 3.1 – Выбор «минимальной» стратегии защищенности информационных активов бизнес-процесса организации

Главной особенностью данной стратегии выбора информационной безопасности является наличие «порога» условности, что атака нарушителя с высоким потенциалом учтена таким образом, что руководство организации

понимает, что со стороны ближайших конкурентов возникновение атаки на бизнес-процесс уже ограничено по 2-м зонам, и ресурсы злоумышленников должны превышать кратно стоимость информационных ресурсов от их текущей стоимости на сумму 610 ты. рублей.

Произведем расчет следующего этапа комбинаторики математической модели методом приближения к «последнему» нулю возможных ущербов в зоне бизнес-процесса «производство».

Составим таблицу 3.5, исходные данные для выбора «максимальной» стратегии защищённости бизнес-процесса организации.

Таблица 3.5 – Исходные данные для модели выбора «максимальной» стратегии защищенности организации

№ пп	Факторы выбора	Тип возможных атак		
		агрессивная	умеренная	минимальная
1	2	3	4	5
1	Вероятность атак = (Потенциал нарушителя *фактические случаи)	0,99	0,25	0,03
2	По данным InfoWatch	1	0,5	0,2
		высокий (Н6)	средний (Н5-Н4)	низкий(Н1-Н3)
3	Потенциал нарушителя по ФСТЭК	0,99	0,5	0,15
4	Уровень оплаты труда специалиста по ИБ (руб./час)	928,9127	450,717	210,335
5	Зарплата специалиста ИБ в месяц (на 01.11.2019 г.)	148626,03	72114,72	33653,6
	где -*(регион оплаты)	зарубежье	г. Москва	г. Ставрополь

Как видно из таблицы 3.5 уровень оплаты труда специалистов для достижения «минимальной» стратегии защищенности бизнес-процесса должен составлять по зонам бизнес-процесса и в зависимости от уровня потенциала нарушителя ФСТЭК: Н6 = 928 руб./час и сумма 148,6 тыс. рублей, Н5-Н4 = 450,7 руб./час, или 72114,7 рублей зарплаты в месяц, и для Н1-Н3=210,335 ру./час. Или 33653 рублей в месяц.

Далее в таблице 3.6 и рисунке 3.3 отразим расчетные значения защищённости информационных активов бизнес-процесса для такого типа стратегии как «максимальная».

Таблица 3.6 – Результат «максимальной» стратегии ИБ для информационных активов организации

№ пп	Информационные активы организации	Зоны БП	Сверхзащищённость ИА (+) / Незащищенность ИА (-) информационных активов организации по зонам БП		
	Зоны БП	Угрозы по зонам БП	высокий (Н6)	средний (Н5-Н4)	низкий(Н1-Н3)
		Тип стратегии по зонам БП	X1	X2	X3
1	Учет офиса	M1=t1	411890,1	89588,0	8704,0
2	Производство	M2=M1+t2	0,0	0,0	0,0
3	Сервис офиса	M3=M1+M2+t3	345682,5	102740,0	15708,1
4	Весь БП		757572,6	192328,0	24412,1

Как видно, из значений таблицы 3.6 для «максимальной» стратегии ИБ возможный ущерб по самой «уязвимой» зоне бизнес-процесса – производство составит 0 рублей, что и является условно-оптимальной стратегией, но однако уже превышает саму стоимость информационных активов бизнес-процесса согласно таблице 2.2 настоящего исследования 757,5 тыс. рублей вместо суммы 630 тыс. рублей.

Т.е. данная стратегия говорит о некой «переплате» (сверхзащищённости) на мероприятия по восстановлению, настройке и резервированию информационных активов бизнес-процесса организации на сумму 27,5 тыс. рублей.

Но мы уже не видим величину возможных экономических ущербов для информационных активов по зонам бизнес-процесса.

На рисунке 3.3 отразим стратегию ИБ «максимальную» защищенность.

Рисунок 3.3 – Выбор «максимальной» стратегии защищенности информационных активов бизнес-процесса организации

Главной особенностью максимальной стратегии выбора информационной безопасности является наличие «порога» условности, что атака нарушителя с высоким и средним потенциалом учтена таким образом, что руководство организации понимает, что со стороны ближайших конкурентов возникновение атаки на бизнес-процесс уже ограничено по всем 3-м зонам, и ресурсы злоумышленников должны превышать кратно стоимость информационных ресурсов от их текущей стоимости на сумму более чем 757 тыс. рублей.

3.2 Технико-экономическое обоснование выбора стратегии информационной безопасности бизнес-процесса

Среди известных методик технико-экономического обоснования выбора стратегий и политик информационной безопасности, наиболее известными или целесообразными в данном контексте исследования, можно применить

методику бюджетозащищенности организации, видоизменив ее основной показатель на процессозащищенность информационных активов организации.

Процессозащищенность (Ps – *Process safety*) в данном случае (3.15), будет отражать отношение стоимости восстановления информационных активов $CR^z_{process}$ (*Cost of Reconstruction information assets*) к их стоимости $CIA^z_{process}$ (*Cost of Information Assets*) по зонам бизнес-процесса.

$$P_s = \frac{CR^z_{process}}{CIA^z_{process}} \qquad (3.15)$$

Соответственно представим в таблице 3.7 исходные данные для расчета процессозащищенности.

Таблица 3.7 – Исходные данные для технико-экономического обоснования выбора стратегии ИБ для информационных активов организации

Тип стратегии	Стоимость 1 часа восстановления информационного актива	Стоимость 1 часа бизнес-процесса	$CR^z_{process}$ - затраты по восстановлению ИА блока БП (руб.)			$CIA^z_{process}$ Стоимость ИА по зоне БП (руб.)		
			Высокий (Н6)	средний (Н5-Н4)	Низкий (Н1-Н3)	X1	X2	X3
1	2	3	4	5	6	7	8	9
Нулевая	0,0	444,0	0,0	0,0	0,0	97581,3	24641,8	2957,0
	0,0	1864,8	0,0	0,0	0,0	494757,5	124938,8	14992,7
	0,0	364,1	0,0	0,0	0,0	31363,2	7920,0	950,4
	0,0	1091,9	0,0	0,0	0,0	623702,0	157500,5	18900,1
минимальная	210,3	444,0	115360,3	53307,3	11661,0	87823,2	22177,6	2957,0
	210,3	1864,8	112028,6	58304,9	14992,7	445281,7	112444,9	14992,7
	210,3	364,1	85375,0	51641,4	16658,5	28226,9	7128,0	950,4
	210,3	1091,9	312763,9	163253,6	43312,2	561331,8	141750,5	18900,1
максимальная	928,9	444,0	509471,5	114229,7	11661,0	97581,3	24641,8	2957,0
	450,7	1864,8	494757,5	124938,8	14992,7	494757,5	124938,8	14992,7
	210,3	364,1	377045,7	110660,0	16658,5	31363,2	7920,0	950,4
	530,0	1091,9	1381274,6	349828,5	43312,2	623702,0	157500,5	18900,1

Для нашего исследования так же будет целесообразно посчитать процессозащищенность в целом для бизнес-процесса как отношение суммы Ps

и отдельно по зонам офиса организации – их три: «учет офиса», «производство» и «сервис офиса».

В результате выполнения формулы 3.15 мы получим следующие результаты процессозащищенности (таблица 3.8) по зонам бизнес-процесса организации и в целом.

Таблица 3.8 – Результаты показателя процессозащищенности для информационных активов организации (нумерация столбцов продолжена согласно данным таблицы 3.7)

Тип стратегии	Показатель P_s процессозащищенности информационных активов (руб. /руб.)			Стратегический "рычаг" процессо-защищенности ИА (руб./руб.)	Удельный вес "рычага" в коэффициенте процессозащищенности ИА (отн. число)		
	стл.4/стл.7	стл.5/стл.8	стл.6/стл.9	стл.2/стл.3	стл.13/стл.10	стл.13/стл.11	стл.13/стл.12
1	10	11	12	13	14	15	16
минимальная	1,314	2,404	3,944	0,474	0,361	0,197	0,120
	0,252	0,519	1,000	0,113	0,448	0,218	0,113
	3,025	7,245	17,528	0,578	0,191	0,080	0,033
	0,557	1,152	2,292	0,193	0,346	0,167	0,084
максимальная	5,221	4,636	3,944	2,092	0,401	0,451	0,531
	1,000	1,000	1,000	0,242	0,242	0,242	0,242
	12,022	13,972	17,528	0,578	0,048	0,041	0,033
	2,215	2,221	2,292	0,485	0,219	0,219	0,212

Поскольку для нулевой стратегии значения выпадают и не актуальны, данные расчеты «опущены». Расчет произведен для двух типов стратегий – «минимальная» и «максимальная» защищенность информационных активов.

Как видно из полученных значений таблицы 3.8, столбцы 10,11,12 и 13 показали что по строке «производство» для «минимальной» стратегии защищенности информационных активов – руководство организации привлекая 0,113 рубля (11 копеек) на 1 рубль стоимости информационных активов по зоне «Производство» бизнес-процесса минимальная стратегия НЕ защищает от потенциальных нарушителей по приказу ФСТЭК Н6 – Н4.

А «вкладывая» 0,242 рубля (24 копейки) на 1 рубль информационных активов по «максимальной» стратегии – руководство уже получит Защиту от всех типов потенциальных нарушителей.

Таким образом, выбор стратегии ИБ (мероприятий по защищенности) фокусируется между значениями 11 копеек или 24 копейки на 1 рубль стоимости информационных активов участвующих в бизнес-процессе всей организации.

Отразим на рисунке 3.3 линию Парето – как метод выбора руководством организации стратегии информационной безопасности – или защищенности информационных активов при максимальном типе.

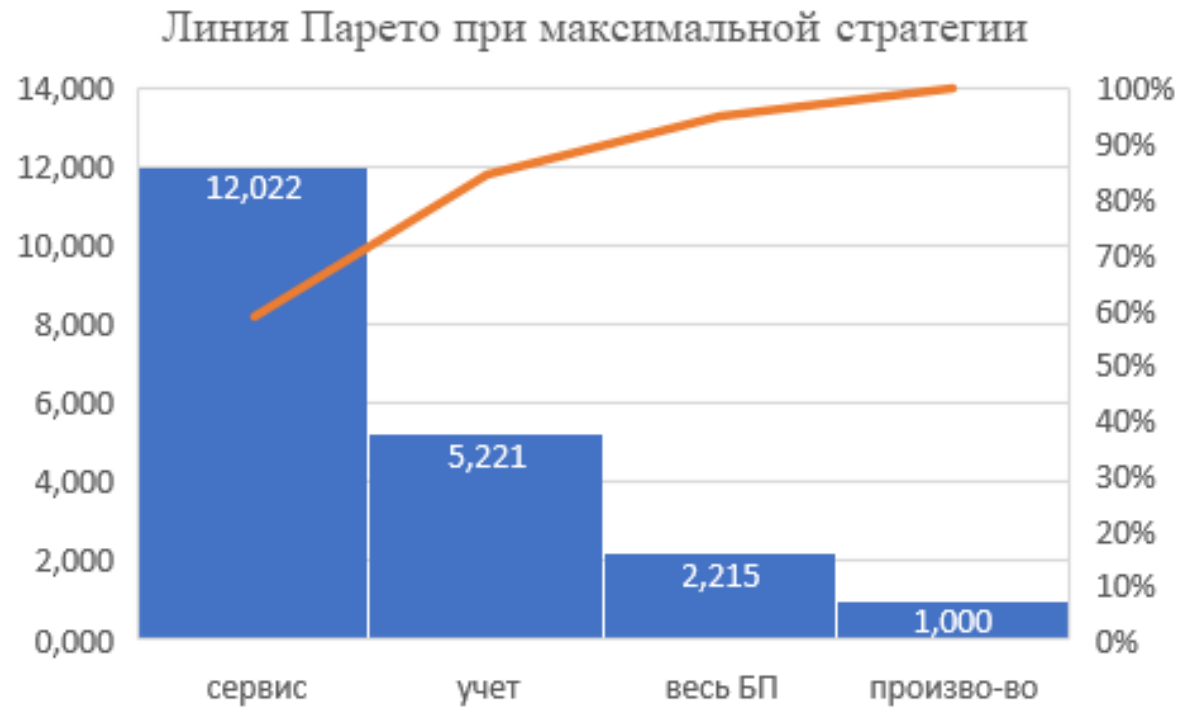

Рисунок 3.3. – Линия Парето – эффективности для максимальной стратегии (Microsoft Excel ресурс)

Как видно из рисунка 3.3 при выборе стратегии руководству исследуемой организации выбор максимальной стратегии будет «стоить» по принципу Парето – 80% защищенности, если руководством данной организации будет затрачено 2,215 рублей – или 20% усилий, на затраты

(мероприятия) по восстановлению или защите её информационных активов в целом по всему бизнес-процессу.

При этом не менее интересный вывод можно сделать о «рычаге» стратегии, который, по сути, отражает «плечо» (силу) стратегии для повышения защищенности информационных активов.

Так значение для зоны «учет офиса» 2,092 означает что по максимальной стратегии будет привлечено 2 рубля мероприятий по защите информационных активов на 1 рубль их совокупной стоимости по данной зоне.

Таким образом, руководство может сделать свой окончательный выбор за минимальные или максимальные стратегии по экономическому критерию – достаточно или недостаточно, выгодно или не выгодно применить минимальную или максимальную типы стратегий.

3.3 Выводы по разделу

В данном разделе представлены методы расчета значений по выбору стратегии информационной безопасности информационных активов организации задействованные в ее бизнес-процессе, а также вероятные угрозы и их оценка, разработаны предложения по регистрации и идентификации информационных угроз и моделированию стратегии информационной безопасности, а именно рекомендации по применению математической модели при расчете необходимых и оптимальных параметров выбора стратегии информационной безопасности бизнес-процесса организации.

Исходя из деятельности организации, представлены расчёты технико-экономического обоснования использования данных рекомендаций.

ЗАКЛЮЧЕНИЕ

В первом разделе выпускной работы рассмотрены:

– основы информационной безопасности бизнес-процессу организации и современные проблемы данной теории,

– цель обеспечения информационной безопасности информационных активов организации участвующих в бизнес-процессе,

– методологические основы информационной безопасности для выбора стратегии ИБ,

– типы современных угроз информационной безопасности,

– компоненты, подлежащие защите информационной безопасности.

Также перечислены тактические мероприятия по обеспечению информационной безопасности организации.

Представлена динамика угроз информационной безопасности в 2018 году на примере нескольких организаций, которая включила в себя всевозможное оборудование, которое контактирует с сетью.

Более подробно рассмотрен зарубежный опыт разработки стратегии информационной безопасности, а также, опыт регистрации угроз и законодательство о киберпреступлениях, где указаны статьи и сроки наказаний Уголовного кодекса в различных странах.

Приведены наглядные примеры факторов, влияющих на разработку стратегии информационной безопасности для организаций.

Во втором разделе описаны теоретические основы моделирования стратегии и методологические проблемы определения целей стратегического моделирования информационной безопасности для бизнес-процесса организации.

Представлены рисунки расположения субъектов управления информационной системой бизнес-процесса организации, объединённых единым киберпространством. Указаны возможные атаки по зонам бизнес-процесса, а также разработаны необходимые мероприятий по противодействию кибератакам извне среды организации.

Представлено вербальное математическое описание факторной модели информационной безопасности для бизнес-процесса с использованием входных и выходные величин вероятности угроз для всей системы информационной безопасности, а также любые влияющие на них факторы со стороны внешней среды. Вероятные угрозы приводят в простою бизнес-процесса на величину времени, а меры противодействия имеют время необходимое для реализации типа стратегии ИБ.

В третьем разделе представлена методика расчета математической модели подбора факторов противодействия угрозам, их оценка, и расчет уровня защищенности информационной системы бизнес-процесса в рамках тех предложений стратегии безопасности которые противостоят угрозам, а именно методические рекомендации по выбору оптимально-достаточной стратегии информационной безопасности в среде организации с позиции необходимых ресурсов.

Исходя из деятельности организации, представлены расчёты технико-экономического обоснования использования данных рекомендаций.

Таким образом, цель работы достигнута, применение разработанных рекомендаций дает возможность методом Парето выбрать одну из предлагаемых стратегий – минимальную или максимальную защищенность информационных активов.

Теоретическая значимость работы состоит в основах моделирования стратегии кибербезопасности организации и в оценке технико-экономической оценке разработанных рекомендаций.

Практическая значимость работы заключается в возможности использования разработанной модели угроз для бизнес-процесса стратегии организации ООО «Кронвел», а также применение методики обоснования оптимальной политики информационной безопасности (методом оптимального программирования).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Mandritsa I.V., Petrenko V.I., Mandritsa O.V., Solovieva I.V., Sevastianov S.A., Lazyrina E.A.«Defying of risk cybersecurity organization», сборник материалов V-ой всероссийской с международным участием научно-практической конференции «Проблемы информационной безопасности» (Симферополь – Гурзуф, 14-16 февраля 2019 г.). стр. 25–28.

2 «Технология цифрового общества блокчейн – уникальные возможности применения», сборник материалов VIII Всероссийской научно-технической конференции, (Ставрополь, 22-23 мая 2018). Том 1. стр. 173–176.

3 Mandritsa I.V., Stefano S., Mandritsa O.V., Petrenko V.I. Mechanism of economic security relatively to market agents on possible leaks of business information // Modern Economy Success. 2016. № 1. С. 19-31.

4 Бойченко О.В. Решение проблем сетевой безопасности на уровне DDoS, труды IV международная научно-практическая конференции, Симферополь-Гурзуф, 5-17 февраля 2018 г. С. 4-7.

5 Мандрица И.В., Мандрица О.В., Соловьева И.В., Петренко В.И. Метод обоснования затрат на информационную безопасность бюджетных организаций, //Вестник Северо-Кавказского федерального университета. 2017. № 1 (58). С. 67-71.

6 Мандрица И.В., Минкина Т.В., Хныкина А.Г. Математическое моделирование стратегии развития охранной организации // Вестник Северо-Кавказского федерального университета. 2017. № 6 (63). С. 97-103.

7 Richard L. Glossary of Key Information Security Terms : [англ.] // Computer Security Division, Information Technology Laboratory. — Revision 2. — Gaithersburg, MD, USA : National Institute of Standards and Technology, 2013. — 222 p.

8 Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014. — 240 p.

9 Richard B. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. – No Starch Press, 2013. – 335 p.

10 Коцыняк М.А. Киберустойчивость информационно-телекоммуникационной сети. /М.А. Коцыняк – Спб.:ПАО «Информационные телекоммуникационные технологии», 2015. – 150 с.

11 Мельников В.П. Информационная безопасность и защита информации: учебное пособие для работников вузов, обучающихся по спец. "Информационные системы и технологии". – М.: Академия, 2011. – 332 с.

12 Утечки данных: ущерб и борьба российских компаний (Электронный ресурс). — 2018. — URL: https://www.cfo-russia.ru/issledovaniya/index.php?article=39387 (дата обращения 28.05.2019).

13 Уязвимость нулевого дня (0day) (Электронный ресурс). — 2011. — URL: https://tcinet.ru/press-centre/glossary/article.php?ELEMENT_ID=5120 (дата обращения 28.05.2019).

14 Что такое «фишинг» (Электронный ресурс). — 2018. — URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/ (дата обращения 28.05.2019).

15 Основы киберугрозы, типы угроз (Электронный ресурс). — 2017. — URL: https://itsecforu.ru/2017/03/08/основы-киберугрозы-типы-угроз/(дата обращения 28.05.2019).

15 Пять главных направлений киберугроз в 2016 году (Электронный ресурс). — 2016. — URL: https://www.itweek.ru/security/article/detail.php?ID=183260 (дата обращения 28.05.2019).

16 Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) году (Электронный ресурс). — 2013. — URL: https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1 (дата обращения 28.05.2019).