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

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

Кафедра «Прикладная математика и информатика»
(наименование кафедры)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль)

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему «Разработка политики информационной безопасности для департамента финансов г.о. Тольятти»

Студент А.А. Украинский _____
(И.О. Фамилия) (личная подпись)

Научный руководитель О.М. Гущина _____
(И.О. Фамилия) (личная подпись)

Руководитель программы д.т.н., доцент, С.В. Мкртычев _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Допустить к защите
Заведующий кафедрой к.т.н., доцент, А.В. Очеповский _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____» _____20_____г.

Тольятти 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Ежедневная работа, связанная с обработкой электронных документов, а также с обработкой конфиденциальных данных подразумевает в себе множество рисков и угроз для целостности обрабатываемой информации. Ежегодно объем обрабатываемых данных растёт, следовательно, растёт и количество вероятных угроз.

Принято считать, что чем больше объемы конфиденциальной информации, которыми владеет организация, тем выше её стоимость. Следовательно, любая компрометация данных, может повлечь к существенным финансовым потерям, от которых организация может уже никогда не восстановиться.

В современном мире существует невероятное множество угроз информационной безопасности и целостности данных. Киберпреступники постоянно меняют методы и средства с помощью которых они бы могли заполучить необходимые данные.

С точки зрения киберпреступников информация - это товар и чем актуальнее, новее информация, тем выше её цена. На текущий момент, киберпреступления это уже не просто удалённые атаки на определенные ресурсы, сейчас всё чаще для киберпреступлений задействуются методы социальной инженерии.

Сами по себе методы социальной инженерии направлены на получение необходимого доступа к информации, данные методы основаны на особенности психологии человека, на которого оказывается воздействие.

Использование таких методов порождает вид угрозы, который образуется не извне, а внутри организации, так называемые «инсайд атаки». Такой вид атак опасен тем, что человек или сотрудник, нарушивший информационную безопасность, может даже и не подозревать, что совершил противоправные действия.

Чтобы избежать этого, необходимо задействовать политику информационной безопасности. Данная политика должна снизить вероятность компрометации данных либо их искажения.

Итак, политика информационной безопасности должна обеспечить максимальную защиту от возможных рисков, а именно:

- кражи информации;
- уничтожения информации;
- искажения информации.

Целью диссертационной работы является создание политики информационной безопасности с учётом угроз, исходящий от методов социальной инженерии.

Для достижения данной цели были поставлены и решены следующие **задачи:**

1) провести анализ угроз информационной безопасности характерных для организаций финансовой отрасли;

2) провести анализ текущей политики информационной безопасности, используемой в организации;

3) провести анализ IT рынка и средств, направленных на защиту информации;

4) выбрать средства, которые необходимо задействовать в разрабатываемой политике ИБ;

5) провести анализ экономической эффективности новой политики ИБ;

6) провести тестирование политики ИБ;

7) сделать вывод о пригодности для использования новой политики информационной безопасности.

Предмет исследования – степень защиты информации с помощью политики информационной безопасности.

Объект исследования политика информационной безопасности департамента финансов.

Гипотеза диссертационного исследования состоит в том, что можно повысить уровень защиты информации, если при разработке политики информационной безопасности сделать уклон на защиту от внутренних угроз и социальной инженерии.

Теоретической и методологической основой исследования являются разработки зарубежных и отечественных специалистов, осуществляющих работу по разработке и модернизации политики информационной безопасности в различных секторах бизнеса, а также материалы научных конференция, данные информационно-аналитических отчетов.

Научная новизна диссертационной работы заключается в разработке политики информационной безопасности, способной обеспечить защиту информации от угроз, исходящих изнутри организации.

Практическая значимость исследования заключается в повышении уровня защиты информации в финансовых организациях за счёт разработки политики информационной безопасности.

Основой для теоретического исследования выступили труды отечественных и зарубежных деятелей в области информационной безопасности, а также исследования лабораторий, которые занимаются защитой информации.

В процессе исследования были использованы средства и методы защиты: основные положения об информационной безопасности, анализ и сопоставление имеющихся средств для защиты данных, анализ и классификация собранных данных с последующим моделированием и проектированием политики ИБ, апробацией результатов и оценкой итогов.

Основные этапы исследования: исследование проводилось с 2017 по 2019 года в несколько этапов:

На первом этапе формулировалась тема исследования, проводился сбор информации по теме исследования из различных источников, осуществлялась формулировка гипотезы, постановка цели, задач.

Второй этап – в ходе данного этапа осуществлялся анализ методов и средств, которые задействуются в организации, а также проводился анализ средств представленных на IT рынке, осуществлялось написание и публикация научных статей по теме исследования.

Третий этап заключался в том, что осуществлялось тестирование разработанной политики информационной безопасности на тестовом стенде, осуществлялся сбор и анализ данных, полученных в результате тестирования, а также последующая оценка полученных результатов.

На защиту выносится:

- Документ- политика информационной безопасности;
- Модель политики информационной безопасности, показывающая список средств защиты;
- Результаты апробации разработанной политики информационной безопасности.

В первой главе рассматривается сущность политики информационной безопасности. Раскрывается суть, назначения, цели и принципы использования политики информационной безопасности. Производится анализ угроз, а также статистические данные из исследований компаний направленных на защиту данных. Также происходит анализ средств для защиты данных.

Во второй главе производится анализ текущей политики информационной безопасности, определяются слабые места. Производится анализ помещений, с точки зрения внутренней угрозы.

В третьей главе производится разработка политики информационной безопасности. Выбираются средства, которые необходимо задействовать для повышения уровня защиты данных.

В четвёртой главе производится тестирование политики информационной безопасности, производится экономический анализ эффективности политики информационной безопасности.

Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложений. Работа изложена на 71 страницах и включает 22 рисунка, 17 таблиц.

ГЛАВА 1 ОПРЕДЕЛЕНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В век высокого уровня развития информационных технологий, многие компании переходят на электронный документооборот. Использование электронных документов, подразумевает хранение, обработку и передачу информации, в том числе и конфиденциальной с помощью электронных средств.

Для того чтобы снизить к минимуму риск компрометации конфиденциальной информации и урегулирования вопросов касательно обеспечения безопасности данных, в организациях вводят политику информационной безопасности.

В данной работе будет рассмотрена и разработана политика информации для Департамента финансов г.о. Тольятти.

В этой главе будет дано определение политике информационной безопасности, её назначение и нюансы применения, а так же рассмотрены методы и средства которые есть на рынке ИТ индустрии, которые направлены на обеспечение безопасности информации.

Для того чтобы разработать политику информационной безопасности, следует чётко понимать, что она из себя представляет и для чего она предназначена. На сегодняшний день, единого и общепринятого определения термину «политики информационной безопасности» нет.

Исходя из этого, в рамках данной работы, будет дано приблизительное и развёрнутое определение.

Итак, прежде всего политика информационной безопасности необходима для того, определить цели и задачи информационной безопасности организации и донести их до всех, без исключения, сотрудников. Руководство организации должно чётко понимать, что основная задача специалиста по информационной безопасности это не только расследование фактов утечек данных, но и

предотвращение или максимальная минимизация рисков потери данных, следовательно, повышение стабильности работы организации.

В общепринятой форме политика информационной безопасности представляет собой документ, в котором отражены и изложены объекты защиты, ответственные лица, обязанности и инструкции по работе с информацией.

Если рассматривать отечественный стандарт ГОСТ Р ИСО/МЭК 17799-2005, в нём сказано, что в политике информационной безопасности должна быть прописана ответственность руководства, а также изложен подход к управлению информационной безопасностью. В соответствии с этим стандартом, необходимо, чтобы политика информационной безопасности включала в себя:

- основные цели и задачи по защите данных;
- ответственных лиц;
- требования к работе с информацией;
- изложение принципов, правил и требований;
- определение обязанностей сотрудников.

Для того чтобы политика информационной безопасности была исполняемой, а не «только на бумаге», можно определить основные требования к политике информационной безопасности:

- политика информационной безопасности должны быть непротиворечивой, то есть все методы обработки информации, описываемые в разных документах, должны быть единообразными и не приводить к конфликту;
- политика информационной безопасности не должна ограничивать бизнес-процессы организации, иными словами, не должна толкать сотрудника на нарушение политики информационной безопасности при выполнении своих прямых должностных обязанностей;
- политика информационной безопасности не должна предъявлять невыполнимых требований и обязанностей для простых пользователей;

- политика информационной безопасности не должна раскрывать средства, используемые для защиты данных;
- политика информационной безопасности должна быть доступна простому обывателю, иными словами, простой пользователь должен понимать, что написано в политике информационной безопасности;
- политика информационной безопасности должна быт основным документом первого уровня, а дополнять её будут уже положения и инструкции, описывающие более конкретные моменты и направленная более узкому кругу специалистов.[12]

Назначение политики информационной безопасности заключается в защите информационных активов организации и обеспечении защиты от противоправных действий злоумышленников, а также снижения рисков и уменьшение потенциального вреда от аварий и непреднамеренных действий персонала.

Как показывает практика, в последние годы произошла переориентация киберпреступлений и возросло количества случаев, а также масштабы ущерба от работы «инсайдеров». Иными словами, от действий сотрудников организации или иных лиц, которые получили доступ и намеренно или непреднамеренно совершили действие, которое привело к нанесению ущерба. [36]

При грамотно составленной политике информационной безопасности, можно исключить или максимально минимизировать вероятность нанесения ущерба даже инсайдерами, либо, в случае эксцесса, быстро вычислить канал утечки либо личность, которая рассекретила информацию.

При рассмотрении информационной безопасности выделяют три принципа:

Конфиденциальность – то есть предотвращение разглашение либо утечки секретной информации.[11]

Целостность – то есть недопущение изменения или искажения информации при выполнении обработки информации, например передачи, хранении, отображении.[11]

Доступность – то есть организация доступа к данным. Лица имеющие необходимые права доступа, должны реализовать их беспрепятственно.

Исходя из вышесказанного, можно подвести итог и сформулировать определение термину «политика информационной безопасности».[11]

Политика информационной безопасности – это комплекс превентивных мер, правил и принципов, направленных на защиту конфиденциальных данных и информационных процессов на предприятии. Политика безопасности включает в себя требования, правила для персонала, менеджеров и технических служб. В политике информационной безопасности изложены цели и задачи, которые должны достигаться и решаться во время выполнения политики ИБ. Зачастую политика ИБ формализуется и разрабатывается индивидуально под конкретную организацию, с данным документом должны быть ознакомлены все без исключения сотрудники. [4]

Сформулировав определение термину «политика информационной безопасности», следует рассмотреть для чего же нужна политика информационной безопасности в организации и какие цели с помощью неё можно достичь.

Цели политики информационной безопасности относятся к одной или нескольким из следующих категорий:

- защита ресурсов;
- аутентификация;
- авторизация;
- целостность;
- конфиденциальность;
- аудит безопасности.

Таким образом, можно сделать вывод, что политика информационной безопасности является неотъемлемым элементом любой организации. Задействование политики ИБ может существенно увеличить уровень защиты

информации, что в свою очередь влечет снижение риска финансовых и репутационных потерь.

В области информационной безопасности компании, которые занимаются разработкой ПО проводят свои исследования. Данные исследования полезны для изучения специалистам по информационной безопасности, для того чтобы спрогнозировать тип и характер угроз. Согласно отчёту портала ptsecurity в первом квартале 2019 года наиболее распространёнными средствами атаки на финансовые организации стало использование ВПО и социальная инженерия или «фишинг», именно «фишинг» направлен на задействование сотрудников организации. На рисунке 1.1 представлена диаграмма методов атак на финансовые организации.[33, 36]

Рисунок 1.1- Методы атак на финансовые организации в Q1 2019

Если учесть, что средства защиты развиваются вместе с угрозами, то можно предположить, что способы и задействованные средства при кибератаках претерпят существенные изменения. Наиболее вероятный метод, это осуществить атаку с помощью ничего не подозревающего сотрудника, например, чтобы он запустил вредоносный исполняемый файл. Такой вид атак классифицируется как «социальная инженерия», в повседневной жизни такие атаки называются «фишинг» или «инсайдерские».[36]

Как видно из диаграммы, такой вид атак почти стал вровень по популярности с ВПО. Основная опасность фишинга заключается в том, что его трудно предотвратить. Подобный вид атак, всё ещё остаётся наиболее опасным для финансовых организаций, так как реализованная угроза с помощью сотрудника, может повлечь серьёзные последствия. Защита организации изнутри всё ещё является слабым местом многих организаций.

В подтверждение слов о серьёзности внутренней угрозы. Портал anti-malware провёл исследование о характере внутренних угроз. В результате этого исследования была составлена диаграмма (рисунок 1.2).

Рисунок 1.2 -Диаграмма угроз

Для выбора способов защиты следует рассмотреть причины потери конфиденциальной информации. Для этого составлена схема, которая отображена на рисунке 1.3.[36]

Исходя из вышеописанного, при разработке политики информационной безопасности следует сделать уклон на защиту данных от угроз исходящих изнутри организации, то следует рассмотреть условия для формирования «внутренней угрозы».

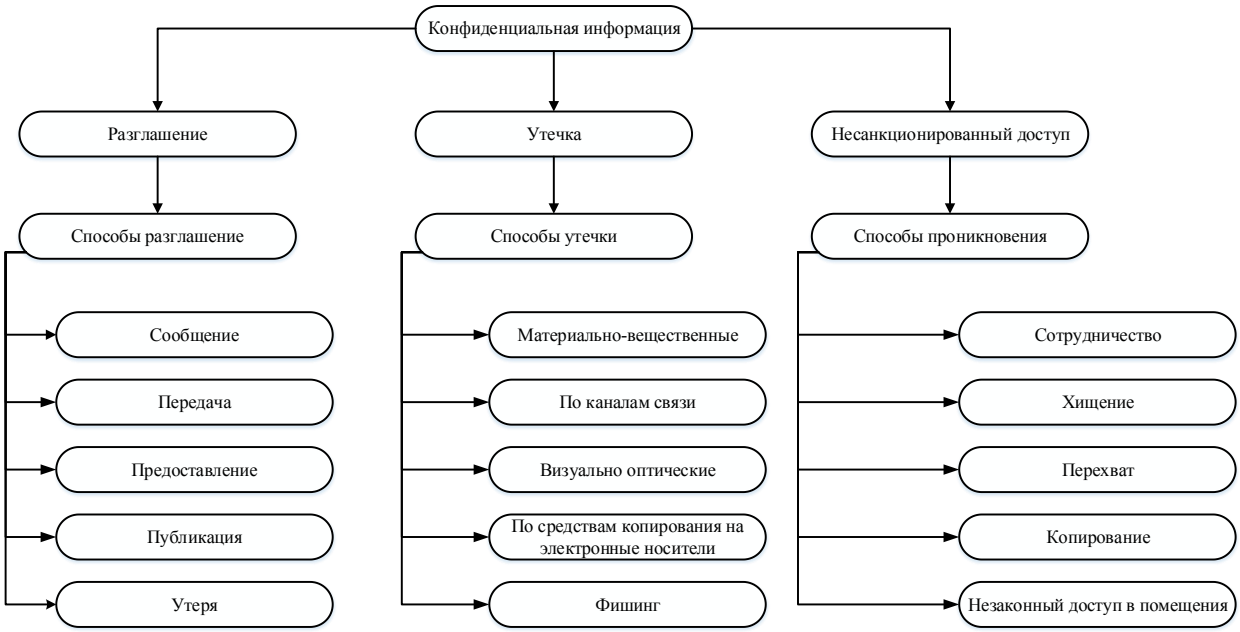

Рисунок 1.3 - Способы утери конфиденциальной информации

Такими условиями можно считать:

- подкуп ответственного лица;
- чрезмерная разговорчивость сотрудника, нарушение условий конфиденциальности в разговорах;
- недобросовестное выполнение условий политики информационной безопасности;
- низкий уровень компьютерной грамотности;
- халатное обращение с конфиденциальной информацией.

Таким образом, в первой главе было сформировано определение термина «политика информационной безопасности». Определено наиболее слабое направление в политиках информационной безопасности, на основе исследований организаций занимающейся защитой данных, этим слабым местом является – защита от внутренних угроз.[16]

ГЛАВА 2 АНАЛИЗ ТЕКУЩЕЙ ПОЛИТИКИ ИБ И ПОСТАНОВКА ЗАДАЧИ НА РАЗРАБОТКУ ПОЛИТИКИ ИБ

Во второй главе производится анализ текущего положения, связанного с обеспечением безопасности. В этой главе рассматривается как сама текущая политика информационной безопасности, журнал в который заносятся все важные отметки и средства защиты (программные и инженерные).

Целью данного анализа является выявление недостатков, уязвимостей, которые могут привести к раскрытию или компрометации конфиденциальной информации. Попутно с рассмотрением и анализом текущего положения об информационной безопасности, будут даны комментарии и пути исправления, устранения недостатков, которые могут повлечь к утечки данных.

2.1 Анализ политики информационной безопасности Департамента финансов

В первой главе были определены принципы и задачи, которые должны решаться с помощью политики информационной безопасности. Руководствуясь этими данными, следует провести анализ текущей политики информационной безопасности и постановить задачу на разработку политики информационной безопасности.

Рассмотрение текущего состояния защищенности данных необходимо использовать метод МАРИОН (MARION). Данный метод был изобретен во Франции, ассоциацией Assemblie Plinihre des Sociitis d'Assurances contre L'Incendie et les Risques Divers (APSAIRD) и затем доработан Club de la Sicuriti Informatique Frangaise (CLUSIF). Метод является стандартом де-факто по определению компьютерных рисков. Соответствует стандарту ISO-SC27-WG1. В мире насчитывается порядка тысячи планов по безопасности информационных систем, рассчитанных по методике МАРИОН. [12]

Суть методики заключается в составлении основных, базовых вопросов и ответов на них. В качестве ответа используется оценка в диапазоне от 1 до 4, где:

1 - это отрицательная оценка, то есть высокий уровень угрозы;

4 – это положительная оценка, то есть низки уровень угрозы.

Каждый критерий (вопрос) имеет свой «вес», то есть уровень важности, значимости для защиты информации, данный критерий определяется индивидуально, согласно специфике организации.

Для рассмотрения уровня безопасности выявлено 6 секция, в которых оцениваются основные факторы. Оценка происходит по следующей формуле:

Уровень защиты = Max. Ric – (S. Ric / P. Ric), где

Max. Ric – максимальный уровень риска, в качестве максимального уровня принимается значение 3. То есть градация рисков будет выглядеть следующим образом:

- Max. Ric < 1 – низкий уровень угрозы;
- 1 < Max. Ric < 2– средний уровень угрозы;
- 2 < Max. Ric < 3– высокий уровень угрозы.

S. Ric – это взвешенная сумма рисков, которая рассчитывается по формуле: оценка критерия * на его «вес».

P. Ric – это сумма «веса» оценок.

Содержание разделов представлено в таблице 2.1.

Таблица 2.1 - Содержание оцениваемых разделов

Номер	***Описание***
101	Общая безопасность: Общая организация
102	Общая безопасность: Общий контроль
103	Общая безопасность: Процедуры безопасности и аудит
201	Социо-экономические факторы: Социо-экономические факторы
301	Общая компьютерная безопасность: Окружение
302	Общая компьютерная безопасность: Контроль физического доступа

Номер	*Описание*
303	Общая компьютерная безопасность: Загрязнение
304	Общая компьютерная безопасность: Инструкции по безопасности
305	Общая компьютерная безопасность: Пожарная безопасность
306	Общая компьютерная безопасность: Безопасность от проникновения воды
307	Общая компьютерная безопасность: Правильность установки компьютеров
308	Общая компьютерная безопасность: Процедуры восстановления после аварии
309	Общая компьютерная безопасность: Связь между пользователями и персоналом ИТ
310	Общая компьютерная безопасность: Кадровая политика отдела ИТ
311	Общая компьютерная безопасность: Стратегия ИТ
401	Логический контроль доступа (вкл. телекомм.): Безопасность аппаратного и сист. ПО
402	Логический контроль доступа (вкл. телекомм.): Безопасность телекоммуникаций
403	Логический контроль доступа (вкл. телекомм.): Безопасность баз данных
501	Безопасность операций: Сохранение и восстановление данных
502	Безопасность операций: Подготовка и передача данных
503	Безопасность операций: Резервное копирование
504	Безопасность операций: Оперативные процедуры
505	Безопасность операций: Поддержка аппаратного и программного обеспечения
601	Безопасность разработки и внедрения систем: Контроль изменений
602	Безопасность разработки и внедрения систем: Процедуры разработки систем
603	Безопасность разработки и внедрения систем: Программные проверки
604	Безопасность разработки и внедрения систем: Другой контроль прикладного ПО

Далее, в таблице 2.2 привозится пример рассмотрения и оценки раздела безопасности. В качестве примера выбран раздел 304 - Общая компьютерная безопасность: Инструкции по безопасности.

Таблица 2.2 – Пример рассмотрения и оценки раздела безопасности

СЕКЦИЯ 3: Общая компьютерная безопасность **Вес:** 345,00			***Сумма баллов***	
ФАКТОР 04: Инструкции по безопасности **Вес:** 15,00			**2,90**	
Содержание вопроса	***Вес***	***Оценка***	***P. Ric***	***S. Ric***
Тема : Инструкции по безопасности				
Хорошо ли составлены инструкции по безопасности?	2,00	3,00	2,00	6
Вывешены ли инструкции по безопасности, касающиеся компьютерной безопасности от пожара, воды и т.д. в соответствующих местах и правильно ли подобрано место и тип риска?	3,00	4,00	3,00	12
Тема : Проверка знания инструкций				
Проводятся ли тестирования, проверки и тренировки знания и понимания инструкций сотрудниками?	2,00	1,00	2,00	2
Производятся ли тренировки регулярно (не реже трех раз в год) и неожиданно?	2,00	3,00	2,00	6
Записываются ли результаты тренировок?	1,00	3,00	1,00	3
Итого:	***10,00***	***14,00***	***10,00***	***29,00***

Итак, на таблице 2.2 представлены вопросы, ответив на которые, производится оценка рисков по выбранному разделу. Как видно сумма набранных баллов равна 2.9, что является высоким показателем защищенности. Все вопросы и оцениваемые разделы представлены в приложении А.

С результатами оценки всех разделов сформирована таблица 2.3, показывающая результат оценки каждого раздела.

Таблица 2.3 - Результаты оценки разделов

Номер	Наименование	Сумма баллов	Уровень риска
101	Общая безопасность: Общая организация	1,57	1,43
102	Общая безопасность: Общий контроль	2,06	0,94
103	Общая безопасность: Процедуры безопасности и аудит	2,62	0,38
201	Социоэкономические факторы: Социоэкономические факторы	2,70	0,30
301	Общая компьютерная безопасность: Окружение	2,56	0,44
302	Общая компьютерная безопасность: Контроль физического доступа	0,96	2,04
303	Общая компьютерная безопасность: Загрязнение	2,80	0,20
304	Общая компьютерная безопасность: Инструкции по безопасности	2,90	0,10
305	Общая компьютерная безопасность: Пожарная безопасность	2,93	0,08
306	Общая компьютерная безопасность: Безопасность от проникновения воды	2,90	0,10
307	Общая компьютерная безопасность: Правильность установки компьютеров	2,91	0,09
308	Общая компьютерная безопасность: Процедуры восстановления после аварии	3,00	0,00
309	Общая компьютерная безопасность: Связь между пользователями и персоналом ИТ	1,97	1,03
310	Общая компьютерная безопасность: Кадровая политика отдела ИТ	1,30	1,70
311	Общая компьютерная безопасность: Стратегия ИТ	1,00	2,00

Продолжение таблицы 2.3 - Результаты оценки разделов

401	Логический контроль доступа (вкл. телекомм.): Безопасность аппаратного и сист. ПО	1,26	1,74
402	Логический контроль доступа (вкл. телекомм.): Безопасность телекоммуникаций	1,06	1,94
403	Логический контроль доступа (вкл. телекомм.): Безопасность баз данных	0,96	2,04
501	Безопасность операций: Сохранение и восстановление данных	1,00	2,00
502	Безопасность операций: Подготовка и передача данных	1,00	2,00
503	Безопасность операций: Резервное копирование	1,00	2,00
504	Безопасность операций: Оперативные процедуры	1,00	2,00
505	Безопасность операций: Поддержка аппаратного и программного обеспечения	1,20	1,80
601	Безопасность разработки и внедрения систем: Контроль изменений	0,90	2,10
602	Безопасность разработки и внедрения систем: Процедуры разработки систем	0,98	2,02

В результате проведения оценки были сформированы радарная диаграмма график и, которые наглядно показывают уровень защищенности того или оного раздела относительно друг друга. Построение данных моделей поможет выявить наиболее слабые разделы в текущей политике информационной безопасности.

На рисунке 2.1 представлена радарная диаграмма рисков.

Построение радарной диаграммы позволит наглядно определить те области, в которых необходима модернизация и повышение уровня информационной безопасности. Суть данной диаграммы заключается в том, что проверяемый критерий должен занимать как можно большую площадь на диаграмме.

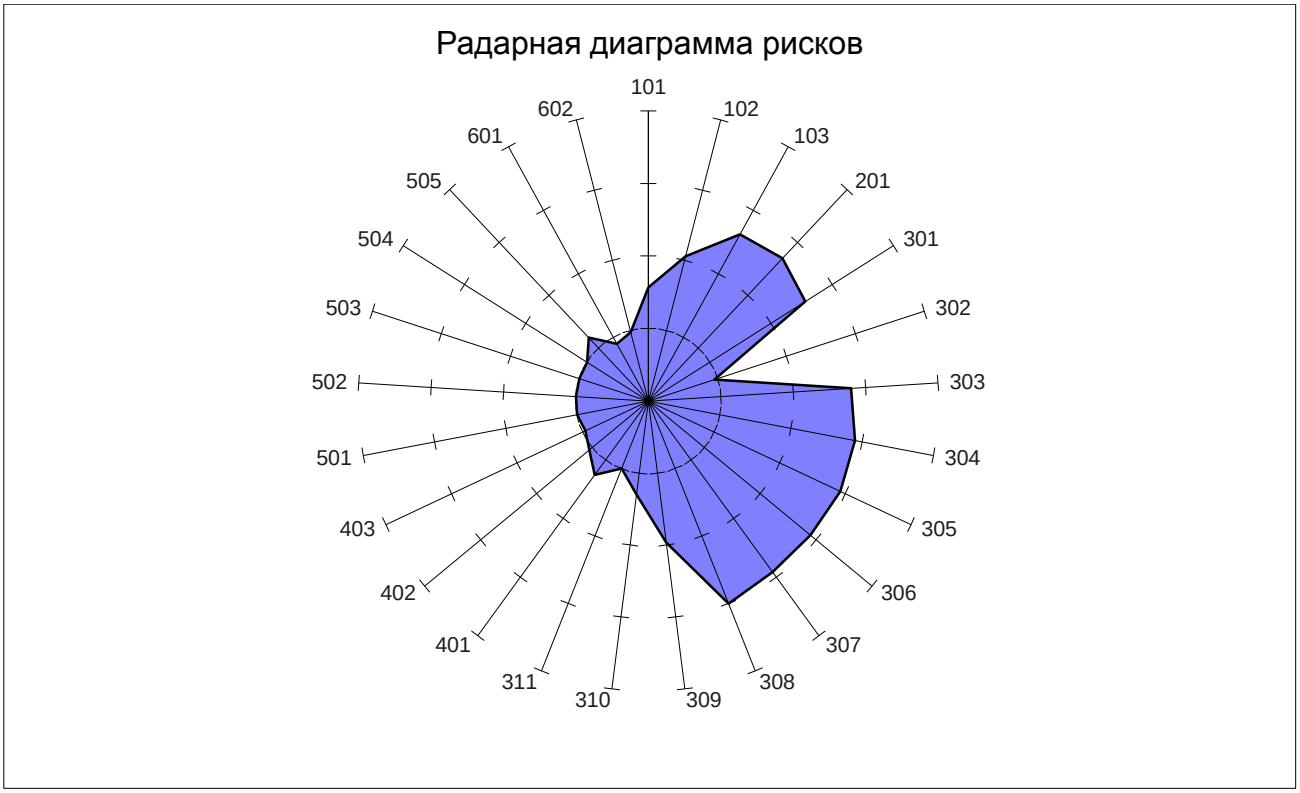

Рисунок 2.1 – Радарная диаграмма рисков

В добавок к радарной диаграмме сформирован график оценки уровня угроз, на котором наглядно показан уровень угрозы каждого раздела относительно друг друга. Данный график представлен на рисунке 2.2.

Построив диаграмму и график, необходимо перейти к анализу полученных данных.

Наибольший уровень угрозы наблюдается при рассмотрении секций: 302, 309, 310, 311,401, 402, 403, 501, 502, 503, 504, 505, 601, 602, 603. Именно этих областей нужно провести для выявления критериев, которые необходимо улучшить.

Анализируя полученные результаты, можно сделать следующий вывод: в целом уровень защиты департамента финансов при текущей политике информационной безопасности ниже среднего, то есть имеется реальная угроза конфиденциальности данных. Следует рассмотреть слабые места более подробно.

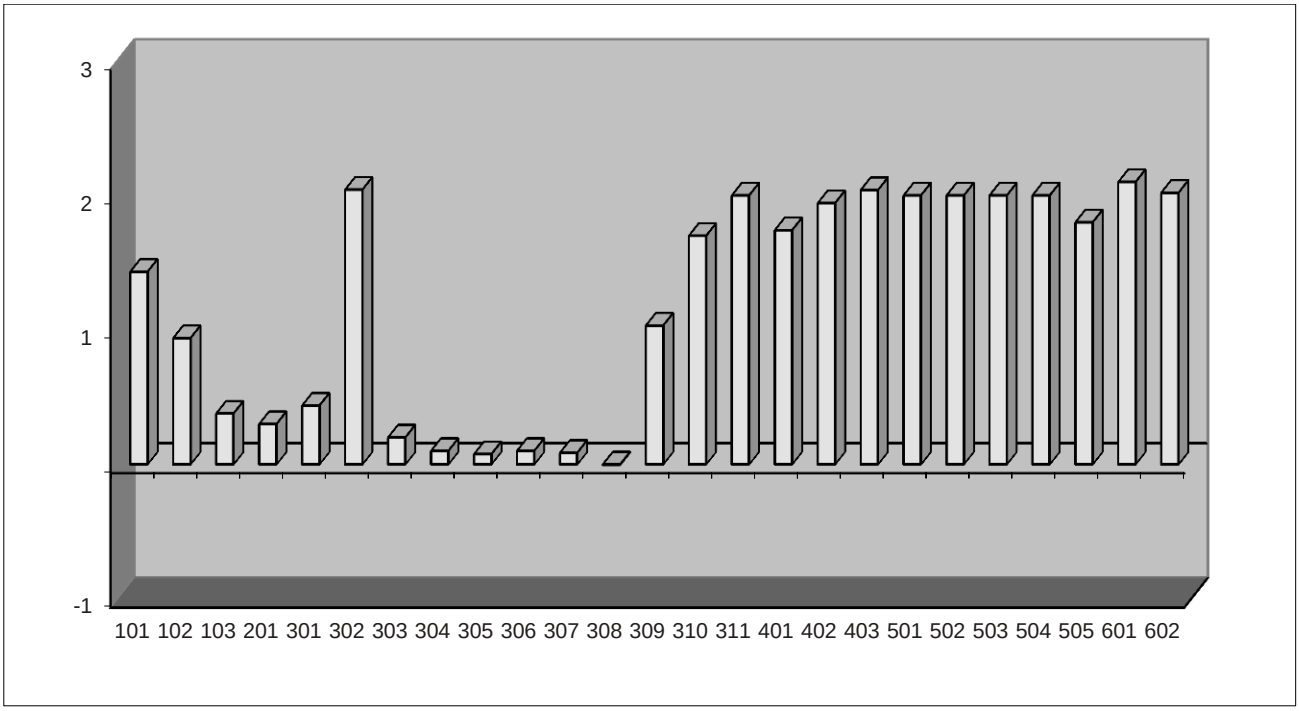

Рисунок 2.2 – График оценки угроз

Секция 302 - необходимо наладить контроль физического доступа в здание, компьютерные помещения и смежные с ними помещения, необходимо внедрить электронную пропускную систему взамен используемых бумажных пропусков.

Секция 309 – необходимо наладить взаимодействие между ИТ отделом и рядовыми пользователями. Прописать и задокументировать степень ответственности сторон.

Секция 310 – необходимо осуществлять тестирование, собеседование кандидата на трудоустройство с целью выявления у него предрасположенностей либо намерений для нарушения политики информационной безопасности.

Секция 311 - необходимо обновлять каждый год стратегию защиты информации, которая бы включала количественную оценку рисков, определение нетерпимых рисков, имеющиеся и планируемые меры безопасности, установку приоритетов, бюджет безопасности, список рекомендаций для информационного центра и для микрокомпьютеров.

Секция 401 – необходимо задействовать систему аутентификации пользователей, задействовать биометрическую или двухфакторную аутентификацию пользователей. Организовать работу с данными пользователя для входа в системы. Организовать шифрование конфиденциальных данных. Организовать контроль за учётными записями пользователей.

Секция 402 - необходимо обеспечить безопасность линий связи. Сюда относиться наблюдение за линиями и ключевыми передачами данных, защита передачи ключевых данных с помощью известных сертифицированных алгоритмов, а также использование сертифицированного оборудования, например оборудование, имеющее сертификат ФСТЭК. Разработать удовлетворительную процедуру распределения ключей.

Секция 403 – необходимо обеспечить как минимум частичное шифрование данных, ключевых файлов. Обеспечить разделение прав доступа к данным, чтобы исключить нарушение целостности данных и несанкционированный доступ к данным.

Секция 501 - необходимо осуществлять защиту хранилищ. Изолировать их от компьютерных помещений физически и защитить от случайных рисков. Защитить их системой контроля доступа, и, в нерабочее время, системой контроля вторжения.

Секция 502 – необходимо обеспечить процесс подготовки данных в организации, а именно осуществлять контроль информации. При передаче носителей данных использовать специализированные организации или курьерскую службу.

Секция 503 – необходимо обеспечить сохранение и восстановление данных. Сюда относиться обеспечение безопасности операции резервного копирования. В том числе особое внимание стоит обратить на регулярность резервного копирования чрезвычайной важности для ключевых программ и файлов.

Секция 504 – необходимо обеспечить каждый ПК средствами антивирусной защиты, а также ПК, работающие с важными данными средствами криптографии.

Секция 505 – необходимо заключить договор с организацией, которая может обеспечить поставку и ремонт оборудования в кротчайшие сроки.

Секция 601 – необходимо рамках тестирования необходимо поставлять данные для тестирования пользователями. В рамках процедуры приемки и контроля изменений необходимо разработать формальные процедуры контроля изменений (приемки), которые всегда применяются перед внедрением программ в эксплуатацию, для каждой новой системы или изменении, а также использовать комплекс тестирования.

Секция 602 - в рамках системной документации необходимо разработать структурированную, ясную документацию для приложений, программ и данных, которая регулярно обновляется и соответствует используемой методологии, и хранится ли резервная копия в безопасном месте.

Проанализировав текущую политику информационной безопасности, необходимо рассмотреть и проанализировать задействованное ПО в Департаменте финансов. Этот анализ необходим для рассмотрения возможной уязвимости в используемом ПО. Для начала в таблице 2.4 приведён перечень используемых программ в департаменте финансов г.о. Тольятти.

Таблица 2.4 - Список программ используемых в ДФ

№ПО	Название ПО
1	СУФД
2	СМЭВ
3	СЭД Дело
4	АЦК «Финансы», АЦК «Планирование
5	САУМИ
6	Картотека судебных дел
7	WEB-Консолидация

Стоит отметить, что список из таблицы 2.4 не включает в себя стандартный набор MS Office.

Всех ПК в департаменте финансов работают на Windows 7 x32 или x64. Программный комплекс СУФД подразумевает передачу электронных документов, в том числе и конфиденциальной информации. В связи с этим, передача данных осуществляется через защищенный канал связи по типу VPN. Аутентификация в защищенном канале связи происходит с помощью электронного сертификата. Помимо СУФД работа с электронными сертификатами происходит в системах АЦК «Финансы» и АЦК «Планирование», а также СЭД Дело.

Аутентификация в системах с помощью электронного сертификата происходит с помощью PIN-кода.

На каждом ПК в обязательном порядке установлено антивирусное ПО, но защищенный канал связи установлен лишь на 6 ПК, это ПК тех сотрудников, на которых организована передача данных в ЦБ РФ. Стоит отметить, что данный канал связи находится на обслуживании у ЦБ РФ и не влияет на общий уровень защиты информации в ДФ.

Таблица 2.5- Сравнение ПО используемое в ДФ

Наименование ПО	**Защита паролем**	**Использование эл.сертификата**	**WEB-интерфейс**	**Наличие защищенного канала связи**	**Обработка конфиденциальных/персональных данных**	**Критичность нарушения работы ПО для организации**
СУФД	+	+	+	+	+	+
СМЭВ	+	-	+	-	+	-
СЭД Дело	+	+	+-	-	-	-
АЦК «Финансы», АЦК «Планирова	+	+	+-	-	+	+

Наименование ПО	**Защита паролем**	**Использование эл.сертификата**	**WEB-интерфейс**	**Наличие защищенного канала связи**	**Обработка конфиденциальных/персональных данных**	**Критичность нарушения работы ПО для организации**
ние						
САУМИ	+	-	-	-	-	+
Картотека судебных дел	+	-	-	-	-	+
WEB-Консолидация	+	+	+	-	-	-

Как видно из таблицы выше у 5 из 8 программных продуктов стоит высокая важность для работы организации. То есть в случае нарушения или прекращения работы одного из этих программных продуктов, может существенно, если не полностью нарушить работу организации. [37]

Защищенный канал связи задействует лишь один программный продукт. Это обусловлено требованиями ЦБ РФ. Обслуживание канала связи ведётся сторонней организацией.

Задействование интерфейса обуславливается различными рисками кражи информации. Символами +- обозначается тот программный продукт, который поддерживает как работу в тонком клиенте (WEB-интерфейс), так и в толстом клиенте в виде устанавливаемого дистрибутива.

С электронными сертификатами взаимодействуют те программные продукты, которые подразумевают работу с электронными документами. Аутентификация по сертификату однофазная, то есть по паролю (PIN-коду).

Учитывая совокупность рассмотренных аспектов текущего состояния политики информационной безопасности, выявленных недочётах. Можно сделать

вывод, что на текущий момент в ДФ существует уязвимость в виде внутренних угроз и текущей политике информационной безопасности необходима модернизация.

Таким образом, необходимо сформулировать задачу на разработку политики информационной безопасности.

2.2 Постановка задачи на разработку политики информационной безопасности для департамента финансов

Ежедневная обработка информации, в том числе и конфиденциальной, сопряжена с определёнными рисками. Ежегодно уровень угрозы информации возрастает, злоумышленники постоянно меняют способы по краже, искажению или уничтожению информации.

Рассмотрим процесс работы с информацией на примере процесса создания бюджета на очередной финансовый год (рисунок 2.3). Для описания процесса формирования бюджета на очередной финансовый год была задействована методология BPMN.

Как видно из диаграммы на рисунке 2.3 во время повседневной работы внутри организации происходит обмен данными. В результате анализа текущей политики информационной безопасности и выявленных уязвимостей, можно сделать заключение, что процесс обмена данными внутри организации небезопасен.

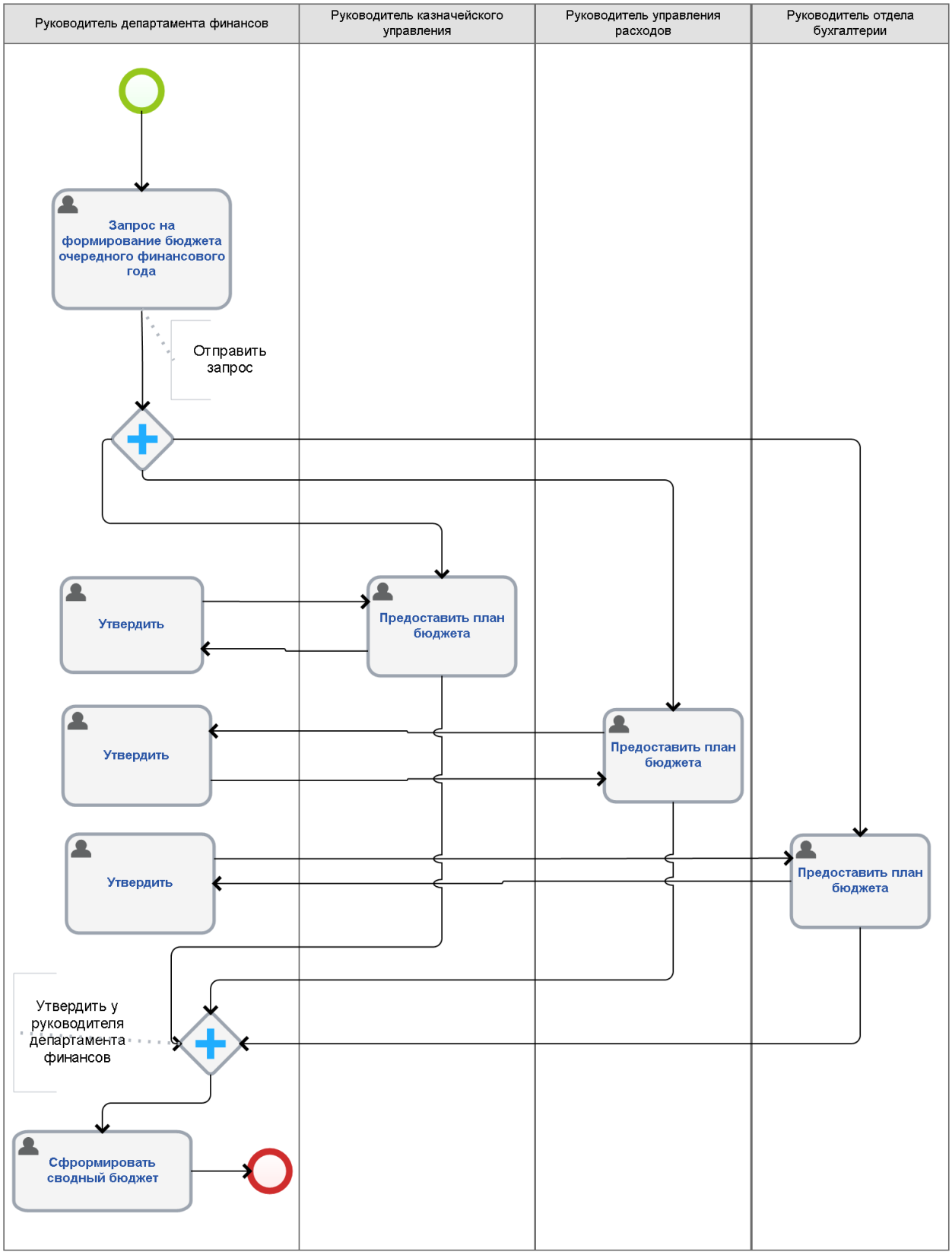

Рисунок 2.3 – Процесс формирования бюджета на очередной финансовый год

Для анализа процесса обмена данными построена диаграмма BPMN, изображённая на рисунке 2.4.

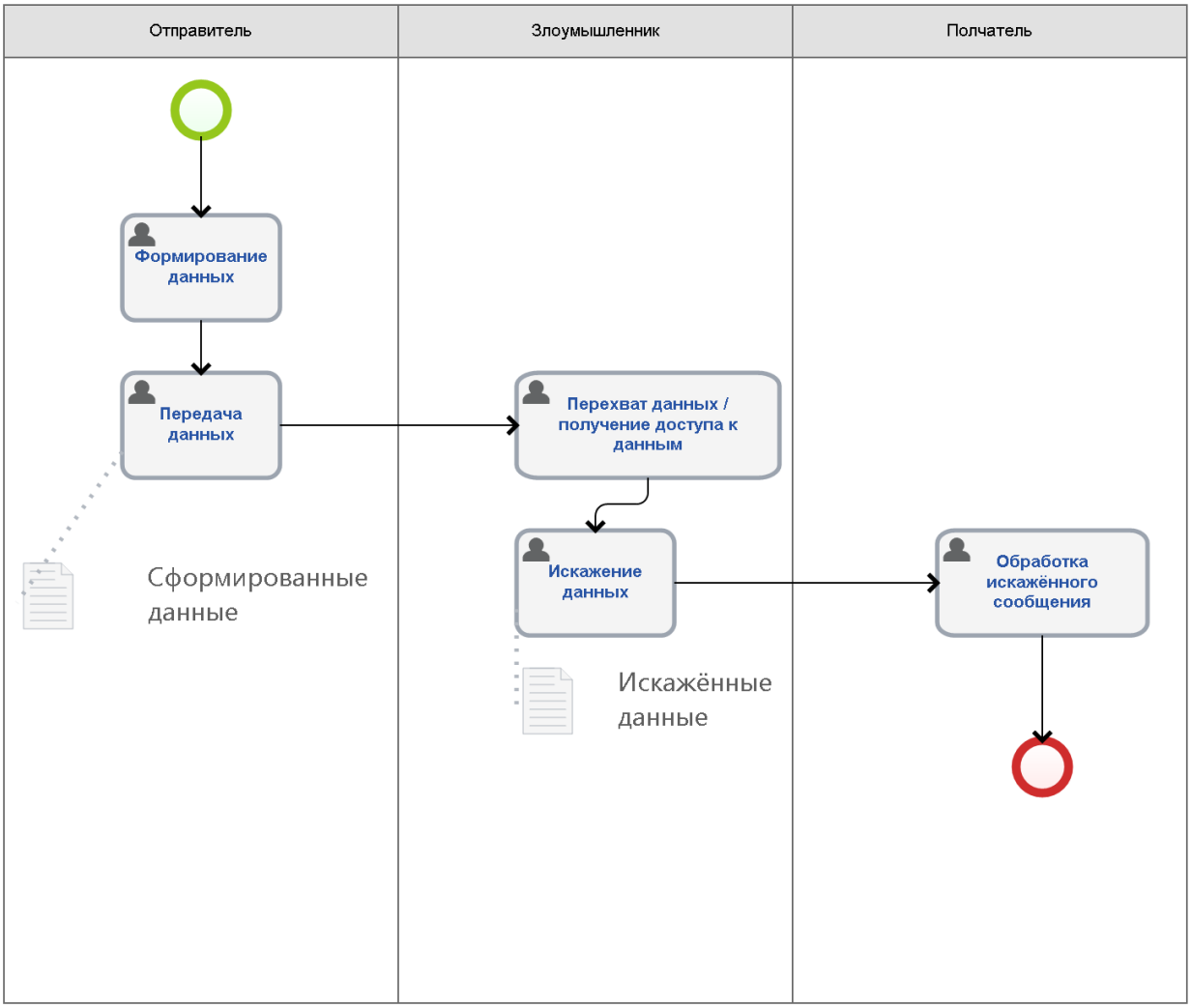

Рисунок 2.4 – Процесс обмена данными внутри организации

Как видно из представленной диаграммы обмена данными внутри организации, перехват и искажение данных вполне возможны, если не происходит использование средств шифрования данных.

В результате анализа можно сделать заключение, что с каждым годом число внешних атак снижается, уступая методам социальной инженерии или «фишингу». Такой вид угроз по своей сути формируется внутри организации, что

делает задачу по обнаружению такой угрозы и борьбе с ней сложно выполнимой. Предотвратить свершение такого инцидента невероятно трудно.

Анализ текущей защищенности показал, что внутренняя защита организации нуждается в модернизации, следовательно, появляется необходимость в разработке политики информационной безопасности, которая могла бы снизить риски и повысить уровень защиты информации от внутренних угроз.

Основные функции, которые должны быть реализованы с помощью политики информационной безопасности:

- разграничение доступа в помещения с повышенным уровнем защиты;
- организация защиты ПК;
- предотвращение несанкционированного доступа к ПК и данным обрабатываем в ДФ;
- организация защиты от проникновения извне.

В разрабатываемой политике информационной безопасности данные функции будут реализованы надлежащим программным обеспечением. Реализация функций необходимых для обеспечения защиты информации от внутренней угрозы выполняется с помощью совокупности программных средств, а также программно-аппаратных средств.

Резюмируя, во второй главе рассмотрена и проанализирована текущая политика информационной безопасности, выявлены уязвимости. Осуществлена постановка задачи на разработку политики информационной безопасности.

ГЛАВА 3 ПРОЕКТИРОВАНИЕ ПОЛИТИКИ ИНФОМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрев текущее положение политики информационной безопасности, следует перейти непосредственно к проектированию политики информационной безопасности.

Разрабатываемая политика информационной безопасности должна распространяться на всех сотрудников организации, соответственно весь персонал организации в обязательном порядке должен быть ознакомлен с данной политикой. Ответственное лицо за информационную безопасность должен вести журнал учёта ознакомления с политикой информационной безопасности.

Ответственность за исполнение политики информационной безопасности несет не только специалист по информационной безопасности, но и руководитель организации вместе с руководителями отделов и их подчинёнными. Каждый сотрудник обязан исполнять требования политики информационной безопасности как часть своих прямых должностных обязанностей.

Для наглядности следует построить диаграмму причины-следствия для политики информационной безопасности. Эта диаграмма создаётся с учётом недочётов, выявленных в результате анализа, проведённого во второй главе.

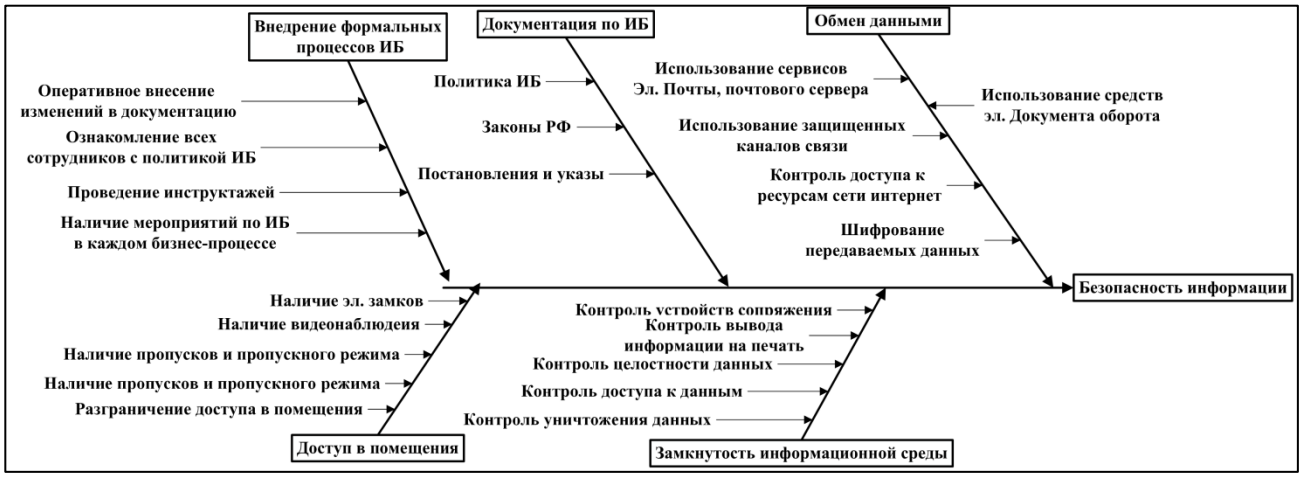

Рисунок 3.1 - Диаграмма причины-следствия разрабатываемой политики информационной безопасности

Из данной диаграммы видно, что необходимо определить какие средства могут обеспечить критериям безопасности информации. Для этого следует определить, какие программно-аппаратные средства следует задействовать для защиты данных. [18]

3.1 Перечень задействованных средств защиты информации

В разрабатываемой политике информационной безопасности приводится перечень программно-аппаратных средств направленных на защиту данных.

Для начала следует дать определение понятию «программно-аппаратный» комплекс. Программно-аппаратный комплекс – это совокупность технических и программных средств.

В качестве аппаратных средств можно могут быть:

- устройства идентификации сотрудника;
- устройства шифрования информации;
- электронные замки и блокираторы.

А в качестве программного комплекса может выступить ПО, которое поможет обеспечить защиту данных и разграничить доступ к ним можно рассмотреть такие программы как:

- программы для аутентификации пользователей (можно использовать штатные средства, если такое предусмотрено ПО);
- программы для разграничения доступа к информации;
- программы криптографической защиты;
- программы для предотвращения вирусного заражения;
- программы для обнаружения незаконного вторжения или доступа к информации.

Первоначальным фактором, который требует модернизации, является обновление операционной системы. Так как компания Microsoft объявила об

остановке сопровождения ОС Windows 7, на которой на данный момент осуществляется работа, необходимо осуществить обновление ОС до Windows 10.

Стоит отметить, что для такой организации, как Департамент финансов необходимо использовать ПО, разработанное на территории Российской Федерации. То есть при выборе средств защиты информации необходимо обратить внимание на то, имеет ли то или иное средство защиты данных сертификат ФСТЭК.

Основываясь на проведённом анализе во второй главе, необходимо выбрать средства защиты. При более детальном рассмотрении недочётов можно заметить, что секции 302, 401, 501 являются взаимосвязанными, а именно отвечают за доступ к данным, доступ в помещения и аутентификации данных.

Итак, одной из главных проблем, которая была выявлена в результате анализа, проведённого во второй главе, является разграничение прав доступа к данным. Изначально, для работы в локальной сети следует провести разграничение доступа к данным, подобный способ защиты, может быть реализован с помощью деления пользователей на группы и наделить группы следующими правами:

1. Administrator – администраторы сети, могут создавать и изменять политики информационной безопасности, осуществлять настройку сети и оборудования, но имеют ограничения по доступу к данным. Ограничение доступа организовано, для избегания утечек данных.
2. Root – учетная запись, доступ к которой имеет ограниченный круг лиц, данная запись наделена всеми правами и не имеет ограничений.
3. User – учетная запись простого пользователя, имеет ряд ограничений (запрет на установку ПО, ограничение доступа к ресурсам и данным).
4. Guest – учетная запись для гостевых пользователей, имеет сильное ограничение в права (данная запись используется для доступа сотрудников сторонних организаций).

В таблице 3.1, ниже, приведен перечень прав групп пользователей.

Таблица 3.1 - Перечень прав групп пользователей

Действия	Administrator	Root	User	Guest
Создание и блокировка пользователей	+	+	-	-
Создание и редактирование групп пользователей	+	+	-	-
Настройка сети	+	+	-	-
Организация подключения ПК к сети	+	+	-	-
Изменение настроек серверов	-	+	-	-
Настройка прав доступа к каталогам и резервным копиям	+	+	-	-
Возможность скачивать файлы из сети интернет	+	+	+	-
Установка ПО	+	+	-	-
Запись данных	+	+	-	-
Хранение данных	+	+	+	-
Подключение внешних носителей информации	+	+	+	-
Подключение CD/DVD-ROM	+	+	-	-
Доступ к FTP	+	+	+	-
Доступ к POP3	+	+	+	-
Доступ к SMTP	+	+	+	-
Доступ к SSL	+	+	-	-
Доступ к SOCKS	+	+	-	-

В случае если необходимо изменить права для пользователя, администратор вправе изменить или создать новые права доступа.

Для организации доступа в здание необходимо заменить бумажные пропуска на электронные. Такая мера позволит идентифицировать сотрудника при входе в здание. Введение электронных пропусков позволит:

- отследить время прибытия и убытия сотрудников;

- ограничить доступ уволенным, отстранённым или прибывающим в отпуске сотрудникам;
- идентифицировать человека, прошедшего в здание.

Информация, которую должен содержать пропуск заключается в следующем:

- ФИО;
- фото сотрудника;
- принадлежность к департаменту/отделу/управлению;
- кабинет, в котором работает сотрудник;
- время прибытия;
- время убытия.

Про должная говорить о разграничении доступа, следует отметить необходимость установки электронного кодового замка. Данная мера должна применяться к тем помещениям, в которых производится обработка конфиденциальной информации или осуществляется хранение данных, например такая мера может примениться к помещениям серверной.

Помимо кодовых замков к методам аутентификации и разграничения доступа можно добавить двухфакторную аутентификацию. Например, двухфакторную аутентификацию от компании РУТОКЕН. В двухфакторной аутентификации, первым фактором является некоторая вещь, которой обладает пользователь, а вторым — то, что пользователь знает. отличается своей надёжностью. Во-первых, невозможностью изготовить дубликат предмета, которым должен обладать человек.

Очень хорошо на роль такого уникального предмета подходят смарт-карты и USB-токены, которые могут генерировать не извлекаемые криптографические ключи. Однажды сгенерированный, такой ключ используется внутри чипа смарт-карты или токена, не покидая его. Поскольку извлечь такой ключ нельзя, то и изготовить дубликат смарт-карты не представляется возможным.

Второй фактор — фактор знания должен быть неразрывно связан с предметом. Для смарт-карт таким фактором является PIN-код. [37]

В качестве средства двухфакторной аутентификации часто позиционируются аппаратные генераторы одноразовых паролей или OTP-токены. Существует множество реализаций аппаратных генераторов одноразовых паролей. Очевидно, что каждое устройство содержит уникальный код, и это удовлетворяет критерию первого фактора аутентификации. Однако для считывания одноразового пароля, как правило, не применяется PIN-код. Это означает, что условие связанности первого и второго факторов не выполняется и аутентификация, реализованная при помощи таких устройств, не является в полном смысле двухфакторной. Исключение составляют устройства, которые позволяют считывать одноразовые пароли после ввода PIN-кода, но они довольно редки.

В качестве второго фактора аутентификации может использоваться и биометрия. Например, «Match-On-Card» и ей подобные технологии позволяют заменить ввод PIN-кода анализом отпечатка пальца, что добавляет удобства использования, поскольку не нужно запоминать и вводить PIN-код.

Таким образом, можно сказать, что широко применяются следующие виды аутентификации:

- однофакторная аутентификация. Чаще всего по логину/паролю, которые могут вводиться как вручную, так и при помощи аппаратных или программных менеджеров паролей;
- двухфакторная аутентификация;
- двухэтапная верификация (two-step verification), когда к однофакторной аутентификации по логину/паролю добавляется дополнительный фактор в виде, например, одноразового пароля;

- аутентификация по альтернативному каналу (out-of-band), которая похожа на двухэтапную верификацию, но с тем отличием, что верификация производится по другому каналу связи.

«Честная» двухфакторная аутентификация основана, как правило, на применении аппаратных устройств, реализующих функции асимметричной криптографии. Первым фактором аутентификации в этом случае представляется само аппаратное устройство, содержащее приватный ключ пользователя. Приватный ключ должен быть неизвлекаемым, для того чтобы исключить возможность создания дубликата. Вторым фактором будет PIN-код, знание которого дает пользователю возможность воспользоваться устройством. Очень важна взаимосвязь PIN-кода и устройства — одним без другого воспользоваться нельзя.

На самих ПК, на которых происходит обработка конфиденциальной информации, помимо парольной аутентификации пользователей, необходимо установить электронный замок, разблокировка которого происходит с помощью ключа, например электронно-цифровой подписи. С помощью электронного замка происходит не только разблокировка ключом, но и происходит проверка аппаратной части. Проверка определяет был ли изменён или заменён хоть один из элементов ПК. При неудачной проверке произойдёт блокировка доступа. Данная мера безопасности рассчитана, на предотвращение физического вмешательства в работу ПК, например кражу носителя информации.

На рисунке 3.2 Представлен пример входа в систему с помощью электронного замка «СОБОЛЬ». [37]

Задействовав средства, описанные выше, решаются проблемы уязвимостей, выявленные в результате рассмотрения секций 302, 401, 501.

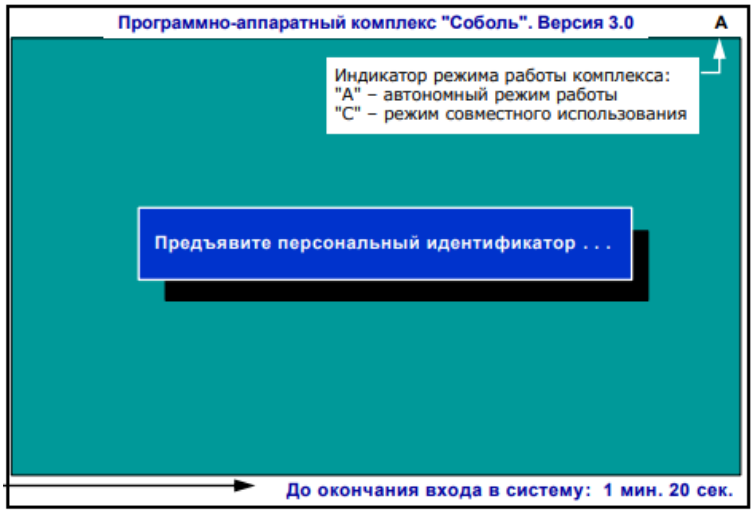

Рисунок 3.2 – Пример входа в систему с помощью ПАК «Соболь»

Далее необходимо перейти к устранению уязвимости секции 402, а именно обеспечение защиты канала связи. Для устранения данной уязвимости необходимо задействовать АПКШ «Континет-АП». Данный комплекс предназначен для криптографической защиты данных, передаваемых по открытым каналам связи, в соответствии с ГОСТ 28147-89.

Другим важным фактором является защита от проникновения в сеть. Обеспечить защиту от проникновения в сеть довольно сложная задача и для начала, необходимо иметь хотя бы возможность отследить проникновение в сеть. Комплекс «Континент-АП» способен обеспечить защиту от проникновения со стороны сетей общего доступа. В режиме обнаружения атак комплекс способен обнаруживать сетевые атаки сигнатурными и эвристическими методами, информировать администратора в режиме реального времени об обнаруженных атаках через программу управления центр управления системой (ПУ ЦУС), а также по электронной почте и строить графические отчетов о работе комплекса и выявленных атаках в ПУ ЦУС. Так же стоит отметить, что АПКШ «Континет-АП» имеет сертификат ФСТЭК РФ, что удовлетворяет критерию при выборе средств защиты для Департамента финансов.[37]

Далее следует перейти к устранению уязвимости в секции 403, а именно обеспечить шифрование данных, ключевых файлов. Хранение конфиденциальных данных на ПК осуществляется в зашифрованном виде по крипто алгоритму ГОСТ 28147-89. На рисунке 3.3 показана схема работы ГОСТ 28147-89 в режиме гаммирования.[21]

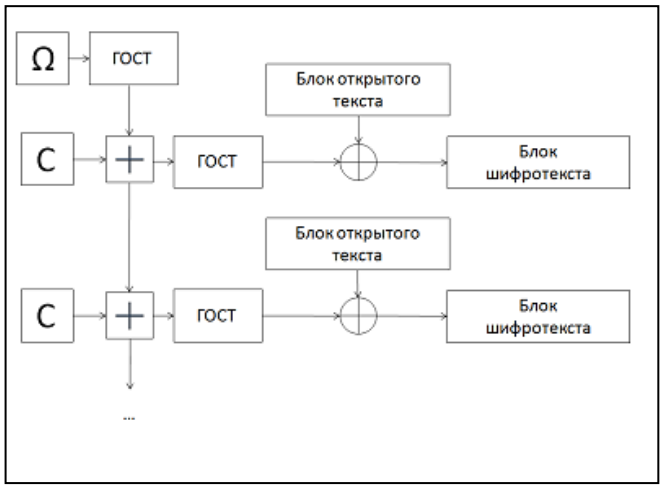

Рисунок 3.3 – Схема работы в режиме гаммирования

Шифрование файлов для хранения на ПК сотрудника, можно осуществить с помощью КРИПТО АРМ. КриптоАРМ - это программа, предназначенная для шифрования и электронного подписания файлов. Данная программа, позволит существенно увеличить уровень защиты корпоративной информации. Такую информацию можно передавать через интернет, электронную почту или на съемных носителях.

Во время шифрования, можно выбрать как сертификаты (рисунок 3.5), которыми можно расшифровать, так и алгоритм, которым будут шифроваться. Пример выбора окна получателя.

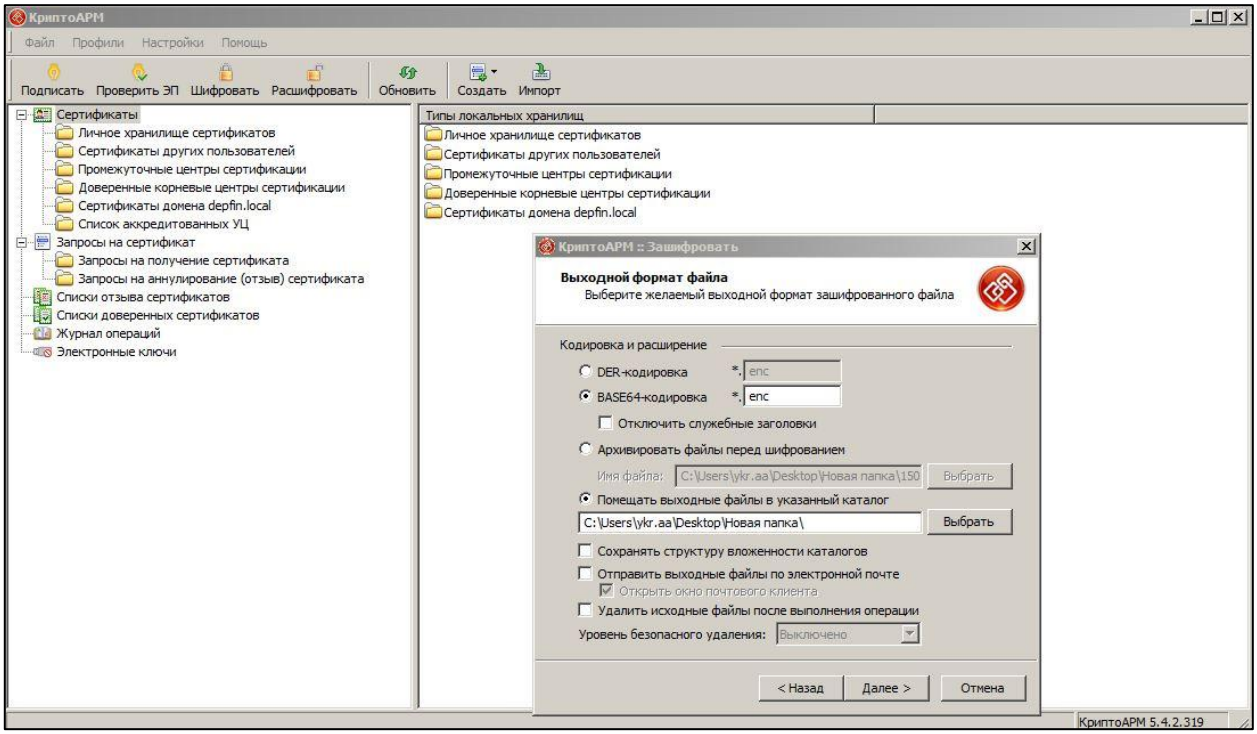

Рисунок 3.4 – Окно шифрования КриптоАРМ

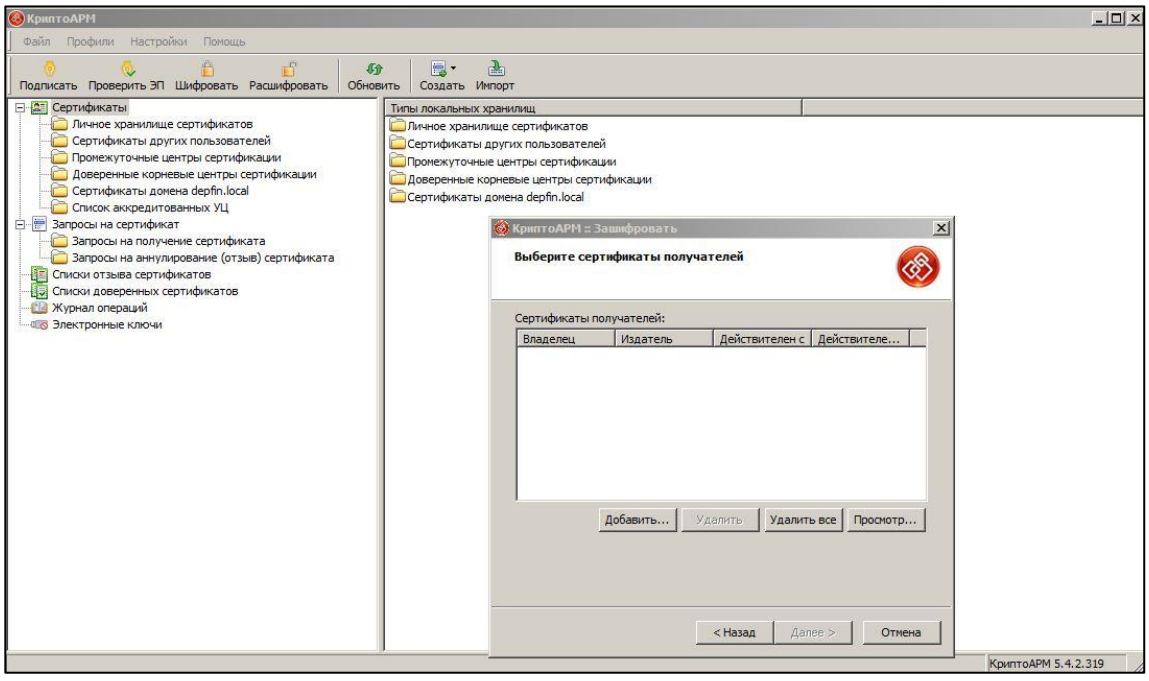

Рисунок 3.5 – Окно выбора получателей КриптоАРМ

Если защиту от внешнего проникновения можно решить установкой и настройкой специальных ПАКов, то предотвратить и отследить действия инсайдера из-за большого количества возможностей и методов, гораздо сложнее. Для обнаружения источника можно включить логирование, эта мера не предотвратит утерю информации, например при физическом скачивании информации на носитель информации.

Эта мера может позволить обнаружить какой пользователь какие действия совершал, что в свою очередь может помочь в обнаружении источника утечки данных или виновника компрометации данных.

Так как ПК с особо важной информацией являются основной целью преступных элементов, то для расследования инцидентов связанных с утечками на таких ПК должно осуществляться теневое копирование данных, подобное решение можно реализовать штатными средствами операционной системы и с помощью данного решения устраняется уязвимость, выявленную в секции 503.

Базовым средством для защиты ПК является использование антивируса, рынок ИТ предложения на данный момент времени обладает массой предложений антивирусных средств защиты. Чтобы выбрать антивирусное ПО необходимо осуществить анализ.

Для анализа были взяты 7 антивирусов. В основу данного сравнения было взято исследование порталов anti-malware.ru и softcatalog.info, а также использовались данные с официальных сайтов разработчиков ПО, которое было проведено в 2018 году. Исследование проводилось на платформе Microsoft Windows 7 x64.

Для исследования было отобрано 9 концептуальных с технологической точки зрения образцов вирусов, которые замечены в общем потоке вредоносных программ.

Таблица 3.2 – Сравнение антивирусов, проверка обнаружения вирусов

Вирус	Антивирусы						
	McAfee Internet Security	Norton Security	Panda Internet Security	Microsoft Security Essentials	Avast! Internet Security	Kaspersky Internet Security	Dr. Web Security Space Pro
APT	-	+	+	+	+	+	+
Cidox	-	-	-	-	+	+	+
Powelix	-	+	-	+	-	+	-
Backboot	-	-	-	-	+	+	+
WMIGhost	-	-	-	-	-	+	-
Stoned	+	+	-	+	+	+	+
Pihar	-	-	-	-	-	+	+
SST	-	-	-	-	+	+	+
Zeroaccess	-	+	-	+	+	+	+
Итог	1/9	4/9	1/9	4/9	6/9	9/9	7/9

В таблице 3.2 знаком (+) означает, что антивирус успешно устранил вредоносное ПО и при это сохранил работоспособность системы. Знак (-) означает, что антивирус не смог устранить вредоносное ПО или работоспособность системы была частично или полностью нарушена. [38]

Таблица 3.3 – Общее сравнение антивирусов

Вирус	**Антивирусы**						
	McAfee Internet Security	**Norton Security**	**Panda Internet Security**	**Microsoft Security Essentials**	**Avast! Internet Security**	**Kaspersky Internet Security**	**Dr. Web Security Space Pro**
Лицензия	платная	бесплатная	бесплатная	бесплатная	бесплатная	платная	платная
Стоимость	1899	-	-	-	-	1340	1200
Язык	Рус.	Рус.	Рус.	Рус.	Рус.	Рус.	Рус.

Вирус	Антивирусы						
	McAfee Internet Security	**Norton Security**	**Panda Internet Security**	**Microsoft Security Essentials**	**Avast! Internet Security**	**Kaspersky Internet Security**	**Dr. Web Security Space Pro**
Использование ЦП	2,5%	7%	3%	5%	2,5%	5,5%	19%
Использование памяти	40 mb	75 mb	40 mb	70 mb	30 mb	147 mb	115 mb
Время сканирования системных папок	> 15 мин.	> 15 мин.	> 20 мин.	> 15 мин.	> 10 мин.	> 20 мин.	> 15 мин.
Время загрузки системы	>1 мин.	<1 мин.	<1 мин.	>1мин.	<1 мин.	<3 мин.	>3мин.
Техническая поддержка	+	-	-	+	+	+*	+*

Как видно из сравнения, проведённого в таблице 3.3, показатели быстродействия системы остаются примерно одинаковыми, но есть существенное различие в плане оказания технической поддержки. В оказании поддержки отличие заключается в том, что две лаборатории могут принять файл, который вызывает подозрение и внести его в базу вредоносного ПО и дать рекомендации в реальном времени. Плюс лаборатории Kaspersky и Dr.Web являются отечественными и имеют сертификат соответствия ФСТЕК. [37, 38]

Далее стоит пройтись по функционалу антивирусного ПО.

Таблица 3.4 –Сравнение функций антивирусов

Вирус	Антивирусы						
	McAfee Internet Security	Norton Security	Panda Internet Security	Microsoft Security Essentials	Avast! Internet Security	Kaspersky Internet Security	Dr. Web Security Space Pro
Сканирование по запросу	+	+	+	+	+	+	+
Постоянная защита	+	+	+	+	+	+	+
Проверка во время загрузки	+	+	+.	-	-	+	+
Веб защита	+	+	+	-	+	+	+
E-mail защита	+	+	-	+	-	+	+
Онлайн обновления	+	+	+	+	+	+	+

Как видно из таблицы 3.4, функционал антивирусного ПО в целом очень схож и не уступает друг другу, но у платных антивирусов присутствуют все проверяемые функции. Принимая во внимание данные из таблиц выше, наиболее предпочтительным становится решения от лаборатории Dr.Web.

Для грамотного использования средств защиты необходимо разделить ПК по уровням защиты:

ПК 1 уровня представляет собой наиболее защищенную рабочую станцию, предназначенную для обработки и хранения конфиденциальных данных

ПК 2 уровня это ПК с базовыми средствами защиты, предназначенный для обработки повседневно, не конфиденциальной информации. В результате описания программных средств можно составить диаграмму программного

комплекса, используемого в разрабатываемой политике информационной безопасности (рисунок 3.6).

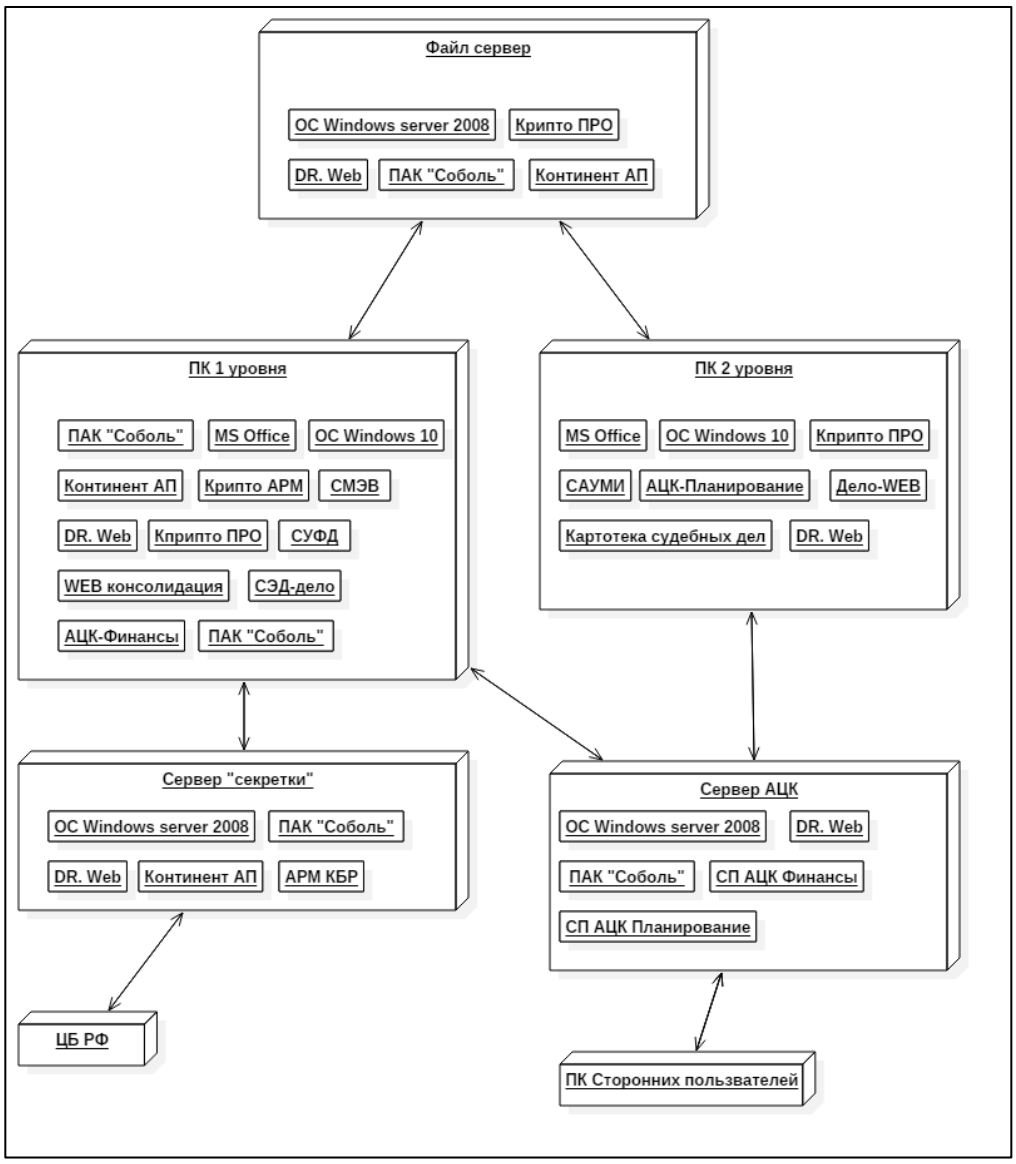

Рисунок 3.6 - Диаграмма средств обеспечения информационной безопасности в разрабатываемой политике ИБ

На всех ПК организации должно быть установлено антивирусное ПО, которое должно оперативно и своевременно обновляться, ответственным за информационную безопасность лицом. Основываясь на данных анализа, проведённого во второй главе, наиболее предпочтительными выглядят Dr.Web и Kaspersky. Принимая во внимание цену лицензии каждого продукта, выбор пал на

Dr.Web. Одним из преимуществ данного продукта является еще и факт наличия сертификата ФСТЕК, что в государственных организациях, по типу департамента финансов является очень важным критерием при выборе ПО для защиты данных.

Каждый ПК организации должен быть оснащен источником бесперебойного питания, для защиты от скачков напряжения или внезапного отключения электроэнергии. Это делается для того, чтобы при внештатном отключении электроэнергии рабочие данные на ПК сохранялись. Так же источником бесперебойного питания должно оснащаться и серверное оборудование, чтобы не спровоцировать потерю данных или же выход оборудования из строя.

3.2 Методы обеспечения информационной безопасности

В первой главе уже рассматривались методы обеспечения защиты информации. В этой главе эти методы будут рассмотрены более предметно, с расчётом на обеспечения защиты данных в Департаменте финансов. Так как нет универсальных методов, направленных на защиту информации, то для каждой организации они составляются индивидуально.

Принимая во внимание, что среднестатистический пользователь ПК не отличается высоким уровнем компьютерной грамотности. Исходя из этого, разрабатываемые методы защиты информации в политике информационной безопасности должна частично регулировать действия пользователей либо дать базовые методические рекомендации, которые будут направлены на защиту данных. Содержать раздел, в котором будет отражён свод правил.

Данный раздел можно расценивать как «инструкцию по применению». Актуален этот раздел политики информационной безопасности будет как для рядового пользователя, так и для опытного сотрудника. Предназначение данного раздела нацелено на увеличение эффективности работы средств, которые были описаны выше. Иными словами, в случае сбоя средств или возникновения внештатной ситуации пользователь мог самостоятельно идентифицировать угрозу

и минимизировать потери данных. Для начала следует определить, структуру документов, задействованных в организации, то есть политика информационной безопасности должен быть высшим документом. То есть иерархия документов используемых в департаменте финансов должна выглядеть следующим образом:

1) Данная политика ИБ является внутренним нормативным документом по ИБ первого (высшего) уровня.

2) Документами второго уровня являются – инструкции, порядки, регламенты и прочие документы описывающие действия сотрудников Организации по реализации документов первого и второго уровня.

3) Документами третьего уровня являются - отчётные документы о выполнении требование верхних уровней. [2]

Данная иерархия более наглядно представлена на рисунке 3.7.

Рисунок 3.7 - Иерархия документов в Департаменте финансов

Следующим фактором, который прямым образом влияет на успешность защиты данных, это следующие требование: к работе с информационными ресурсами допускаются пользователи, ознакомленные по роспись с правилами и принципами работы с информационными ресурсами и ответственностью за их нарушение, а также политикой информационной безопасности.

При трудоустройстве, трудоустраиваемому сотруднику должны быть доведены его права и обязанности по обеспечению безопасности информационных ресурсов, описанные в Политике ИБ Департамента финансов, и внесены в его должностные обязанности, должностную инструкцию. В инструктаж и должностную инструкцию должны входить как общие обязанности по реализации и поддержке Политики ИБ Департамента финансов, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

Все принимаемые на работу сотрудники должны согласиться с возложенными на них обязанностями и подписать свои трудовые договоры, в которых устанавливается их ответственность за выполнение Политики ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Организации по проверке выполнения требований Политики ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть прописаны меры, которые будут приняты в случае несоблюдения сотрудником требований Политики ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника Организации.

Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, установленным уровнем доступа, с мерами ответственности за нарушение этого уровня.

При предоставлении сотруднику доступа к ИС Организации он должен ознакомиться под роспись с инструкцией пользователя ИС.

Каждому сотруднику, допущенному к работе с информационными ресурсами, должно быть сопоставлено присвоено уникальное имя (учетная запись пользователя), под которым он должен быть зарегистрирован и с помощью которого он будет авторизовываться в ИС. В случае необходимости некоторым сотрудникам могут быть присвоено несколько уникальных имен (учетных

записей). Использование несколькими сотрудниками при работе в Организации одного и того же имени пользователя («группового имени») запрещено.

Вдобавок к этому требованию можно отметить, что инструктажи по информационной безопасности должны проводиться регулярно. Помимо инструктажей, следует проверять уровень знаний пользователя, по средствам тестирования и в случае необходимости восполнять пробелы пользователя, например, отправлять на курсы повышения квалификации.

Следующий момент - регистрация пользователя. Процедура регистрации должна производиться ответственным лицом, на основании документа, например заявки. Данная заявка должна содержать в себе необходимую информацию о пользователе такую как:

- ФИО;
- должность;
- срок исполнения обязанностей (если сотрудник временный);
- номер приказа, о зачислении сотрудника на должность.

Сюда же стоит добавить, что при наступлении момента прекращения полномочий пользователя, весь доступ к информационным ресурсам должен быть немедленно закрыт.

Особое внимание следует уделить процедуре предоставления паролей, данный процесс должен быть предоставлен в качестве официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя в систему с помощью выданного ему временного, система сразу же требовала его сменить;
- временные пароли должны выдавать пользователю только после его идентификации;

- необходимо избегать передачи паролей с использованием третьих лиц или по средствам незашифрованной электронной почты;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;
- необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- необходимо изменять пароля пользователя не реже одного раза в 90 дней.

На основе учётных данных пользователя, предоставляются права доступа, протоколируются производимые им в действия и обеспечивается режим конфиденциальности, обрабатываемых данных.

Не допускается использование различными пользователями одних и тех же учётных данных. Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности, после чего, пользователь устанавливает свой собственный пароль.

Сотрудникам департамента финансов запрещено использовать переносные USB накопители третьих лиц. С целью предотвращения заражения ПК или установки шпионского ПО.

Ежедневно при начале работы ПК пользователя должен подвергаться частичной проверке антивирусным ПО и полной проверке в конце рабочей недели или же при возникновении необходимости.

Перед началом работы, пользователь должен визуально осмотреть своё рабочее место, с целью обнаружения шпионского оборудования.

Особое внимание следует уделить почтовым сообщениям, которые поступаю пользователю по средствам E-mail. Категорически запрещается открывать письма с сомнительным содержанием без предварительной проверки.

Каждый пользователь, должен исключить кражу своих паролей, необходимых для работы в информационных ресурсах. Так же, необходимо осуществлять периодическую смену пароля. Ответственность за сохранность паролей несёт сам пользователь.

При возникновении опасности кибератак, необходимо оповестить и проинструктировать всех пользователей.

Специалистом по информационной безопасности должна (или при помощи сторонней организации) проводиться периодическая проверка средств защиты информации Организации путем моделирования возможных попыток осуществления несанкционированного доступа к защищаемым информационным ресурсам.

Специалистом по информационной безопасности должна собираться и анализироваться информация о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения Организации. Источником сведений могут быть официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Так же необходимо учесть и те недочёты, которые были выявлены во второй главе, при рассмотрении текущей политики ИБ, а именно:

- необходимо наладить взаимодействие между ИТ отделом и рядовыми пользователями. Прописать и задокументировать степень ответственности сторон.
- необходимо осуществлять тестирование, собеседование кандидата на трудоустройство с целью выявления у него предрасположенностей либо намерений для нарушения политики информационной безопасности.

- необходимо обеспечить процесс подготовки данных в организации, а именно осуществлять контроль информации. При передаче носителей данных использовать специализированные организации или курьерскую службу.
- необходимо заключить договор с организацией, которая может обеспечить поставку и ремонт оборудования в кротчайшие сроки.

Итак, в третьей главе диссертационной работы на тему Разработка политики информационной безопасности для Департамента финансов г.о. Тольятти, было выполнено устранение недочётов, выявленных в результате анализа, проведённого во второй главе. Было осуществлено написание политики информационной безопасности, которая представлена в приложении Б. Осуществлён выбор средств для защиты данных.

ГЛАВА 4 АПРОБАЦИЯ ЭФФЕКТИВНОСТИ РАЗРАБОТАННОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной главе проводится апробация результатов, проводится повторная оценка политики информационной безопасности по методологии МАРИОН. Рассматривается экономическая составляющая, с целью оценки целесообразности трат на введение разрабатываемой политики информационной безопасности.

Основой экономической эффективности является очевидное предположение, что при нарушении конфиденциальности информации наносится определенный ущерб, следовательно - обеспечение защиты информации подразумевает расходование средств. Таким образом, стоимость обеспечения информационной безопасности может быть выражена суммой расходов на защиту данных и потерь от ее нарушения.

Стоит так же отметить, что экономическая целесообразность мероприятий по обеспечению защиты данных может быть определена, через количество предотвращенных угроз и ущерба от них или уровень снижения риска для информационных ресурсов Департамента финансов.

Так как решение вопроса о необходимом уровне затрат на защиту заключается в том, что уровень затрат должен быть равен уровню возможных потерь при нарушении конфиденциальности информации, следовательно необходимо определить только уровень потерь.

При расчёте суммарного показателя необходимо принять во снимание, что угрозы конфиденциальности, целостности и доступности реализуются злоумышленником независимо. Иными словами, если была нарушена целостность информации, то предполагается, что содержание информации злоумышленнику до сих пор не известно, конфиденциальность не нарушена, а сотрудники по-прежнему имеют доступ к информационным ресурсам. [9, 10]

Рассмотрение величины потерь для критичных информационных ресурсов Департамента финансов приводится в таблице 4.1.

Таблица 4.1 - Величины потерь для критичных информационных ресурсов Департамента финансов

Информационный ресурс	**Тип угрозы**	**Величина потерь (тыс. руб.)**
Проектная документация, созданная ДФ	Нарушение конфиденциальности	1 00
Проектная документация, созданная ДФ	Нарушение целостности	1 00
Проектная документация, созданная ДФ	Нарушение доступа	30
Финансовые проекты, разрабатываемые/обрабатываемые ДФ	Нарушение конфиденциальности	700
Финансовые проекты, разрабатываемые/обрабатываемые ДФ	Нарушение целостности	1000
Финансовые проекты, разрабатываемые/обрабатываемые ДФ	Нарушение доступа	500
Персональные данные сотрудников	Нарушение конфиденциальности	100
Персональные данные сотрудников	Нарушение целостности	50
Персональные данные сотрудников	Нарушение доступа	10
Системное ПО	Нарушение конфиденциальности	10
Системное ПО	Нарушение целостности	100
Системное ПО	Нарушение доступа	500
Прикладное ПО	Нарушение конфиденциальности	10
Прикладное ПО	Нарушение целостности	100
Прикладное ПО	Нарушение доступа	500
Общая сумма вероятных потерь	2910000	

В результате произведённых расчётов и построения таблицы 3 были определены риски финансовых потерь для ДФ, приблизительная общая сумма потерь составила 2910000 рублей. Исходя из этого, можно сделать вывод, что реализация любой из вышеуказанных угроз для Департамента финансов будет существенной потерей. Для понимания насколько эффективна разработанная политика информационной безопасности необходимо произвести расчёт показателей экономической эффективности проекта.

4.1 Расчёт показателей экономической эффективности политики информационной безопасности

Защита информации зависит от уровня эффективности задействованных средств защиты информации, которые определяются как ресурс системы.

Под ресурсом может пониматься количество людей, привлекаемых для защиты данных, в виде программных или инженерно-технических средств используемых для защиты данных. Как ресурс можно рассматривать так же денежные средства необходимые для оплаты персонала и технических средств. Стоит отметить, что использование ресурса, задействованного для защиты, может быть как разовое, так и постоянное.

В качестве разового ресурса может быть выступить:

- закупка оборудования или ПО;
- установка оборудования или ПО;
- наладка оборудования или ПО.

Постоянным ресурсом может выступить:

- заработная плата;
- поддержание уровня безопасности;
- использование текущих технических средств.

Исходя из вышеописанного для определения экономических показателей защиты информации нужны следующие данные:

- Расходы, под расходами подразумеваются денежные средства задействованные для оплаты создания, модернизации и поддержания текущих средств защиты информации в рабочем состоянии.
- Величины потерь, под этим видом данных, подразумевается объем потерь после внедрения/модернизации защиты данных.

Далее, в таблице 4.2 приводится содержание и стоимость разового ресурса, задействованного для защиты данных в ДФ.

Таблица 4.2- Содержание и стоимость разового ресурса, задействованного для защиты данных в ДФ.

Обще организационные мероприятия				
№ п/п	Проводимые действия		Стоимость всего (тыс. руб.)	
1	Создание методик и приказов		1100	
2	Доведение информации до сотрудников		440	
Мероприятия инженерно-технической защиты				
№ п/п	Проводимые действия	Стоимость	Кол-во	Стоимость всего (тыс. руб.)
1	Камеры наблюдения	6 000	14	84 000
2	Датчики движения	500	14	7 000
3	Рутокен	1 600	120	192 000
4	Турникет	50 000	1	50 000
5	Металлоискатель рамка	90 000	1	90 000
6	Токен для фухакторной аутентификации	1 650	6	9 900
7	Кодовый замок	1 500	6	9 000
8	Карточки электронные	300	120	36 000
9	ОС Windows 7	120	2000	240 000
10	Пломбы и инструменты опломбирования	120	14	1680
11	Сейфы	10 000	3	30 000
12	СКЗИ Континент	90 000	1	90 000

Продолжение таблицы 4.2

13	Антивирусное ПО	1 200	120	144 000
14	Система архивирования видеозаписей	30 000	1	30 000
15	Датчики задымления	1 000	150	150 000
16	Эл. Замок Соболь	12 000	6	72 000
17	Провода и прочие расходные материалы	5000	1	5 000
Общая сумма	1 240 580			

Следовательно, для закупки необходимых средств необходимо 1 240 580 рублей. Далее рассмотрим содержание и объем постоянного ресурса, выделяемого на защиту информации. Данная информация рассматривается в таблице 4.3.

Таблица 4.3 - Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия			
№ п/п	Проводимые действия	Прошлая стоимость	Стоимость всего
1	Проведение инструктажей, тренингов	11 000	11 000
2	Проведение курсов повышения квалификации	-	120 000
Мероприятия инженерно-технической защиты			
№ п/п	Проводимые действия	Прошлая стоимость	Стоимость всего
1	Настройка ПО	70 000	160 800
2	Обслуживание системы видеонаблюдения	-	50 000
3	Обслуживание датчиков движения	-	192 000

Продолжение таблицы 4.3

4	Обслуживание электронных замков	-	30 000
5	Обновление ПО	25 000	25 000
Общая сумма		116000	588800

Исходя данных таблицы, приведённой выше, следует, что ежегодное обслуживание оборудования будет обходиться организации в 588800 рублей.

То есть для введения политики ИБ потребуется сумма в размере 1829380 рублей, что значительно ниже, чем сумма вероятных потерь до введения политики ИБ.

Сравнение сумм до и после введения разрабатываемой политики приводится ниже (рисунок 4.1).

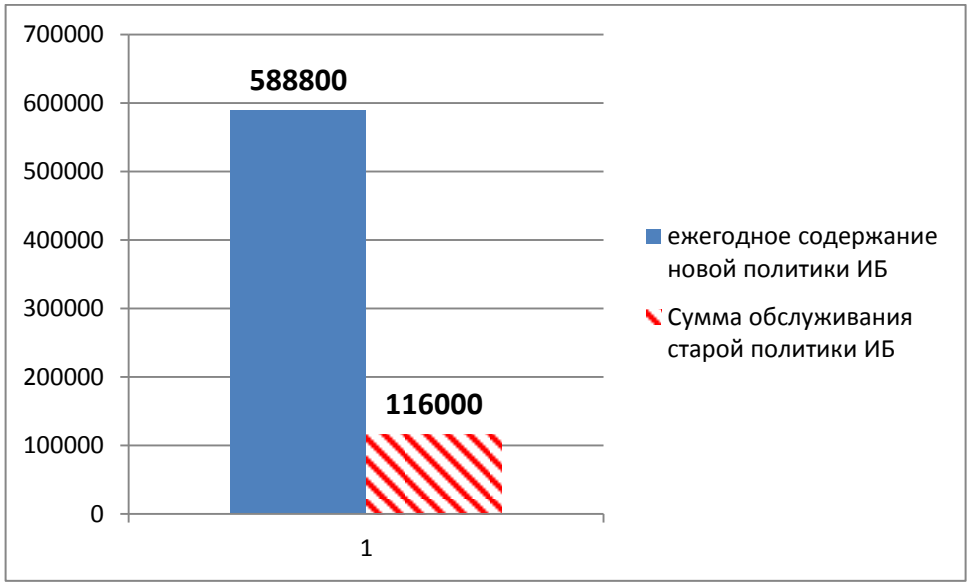

Рисунок 4.1 - Сравнение сумм ежегодного обслуживания

Сравнение суммы вероятных потерь до введения разрабатываемой политики информационной безопасности и общей суммы введения разрабатываемой политики информационной безопасности.

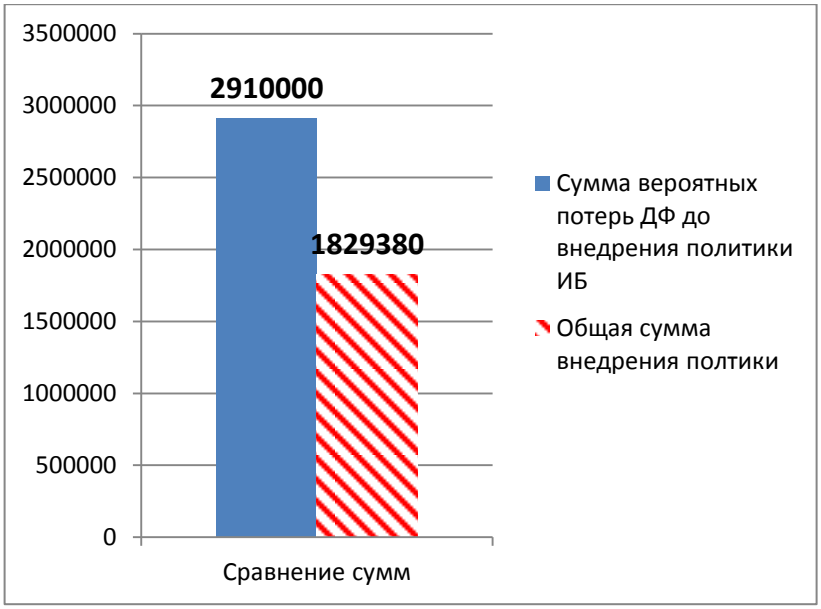

Рисунок 4.2 - Сравнение сумм вероятных потерь и общей суммы внедрения политики ИБ

Далее для проведения расчётов необходимо получить возможные данные о величине потерь для критичных информационных ресурсов после внедрения политики ИБ (таблица 4.4). Результаты формируются по результатам экспертного опроса.

Таблица 4.4 - Данные о величине потерь для критичных информационных ресурсов

Информационный ресурс	**Тип угрозы**	**Величина потерь (тыс. руб.)**
Проектная документация, созданная ДФ	Нарушение конфиденциальности	100
Проектная документация, созданная ДФ	Нарушение целостности	80
Проектная документация, созданная ДФ	Нарушение доступа	15
Финансовые проекты, разрабатываемые/обрабатываемые ДФ	Нарушение конфиденциальности	700
Финансовые проекты, разрабатываемые/обрабатываемые ДФ	Нарушение целостности	100
Финансовые проекты,	Нарушение доступа	350

Информационный ресурс	Тип угрозы	Величина потерь (тыс. руб.)
разрабатываемые/обрабатываемые ДФ		
Персональные данные сотрудников	Нарушение конфиденциальности	100
Персональные данные сотрудников	Нарушение целостности	50
Персональные данные сотрудников	Нарушение доступа	10
Системное ПО	Нарушение конфиденциальности	0
Системное ПО	Нарушение целостности	80
Системное ПО	Нарушение доступа	500
Прикладное ПО	Нарушение конфиденциальности	0
Прикладное ПО	Нарушение целостности	100
Прикладное ПО	Нарушение доступа	350
Общая сумма вероятных потерь	2535000	

Исходя из вероятных данных, представленных в таблице выше, стоит отметить существенное снижение возможных потерь данных. Сравнение показателей до и после введения разрабатываемой политики информационной безопасности привозятся в диаграмме на рисунке 4.3.

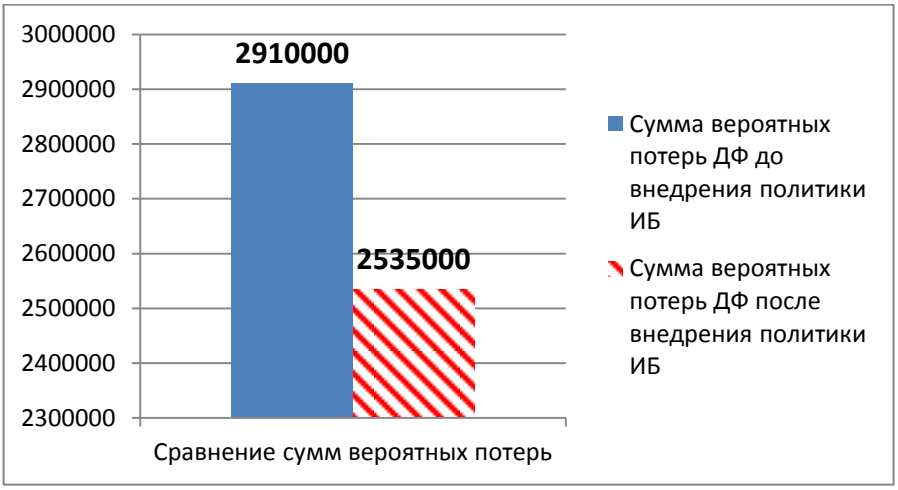

Рисунок 4.3 – Сравнение сумм вероятных потерь

Далее необходимо перейти к оценке рисков и тестированию политики информационной безопасности.

4.2 Тестирование политики информационной безопасности

В данном разделе проводится оценка разрабатываемой политики информационной безопасности. Оценку уровня защиты необходимо провести с помощью методологии МАРИОН, для этого необходимо заново ответить на вопросы, чтобы произвести оценку секторов, которые представлены во второй главе (список рассматриваемых тем в приложении А).

В результате осуществления оценка уровня защищенности по методологии МАРИОН были получены результаты, которые отражены в таблице 4.5.

Таблица 4.5 – Результаты оценки разрабатываемой политики ИБ

Номер	***Описание***	***Очки***	***Риск***
101	Общая безопасность: Общая организация	2,95	0,05
102	Общая безопасность: Общий контроль	2,68	0,32
103	Общая безопасность: Процедуры безопасности и аудит	2,82	0,18
201	Социоэкономические факторы: Социоэкономические факторы	2,70	0,30
301	Общая компьютерная безопасность: Окружение	2,56	0,44
302	Общая компьютерная безопасность: Контроль физического доступа	2,47	0,53
303	Общая компьютерная безопасность: Загрязнение	2,80	0,20
304	Общая компьютерная безопасность: Инструкции по безопасности	2,90	0,10
305	Общая компьютерная безопасность: Пожарная безопасность	2,93	0,08
306	Общая компьютерная безопасность: Безопасность от проникновения воды	2,90	0,10
307	Общая компьютерная безопасность: Правильность установки компьютеров	2,91	0,09
308	Общая компьютерная безопасность: Процедуры восстановления после аварии	3,00	0,00

Номер	*Описание*	*Очки*	*Риск*
309	Общая компьютерная безопасность: Связь между пользователями и персоналом ИТ	2,93	0,07
310	Общая компьютерная безопасность: Кадровая политика отдела ИТ	2,92	0,08
311	Общая компьютерная безопасность: Стратегия ИТ	2,65	0,35
401	Логический контроль доступа (вкл. телекомм.): Безопасность аппаратного и сист. ПО	3,01	-0,01
402	Логический контроль доступа (вкл. телекомм.): Безопасность телекоммуникаций	3,03	-0,03
403	Логический контроль доступа (вкл. телекомм.): Безопасность баз данных	2,80	0,20
501	Безопасность операций: Сохранение и восстановление данных	2,85	0,15
502	Безопасность операций: Подготовка и передача данных	2,35	0,65
503	Безопасность операций: Резервное копирование	2,78	0,22
504	Безопасность операций: Оперативные процедуры	2,79	0,21
505	Безопасность операций: Поддержка аппаратного и программного обеспечения	2,76	0,24
601	Безопасность разработки и внедрения систем: Контроль изменений	2,02	0,98
602	Безопасность разработки и внедрения систем: Процедуры разработки систем	2,40	0,60

Основываясь на данных из таблицы 4.5, полученных в результате оценки рисков были построены радарная диаграмма (рисунок 4.4) и график (рисунок 4.5).

Как видно из радарной диаграммы, «площадь охвата» информационной безопасности возросла, следовательно, вырос и уровень безопасности.

При анализе графика на рисунке 4.6 уровень угроз не превышает <1, что является отличным показателем уровня защищенности данных. Подобный результат достигается в результате использования средств описанных в третьей главе, а также пересмотра методов обеспечения информационной безопасности.

Как видно из графика на рисунке 4.6 уровень угрозы от уязвимостей, выявленных в результате анализа во второй главе, существенно снизился.

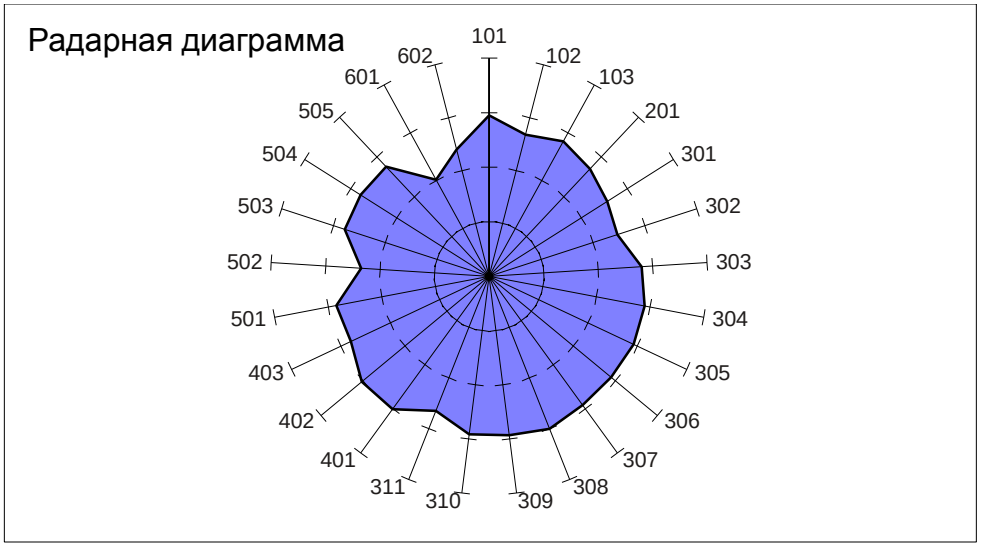

Рисунок 4.5 – Радарная диаграмма рисков разрабатываемой политики ИБ

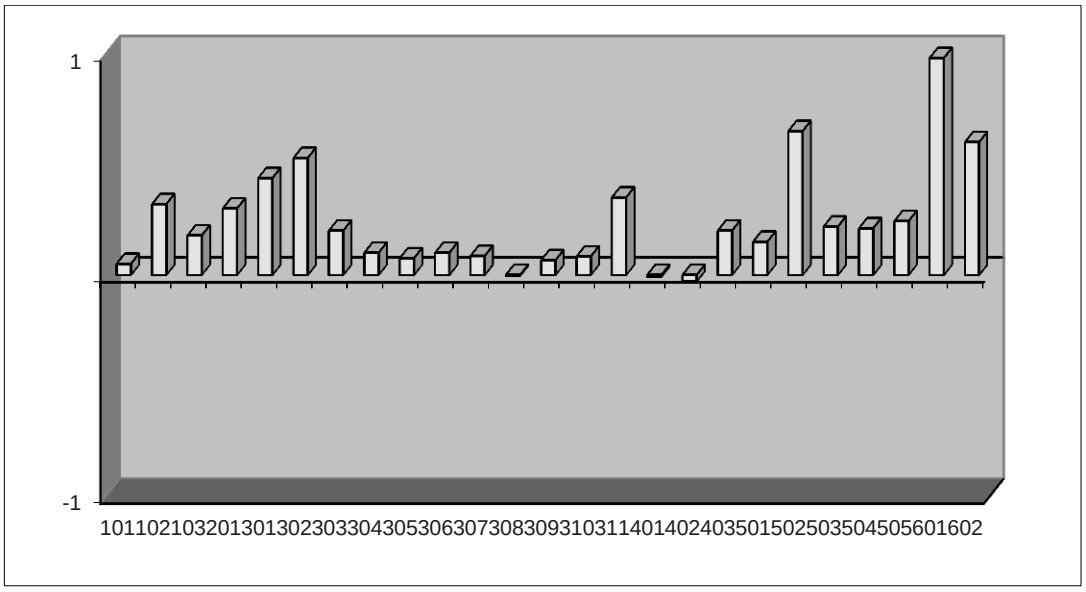

Рисунок 4.6 – График оценки угроз

Рассмотрение изменений в процессах работы сотрудников департамента финансов производится на примере процесса обмена данными внутри организации. Для этого построена диаграмма по методологии BPMN (рисунок 4.7).

Как видно из данной диаграммы, что даже в случае перехвата и дешифровки, повторное шифрование без открытого сертификата невозможно, стоит отметить, что дешифровка данных без закрытого сертификата невозможна. Следовательно, нарушение целостности данных невозможно. Данная мера позволяет исключить угрозу целостности данных, исходящую изнутри организации.

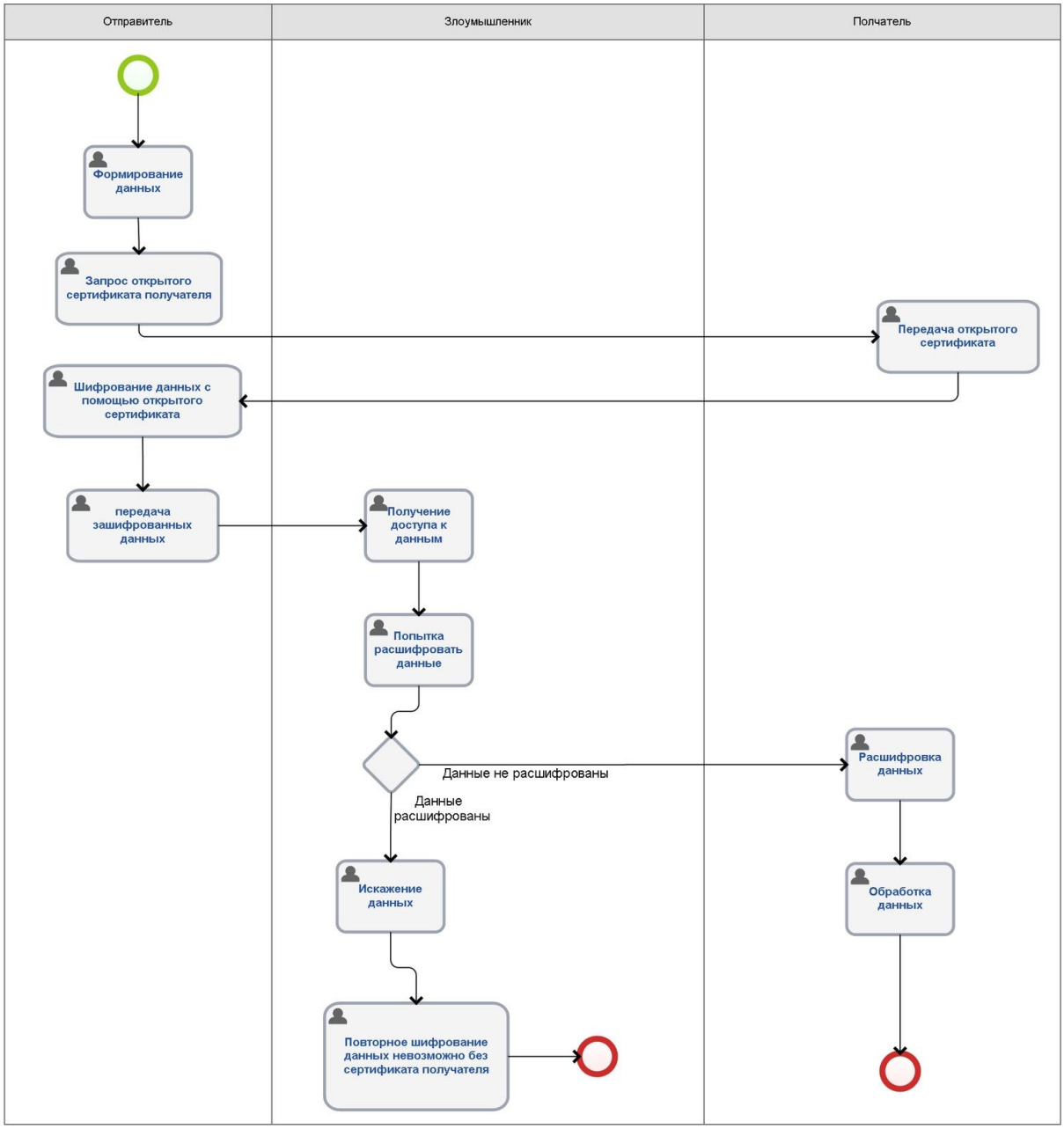

Рисунок 3.7 – Процесс обмена данными с применением шифрования

Для более точного тестирования средств было проведено тестирование с использованием тестового стенда.

Результаты тестирование приведены в таблице 4.6.

Таблица 4.6 – Результаты тестирования политики информационной безопасности

	1кв	2кв	Случаев нарушения работы	Случаев остановки работы
До введения	310	390	200	130
После введения			120	31

Для наглядности построен график (рисунок 4.8).

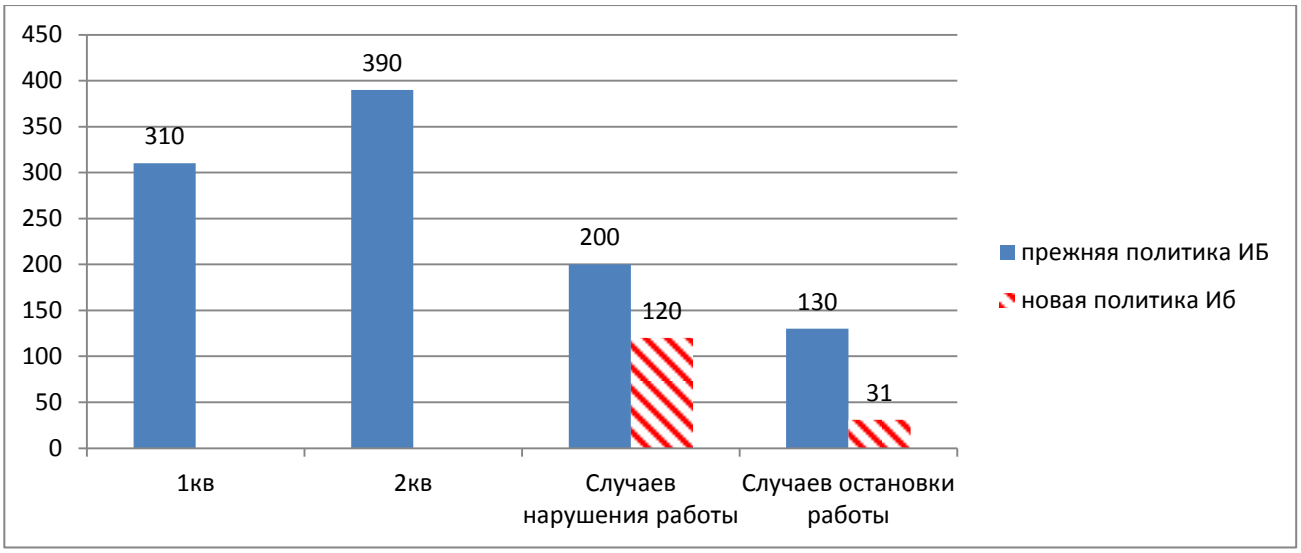

Рисунок 4.8 – Сравнение эффективности политик информационной безопасности

Основываясь на результатах, полученных во время тестирования и принимая во внимание экономический аспект, можно сделать вывод, что разработанная политика ИБ может получить применение. Но чтобы эта политика была эффективна необходимо обеспечить безукоризненное выполнение требований политики абсолютно всеми сотрудниками ДФ. Так же необходимо, чтобы ответственные люди постоянно занимались актуализацией средств, задействованных для обеспечения безопасности.

ЗАКЛЮЧЕНИЕ

Во время работы над магистерской диссертацией была проанализирована научная литература, относящаяся к разработке политики информационной безопасности, обеспечению защиты периметра, а также нормы, стандарты и законы РФ в сфере информационной безопасности. Попутно были рассмотрены труды независимых лабораторий в сфере информационной безопасности и рассмотрены статистические данные за прошлые года. Этот анализ позволил сделать заключение о том, что направление информационной безопасности в настоящее время очень востребовано. Анализ статистических данных и анализ прецедентов происходивших в департаменте финансов показал, что в большинстве случаев реализация угроз и различных утечек данных происходила с участием сотрудников работающих в департаменте финансов.

Были рассмотрены и проанализированы основные угрозы целостности информации и средства защиты от них. Рассмотрены средства защиты информации, проанализирован ИТ рынок и выбраны основные средства для защиты данных.

Была проанализирована текущая политика информационной безопасности и на основе её разработана новая политика информационной безопасности.

Апробация полученных результатов на основе проведенного тестирования политики информационной безопасности Департамента Финансов показала, что использование новой политики информационной безопасности приводит к повышению уровня безопасности, так как позволяет сократить вероятность успешной реализации угроз злоумышленниками.

Основной научный результат магистерской диссертации состоит в том, что разработанная политика информационной безопасности позволяет снизить вероятные риски компрометации, потери или искажения данных. Основные преимущества реализованной политики информационной безопасности заключаются в следующем:

- больший контроль за действиями сотрудников;
- снижение рисков инсайдерской атаки;
- разграничение доступа в помещения;
- частичная автоматизация идентификации персоны.

Таким образом, реализованная политика информационной безопасности может получить широкое применение, её использование позволит снизить риски потери данных, так же с точки зрения экономической составляющей её использование является целесообразным и эффективным.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Веснин В.Р. Информационное обеспечение управления. - Москва: Гном-пресс, 1999. - 440с.

2. Лачихина А.Б. Модели противодействия угрозам нарушения информационной безопасности при эксплуатации баз данных в защищенных корпоративных информационных системах [Текст]: дис. к.т.н: 05.13.19, 05.13.17 / Лачихина Анастасия Борисовна – Москва, 2010.

3. Луцкий, С.Я. Корпоративное управление техническим перевооружением фирм: Учебное пособие / С.Я. Луцкий [Текст]. - М.: Высшая школа, 2016. - 319 с.

4. Ожигова М.И. Повыгение уровня информционной защищенности корпоративной компьютерной сети за счёт разработанных модулей сканирования сетевых ресурсов. М.: ЦРНС. – 2015. – 183-190 с.

5. Edited by Doctor of Economics professor D. Chistov. New Information Technologies in Education [Текст]. Moscow – 2016. Part 1.

6. IBM collaboration software Lotus Notes and Domino [Электронный ресурс]. - Режим доступа: https://www-01.ibm.com/software/lotus/ (09.10.2017).

7. Сатунина А. Управление проектом корпоративной информационной системы предприятия. М.: Инфра М. – 2009- 352 с.

8. Аверченков В. И. Аудит информационной безопасности: учебное пособие для вузов. М. Флинта. 2016 – 269 с.

9. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. М. : КДУ – 2013 - 736 с.

10. Зоря А.И. Обоснование степени защиты информации, протекающих в бизнес-процессах на предприятии: выпускная квалификационная работа. 2015 – 85с.

11. Загийнайлов Ю.Н. Основы информационной безопасности. Директ-Медиа. 2015-105с.

12. Сычев Ю.Н. Основы информационной безопасности. Евразийский открытый институт. 2010 - 328 с.

13. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. Логос. 2010 – 347 с.

14. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. Питер. 2017 – 256 с.

15. Баранова Е., Бабаш А. Информационная безопасность и защита. Инфра – М. 2017 – 324 с.

16. Мэйволд Э. Безопасность сетей. Национальный Открытый Университет «ИНТУИТ». 2016 – 572

17. Бонларев В. Введение в информационную безопасность автоматизированных систем. МГТУ им. Н. Э. Баумана. 2016 – 252 с.

18. Нестеров С. Основы информационной безопасности. Лань. 2016 – 324 с.

19. Кочерга С. А., Ефимова Л. Л. Информационная безопасность детей. Российский и зарубежный опыт: монография. ЮНИТИ – ДАНА. 2013 – 239 с.

20. Логос. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник. Логос. 2011 – 452 с.

21. Фороузан Б. А. Математика криптографии и теория шифрования. Национальный Открытый Университет «ИНТУИТ». 2016- 511 с.

22. Kristen DIETZ. Application of a POD Exercise to University Education Programs Health and Kinesiology, Purdue University West Lafayette, IN 47907, USA.

23. Мешков А.А. Магистерская работа «Обеспечение информационной безопасности хозяйствующего субъекта на примере частного образовательного учреждения ЧОУ ВО Самарская гуманитарная академия». Тольяттинский государственный университет, Институт финансов, экономики и управления. 2017 – 149 с.

24. Голембиовская О.М. Магистерская работа «Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности». Брянский государственный технический институт. 2013 – 171 с.

25. Лейман А.В. Магистерская работа «Защита конфиденциальной информации в медиа-пространстве на базе стенографических методов». Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 213 – 109 с.

26. Десницкий В.А. Магистерская работа «Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления». Санкт-Петербургский институт информатики и автоматизации РАН. 2013 – 98 с.

27. Боридько И.С. Магистерская работа «Методическое обеспечение защиты информации автоматизированной системы от несанкционированного доступа с учетом менеджмента инцидентов информационной безопасности». Институт инженерной физики. 2013 – 143 с.

28. Nguena, I.M. and Richeline, A.-M.O.C. (2017) Fast Semantic Duplicate Detection Techniques in Databases. Journal of Software Engineering and Applications. – 2017, P.529-545.

29. Roland Mas. The DEBIAN administrator’s handbook [Текст]. – 2016. – 522 p.

30. Rizik M.H. A New Approach for Database Fragmentation and Allocation to Improve the Distributed Database Management System Performance. – 2014, p.891-905.

31. Zachman A. A framework for Information Systems Architecture // IBM Systems Journal. 1987. Vol. 26. № 3.

32. Admin. Написание скриптов на BASH Linux [Электронный ресурс]. - Режим доступа: https://losst.ru/napisanie-skriptov-na-bash

33. Годовой отчёт по информационной безопасности. Cisco 2018 [Электронный ресурс] - https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf .

34. Проблемно-игровой метод мотивации студента специальности «Информационная безопасность» [Электронный ресурс] - ttps://habr.com/ru/post/286114/.

35. Цели и задачи политики информационной безопасности [Электронный ресурс] - https://searchinform.ru/products/kib/politiki-informatsionnoj-bezopasnosti/celi-i-zadachi-politiki-informacionnoj-bezopasnosti/.

36. Актуальные киберугрозы. I квартал 2019 года [Электронный ресурс] - https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/#id2

37. Реестр ФСТЭК [Электронный ресурс] - https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00.

38. Сравнение Антивирусов 2019 [Электронный ресурс] - https://www.anti-malware.ru/tests_history

ПРИЛОЖЕНИЕ А

Список тем рассматриваемых при анализе политики информационной безопасности

1. Структура.
2. Комитет по безопасности.
3. Исследование защищенности.
4. правление безопасностью.
5. Управление рисками и страхование.
6. Юридические проблемы.
7. Связь с пользователями.
8. Владелец данных.
9. Выбор контроля пользователя.
10. Контроль пользователя или контроль качества.
11. Обзор основных бухгалтерских данных.
12. Офисные процедуры.
13. Безопасность документации.
14. Хранение и безопасность первичных документов.
15. Структура службы внутреннего аудита.
16. Компьютерный аудит.
17. Социоэкономический климат.
18. Безопасность компьютерных зданий.
19. Безопасность компьютерных помещений.
20. Защита территории.
21. Безопасность электрооборудования.
22. Контроль физического доступа в здания.
23. Механическая защита.
24. Контроль физического доступа в компьютерные комнаты.
25. Контроль доступа в другие помещения.
26. Управление и мониторинг систем безопасности.
27. Качество воды.
28. Статическое электричество.
29. Загрязнение воздуха.
30. Инструкции по безопасности.
31. Проверка знания инструкций.
32. Исследование пожарной безопасности.
33. Система обнаружения огня в здании.
34. Автоматическая система обнаружения огня в компьютерных помещениях.
35. Автоматическая система пожаротушения в здании.
36. Автоматическая система пожаротушения в компьютерных помещениях.
37. Огнетушители.
38. Пожарные гидранты.
39. Предупреждение ущерба от пожара.
40. Безопасность персонала.
41. Повреждения от воды.
42. Трубопроводы.
43. Кондиционирование.

44. Дренаж воды.
45. Детекторы воды.
46. Другие средства.
47. Выбор аппаратного и системного программного обеспечения.
48. Резервирование компьютеров.
49. Кондиционирование.
50. Стабилизация напряжения.
51. Резервные генераторы.
52. План восстановления после аварии.
53. Компьютерный комитет.
54. Персональные компьютеры: выбор и процедуры.
55. Связи между отделом ИТ и пользователями.
56. Текучесть кадров.
57. Обучение и информация.
58. Условия работы.
59. Назначение и ротация поддержки ключевых задач.
60. Штатное расписание и ответственность.
61. Аварийные укрытия для ключевого персонала.
62. Прием на работу и контракты.
63. Компьютерная стратегия.
64. Стратегия безопасности.
65. Планирование изменений.
66. ПО логического контроля доступа.
67. Физическая защита аппаратного обеспечения.
68. Безопасность сети.
69. Наблюдение за линиями и ключевыми передачами данных.
70. Администрирование данных.
71. Администрирование баз данных.
72. Журналирование и безопасность обновлений.
73. Журналирование и отслеживание доступа
74. Шифрование данных.
75. Процедуры хранения.
76. Защита хранилищ.
77. Работа с носителями.
78. Аудит и учет носителей.
79. Подряды специализированных фирм.
80. Подготовка данных.
81. Безопасность передачи носителей.

ПРИЛОЖЕНИЕ Б

Политика информационной безопасности Департамента финансов г.о. Тольятти

Введение

Политика информационной безопасности (далее - политика ИБ) Департамента финансов г.о. Тольятти (далее – организации или ДФ) представляет собой методические рекомендации и инструкции как для продвинутых так и для обычных пользователей. В политике ИБ представлено систематизированное изложение целей и задач для защиты, данной политикой необходимо руководствоваться во время деятельности.

Обеспечение информационной безопасности и соблюдение политики ИБ – это необходимое условие для обеспечения непрерывной и корректной деятельности организации.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов. Политика ИБ охватывает автоматизированные, телекоммуникационные системы, владельцем и пользователем которых является Организация.

Основная идея для реализации Политики ИБ должна мысль, что невозможно обеспечить максимальную защищенность информационных ресурсов, только одной лишь с помощью одного средства или их совокупности.

Основной целью, на достижение которой направлены положения изложенной Политики ИБ, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия, а также минимизация потерь и рисков ИБ.

Для достижения поставленной цели, необходимо обеспечить решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ.
- создание механизма оперативного реагирования на угрозы ИБ.
- предотвращение и/или снижение ущерба от реализации угроз ИБ.
- защита от вмешательства в процесс функционирования ИС третьими лицами.
- соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ.
- обеспечение непрерывности первостепенных бизнес-процессов.

- детальное изучение/анализ партнёров, клиентов, сотрудников и кандидатов на работу.
- недопущение проникновения элементов организованной преступности и лиц с противоправными, преступными намерениями.
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.
- повышение компьютерной грамотности и корпоративной культуры у сотрудников.

Основания для разработки

Данная политика разработана на основе требований законодательства Российской Федерации, накопленного в Организации опыта в области обеспечения ИБ, а так же интересов и целей Учреждения.

При написании отдельных положений данной политики ИБ использовались следующие нормативные документы:

- ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;
- РС БР ИББС-2.0-2007 «Методические рекомендации по документации в области обеспечения информационной безопасности;
- РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности»;
- РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности»;
- СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».

Область действия

Данная Политика распространяется на все бизнес-процессы Департамента финансов и обязательна к исполнению абсолютно всеми работниками и руководством Департамента финансов, а также пользователями его информационных ресурсов.

Настоящая политика распространяется на всех сотрудников и ИС Департамента финансов. Лица, осуществляющие разработку внутренних документов Департамента финансов, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой ИБ.

Система управления информационной безопасностью

Для достижения указанных целей и задач в Департаменте финансов внедряется система управления информационной безопасностью. СУИБ задокументирована в настоящей политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников Департамента финансов в области действия системы. Документированные требования СУИБ доводятся до сведения сотрудников Департамента финансов.

Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.

Стоимость внедряемых средств управления информационной безопасностью не должна превышать возможный ущерб, возникающий при реализации угроз.

Структура документов Департамента финансов

В целях создания единой структуры нормативных документов Департаменте финансов в области обеспечения ИБ, создаваемые или обновляемые нормативные документы должны соответствовать следующей иерархии:

1) Данная политика ИБ является внутренним нормативным документом по ИБ первого (высшего) уровня.

2) Документами второго уровня являются – инструкции, порядки, регламенты и прочие документы описывающие действия сотрудников Организации по реализации документов первого и второго уровня.

3) Документами третьего уровня являются - отчётные документы о выполнении требование верхних уровней.

Ответственность за обеспечение ИБ

Для Департамента финансов и эффективного функционирования системы обеспечения информационной безопасности в Департаменте финансов, функции обеспечения ИБ возложены на ИТ отдел . На ИТ отдел возлагается решение следующих задач:

Определение требований к защите информации:

- определение требований к защите информации;
- организация мероприятий и координация работ всех отделов по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и используемых средств защиты информации;
- оказание методической помощи сотрудникам в вопросах соблюдения политики ИБ;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;
- информирование, обучение и повышение квалификации работников Организации в сфере информационной безопасности;
- расследования инцидентов информационной безопасности;
- сбор, хранение, систематизация и анализ информации по вопросам информационной безопасности;
- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений;
- обеспечивать корректную передачу данных сторонним организациям в безопасном режиме и с соблюдением всех аспектов политики ИБ;
- обеспечение передачи данных в соответствии с принятыми стандартами ЦБ РФ и Министерства финансов РФ.

Для решения задач, возложенных на ИТ отдел, его сотрудники имеют следующие права:

- получать информацию от пользователей информационных систем Департаменте финансов по любым аспектам применения ИТ в Департаменте финансов;
- участвовать в разработке технических решений направленных на обеспечение безопасности данных;
- контролировать деятельность пользователей по вопросам обеспечения ИБ;
- готовить предложения руководству по обеспечению требований ИБ.

Объект защиты, ответственность за ресурсы

В Департаменте финансов, все ресурсы, должны быть выявлены и оценены с точки зрения их важности. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Департамента финансов реализуется защита информации, степень которой соразмерна ценности и важности защищаемых ресурсов.

В ИС Департамента финансов присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Департамента финансов;
- информация находящаяся в открытом доступе, необходимая для работы Департамента финансов, независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого типа ресурсов должен быть назначен ответственный, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством Департамента финансов. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса.

Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

Оценка и обработка рисков

В Департаменте финансов должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями Департамента финансов. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков. Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков. Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения бизнес-требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;
- убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска Учреждение должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Департамента финансов. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике ИБ Департамента финансов и критериям принятия рисков;
- уклонение от риска путём недопущения действий, которые могут повлечь нарушение политики ИБ;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

Безопасность персонала

При трудоустройстве, трудоустраиваемому сотруднику должны быть доведены его права и обязанности по обеспечению безопасности информационных ресурсов, описанные в Политике ИБ Департамента финансов, и внесены в его должностные обязанности, должностную инструкцию. В инструктаж и должностную инструкцию должны входить как

общие обязанности по реализации и поддержке Политики ИБ Департамента финансов, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

Условия найма

Все принимаемые на работу сотрудники должны согласиться с возложенными на них обязанностями и подписать свои трудовые договоры, в которых устанавливается их ответственность за выполнение Политики ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Департамента финансов по проверке выполнения требований Политики ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть прописаны меры, которые будут приняты в случае несоблюдения сотрудником требований Политики ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника Департамента финансов.

Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, установленным уровнем доступа, с мерами ответственности за нарушение этого уровня.

При предоставлении сотруднику доступа к ИС Департамента финансов он должен ознакомиться под роспись с инструкцией пользователя ИС.

Ответственность руководства

Руководство Департамента финансов должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Департаменте финансов политиками и процедурами.

Уполномоченные руководством Департамента финансов сотрудники имеют право в установленном порядке, без предупреждения сотрудников, организовывать проверки:

- выполнения действующих инструкций по вопросам ИБ;
- данных, находящихся на носителях информации;
- порядка использования сотрудниками информационных ресурсов;
- содержания служебной переписки.

Обучение ИБ

Все сотрудники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в Департаменте финансов. Уполномоченные за поддержание

актуальности текущей политики ИБ, должны проходить курсы повышения квалификации в соответствующем направлении.

Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены, доступ полностью заблокирован. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

Физическая безопасность

Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Департамента финансов, должны быть размещены в защищённых местах. В качестве таких средств могут выступить: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.

Защищённые места расположения должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.

Запрещается приём/нахождение посетителей или неуполномоченных сотрудников в помещениях, когда осуществляется обработка информации ограниченного доступа. Помещения в которых хранится служебная информация, должны быть оборудованы электронным замком, например, кодовым, сигнализацией, камерами наблюдения, датчиками движения, температуры, влажности.

Для хранения конфиденциальных документов и съемных носителей с кинфиденциальной информацией помещения оборудуются сейфами, металлическими шкафами или шкафами, оборудованными замком.

Помещения должны быть обеспечены средствами уничтожения документов. Расположение таких помещений должно быть по возможности максимально защищено от природных катаклизмов (пожар, наводнение, землетрясение) и полностью закрыто от внешнего наблюдения.

Области общего доступа

Места доступа, через которые неавторизованные лица могут попасть в помещения Департамента финансов, должны контролироваться и, должны быть изолированы от помещений, в которых расположены средства обработки информации и хранилища особо

важной информации Департамента финансов, с целью предотвращения несанкционированного доступа.

Вспомогательные службы

Все вспомогательные службы, например электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать стабильную и по возможности бесперебойную работоспособность компонентов ИС Департамента финансов.

Утилизация или повторное использование оборудования

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях должно быть проверено уполномоченными сотрудниками ИТ отдела Департамента финансов, о чём должна быть сделана отметка в акте списания.

Перемещение имущества

Оборудование, информация или ПО должны перемещаться за пределы Департамента финансов только при наличии письменного разрешения руководства. Сотрудники, имеющие право перемещать оборудование и носители информации за пределы Департамента финансов должны быть чётко определены. Время перемещения оборудования за пределы Департамента финансов и время его возврата должны регистрироваться. При выносе имущества за пределы здания, охрана должна делать соответствующую пометку в отчётных документах.

Контроль доступа

Основными пользователями информации в информационной системе Департамента финансов являются сотрудники структурных подразделений. Права и уровень доступа каждого сотрудника определяется индивидуально. Каждый сотрудник пользуется только предписанным ему доступом и правами по отношению к информации, с которой ему необходимо работать в соответствии с должностной инструкцией.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения в составе уполномоченных лиц или пользователей, а так же полномочий сотрудников подсистем должны производиться в установленном порядке, в согласии с регламентом предоставления доступа пользователей.

Каждому пользователю, допущенному к работе с определённым информационным ресурсом Департамента финансов, должно быть определено уникальное имя (учётная запись пользователя), под которым он будет осуществлять вход в ИС. В случае производственной необходимости некоторым сотрудникам могут быть предоставлены несколько уникальных

учётных записей (логинов и паролей). При необходимости может быть создана временная учетная запись для пользователя или организации, представителя Департамента финансов, на определённый срок для выполнения задач, требующих расширенных полномочий, или для осуществления настройки, тестирования ИС, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и другим пользователям с временным доступом к ИС).

Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Регистрируемые учётные записи подразделяются на:

- пользовательские – предназначенные для аутентификации пользователей ИР;
- учреждения;
- системные – используемые для взаимодействия с операционной системой;
- служебные – предназначенные для обеспечения отдельных процессов или приложений.

Системные учётные записи формируются операционной системой и должны использоваться только в случаях, описанных в руководстве к операционной системы.

Служебные учётные записи используются только для функционирования сервисов или приложений.

Использование системных или служебных учётных записей для регистрации пользователей в системе строго запрещено. Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

- использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
- использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;
- предоставление и блокирование прав должны быть санкционированы и документированы;
- предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;
- регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Департамента финансов;

- уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
- согласование изменения прав доступа с отделом ИС СМТ;
- документальная фиксация назначенных пользователю прав доступа;
- ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
- предоставление доступа с момента завершения процедуры регистрации;
- немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Департамента финансов;
- аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
- обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;
- обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

Управление привилегиями

Доступ сотрудника к информационным ресурсам Департамента финансов должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий. Должны быть рассмотрены следующие этапы:

- должны быть идентифицированы права доступа, связанные с каждым системным узлом, например, с операционной системой, системой управления базой данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;
- привилегии должны передаваться сотрудникам на основании «производственной необходимости» и только на период времени, необходимый для достижения поставленных целей, например, привилегии, минимально

- необходимые для выполнения их функциональных обязанностей, только тогда, когда эти привилегии необходимы;
- должен быть обеспечен процесс санкционирования всех предоставленных привилегий и создание отчетов по ним, привилегии нельзя предоставлять до завершения процесса их регистрации;
- уникальные привилегии должны присваиваться на другой ID пользователя, не тот, который используется при обычной работе пользователя.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Департамента финансов осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно предоставляться в качестве официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- временные пароли должны выдаваться пользователю только после его идентификации;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;
- необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- необходимо изменять пароля пользователя не реже одного раза в 90 дней;
- для пользователей, с определенными полномочиями, необходимо установить средства проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, например, биометрических технологий.

Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо осуществлять официальный процесс периодической проверки прав доступа пользователей, отвечающий следующим требованиям:

- права доступа сотрудников должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;
- права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Департамента финансов, а также при переходе с одной работы на другую в пределах Департамента финансов;
- изменение привилегированных учетных записей должно протоколироваться.

Контроль над выполнением процедур управления доступом пользователей должен включать:

- проверку подлинности пользователей перед сменой паролей;
- немедленное блокирование прав доступа при увольнении;
- блокирование учётных записей, неактивных более 45 дней, а так же учетных записей сотрудников ушедших в декрет или отпуск;
- включение учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;
- отслеживание удалённых учётных записей, используемых поставщиками, во время работ;
- ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;
- использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;
- разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;
- блокирование учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором;

Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Департамента финансов предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации.

Не допускается использование различными пользователями одних и тех же учётных данных. Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности, после чего, пользователь устанавливает свой собственный пароль.

После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;
- для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

Сотрудник обязан:

- в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль исообщить о факте компрометации сотруднику отдела ИТ;
- немедленно сообщить сотруднику отдела ИС СМТ в случае получения от кого-либо просьбы сообщить пароль;
- менять пароль каждые 90 дней;
- менять пароль по требованию Администратора ИБ.

После 5 неудачных попыток ввода пароля учётная запись блокируется. Разблокировку осуществляет сотрудник ИТ отдела.

Пользовательское оборудование, оставляемое без присмотра

Сотрудники должны соблюдать необходимую защиту оборудования, оставляемого без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

Политика «чистого стола»

Сотрудники Департамента финансов обязаны:

- сохранять известные им пароли в тайне;
- осуществлять блокировку экрана при покидании рабочего места;
- по завершении сеанса выходить из системы;

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён.

Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.

Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги, например шредер, либо сжигаться в печах с пеплоуловителями.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

Мобильное компьютерное оборудование

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Организации. Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и в частности с работой в незащищённой среде.

Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

- при работе с ПО руководствоваться нормативной документацией (руководством пользователя);
- обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой

методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;

- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Департамента финансов.

Использование ПО

На АРМ Департамента финансов допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения. Запрещено незаконное хранение на жестких дисках информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке программного обеспечения, необходимого для реализации финансовых задач, административно-хозяйственных и других задач принимает руководитель Департамента финансов.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в ИТ отделе.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ Департамента финансов. Указанные работы, а так же работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками ИТ отдела.

Сведения о вновь приобретённом программном обеспечении должны быть внесены в перечень разрешённого программного обеспечения.

Использование АРМ и ИС

К работе в ИС Департамента финансов допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Каждому работнику Департамента финансов, которому предоставляется доступ к ИР в рамках его должностных обязанностей, выдаются под роспись необходимые средства.

Каждый сотрудник Департамента финансов, обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.

Работа в ИС сотрудникам разрешена только на закреплённых за ними АРМ, в определённое время и только с разрешенным программным обеспечением и сетевыми ресурсами.

Все АРМ, установленные в Департаментt финансов, имеют унифицированный набор программ, предназначенных для обработки и обмена данными, определённый в стандарте рабочих мест Департамента финансов. Изменение текущей конфигурации возможно после внесения необходимых поправок в стандарт рабочих мест или по служебной записке, согласованной ИТ отделом и руководителем ДФ.

Самостоятельная установка или удаление программного обеспечения на АРМ запрещена.

Сотрудники ИТ отдела имеют право осуществлять контроль над установленным на ПК программным обеспечением.

Передача документов внутри Организации производится только посредством общих папок, а также средствами электронной почты.

При работе в ИС Департамента финансов сотрудник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов Департамента финансов;
- использовать ИС и АРМ Департамента финансов исключительно для выполнения своих
- служебных обязанностей;
- ставить в известность ИТ отдел о любых фактах нарушения требований ИБ;
- ставить в известность ИТ отдел о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания ИТ отдел Организации;
- предоставлять АРМ сотрудникам ИТ отдел для контроля;
- при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- в случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом отдел ИС СМТ.

При использовании ИС Департамента финансов запрещено:

- использовать АРМ и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;

передавать:

- конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;
- информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
- угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Департамента финансов;

- предоставлять сотрудникам Департамента финансов (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в Реестр разрешенного к использованию ПО;
- защищать информацию, способами, не согласованными с ИТ отдел заранее;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Департамента финансов.

Все электронные сообщения и документы в электронном виде, обрабатываемые сотрудниками Департамента финансов подлежат обязательной проверке на наличие вредоносного ПО.

Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения применять средства защиты от неавторизованного доступа;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;

- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС.

Безопасность системных файлов

Чтобы свести к минимуму риск повреждения ИС, в учреждении необходимо обеспечить контроль над внедрением ПО в рабочих системах.

Тестовые данные должны находиться под контролем и защитой. Для испытаний обычно требуются значительные объёмы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы всё же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

Управление инцидентами информационной безопасности

В Организации должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учёта приоритетов Департамента финансов при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

Управление непрерывностью и восстановлением

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнес-процессов Департамента финансов. Данный процесс должен объединять в себе основные элементы поддержки непрерывности бизнес-процессов.

В Департаменте финансов должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес процессов.

В каждом плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Учреждения к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

В Департамента финансов должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация Департамента финансов должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований.

Система хранения и обработки должна обеспечивать чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Департамента финансов.

Криптографические средства должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

Аудит информационной безопасности

Учреждение должно проводить внутренние проверки СУИБ через запланированные интервалы времени.

Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

Руководство и сотрудники Департамента финансов при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

Предоставление услуг сторонним организациям

В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

Услуги, отчёты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

В Департаменте финансов должен быть разработан и утверждён порядок приёмки новых ИС, обновления и новых версий ПО.

Ответственность

Руководитель Департамента финансов определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Департамента финансов.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Департамента финансов лежит на руководстве отдела ИС СМТ.

Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

Сотрудники Департамента финансов несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ИС СМТ.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей.

Руководство Департамента финансов регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких

указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований нормативных актов Департамента финансов по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

Контроль и пересмотр

Общий контроль состояния ИБ Учреждения осуществляется Руководителем Департамента финансов.

Текущий контроль соблюдения настоящей Политики осуществляет отдел ИС СМТ. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Департамента финансов, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Отдел ИС СМТ ежегодно пересматривает положения настоящей политики. Изменения и дополнения вносятся по инициативе отдела ИС СМТ или Департамента финансов и утверждаются Директором.

Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесённые в настоящую Политику ИБ должны учитываться в листе «История изменений».