

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 100503 –

Специализация -

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНАЯ РАБОТА

на тему

МЕТОДИКА ИДЕНТИФИКАЦИИ И ОЦЕНКИ ВАЖНОСТИ
ИНФОРМАЦИОННЫХ АКТИВОВ ОРГАНИЗАЦИИ

Студент Николина Юлия Валерьевна
Руководитель Шумкин С.Н.
Нормоконтролёр Фатеев А.Г.
Рецензент - начальник отдела ООО «НПФ «Кристалл» Амиров А.И.

Работа допущена к защите (протокол заседания кафедры от 20.06.2016 № 14)

Заведующий кафедрой С.Л. Зефиров

Работа защищена с отметкой удовл. (протокол заседания ГЭК
от 23.06.16 № 6)

Секретарь ГЭК А.П. Иванов

Пенза 2016

Проверка ВКР – И. Б. Боров
С. Л. Зефиров

РЕФЕРАТ

Отчет 89с., 13 рис., 25 табл., 25 источников.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УГРОЗА, УЯЗВИМОСТЬ, ИНФОРМАЦИОННЫЙ АКТИВ, РИСК.

Объектом исследования является процесс идентификации и оценки важности информационных активов организации.

Цель работы – разработка методики идентификации и оценки важности информационных активов организации.

В ходе работы был проведен анализ стандартов и практик в области идентификации и оценки важности информационных активов организации. Были рассмотрены подходы и способы идентификации и оценки важности информационных активов организации при оценке рисков информационной безопасности. На основании полученных знаний была разработана методика идентификации и оценки важности информационных активов, которая определяет важность информационного актива на деятельность организации.

Также была выполнена проверка методики идентификации и оценки важности информационных активов.

СОДЕРЖАНИЕ

Введение.....	7
1 Анализ стандартов и практик в области оценки рисков ИБ, идентификации и оценки важности информационных активов	9
1.1 Общие сведения.....	9
1.2 Международный стандарт ISO/IEC 27005:2011.....	12
1.3 Международный стандарт ISO/IEC 27002:2013.....	13
1.4 Стандарт Банка России СТО БР ИББС-1.0-2014	14
1.5 Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009.....	15
1.6 Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007.....	15
1.7 Обзор существующих методик и лучших практик в области идентификации и оценки важности информационных активов организации.....	16
1.7.1 Общие подходы в области идентификации и оценки важности информационных активов организации	16
1.7.2 Методика CRAMM	19
1.7.3 Методика FRAP.....	21
1.7.4 Методика ГРИФ	22
1.7.5 Методика RiskWatch	24
2 Рассмотрение подходов и способов идентификации и оценки важности информационных активов организации при оценке рисков ИБ.....	27
2.1 Идентификация и определение важности информационных активов	27
2.2 Анализ уязвимостей активов	37
2.3 Анализ и оценка угроз информационной безопасности	37
2.4 Оценивание рисков информационной безопасности	42

3	Разработка методики идентификации и оценки важности информационных активов	43
4	Процесс идентификации и оценки важности информационных активов	54
5	Выполнение проверки методики идентификации и оценки важности информационных активов организации	60
5.1	Описание бизнес-целей и бизнес-функций, основных бизнес-процессов организации	60
5.2	Идентификация активов	62
5.3	Оценка важности информационных активов	63
	Заключение.....	87
	Список использованных источников.....	88

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете используются следующие термины с соответствующими определениями:

информационная безопасность – это состояние защищенности организации в условиях угроз в информационной сфере [1];

информационный актив – это все, что имеет ценность для организации и находится в ее распоряжении в информационной сфере [1];

угроза – степень возможности реализации опасности в информационной сфере [1];

уязвимость – слабое место в информационной сфере организации, которое может быть использовано для реализации угрозы информационной безопасности [1];

риск информационной безопасности – это потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимости актива или группы активов [1].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчете применяют следующие обозначения и сокращения:

БД - база данных;

БС РФ - банковская система Российской Федерации;

ИС - информационная система;

ИБ – информационная безопасность.

ВВЕДЕНИЕ

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски организации, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности организации.

Оценка важности информационных активов является начальным шагом в процессе управления информационными рисками.

В тоже время другим актуальным и динамично развивающимся направлением стратегического и оперативного менеджмента в области защиты информации является обработка инцидентов информационной безопасности, которая на сегодняшний день часто обсуждаема и актуальна для организации. Как показывают реальные жизненные примеры, необходимость своевременного выявления инцидентов и реагирования на них обусловлена в первую очередь тем, что зачастую на карту поставлены не только конфиденциальность, целостность и доступность информации, но также репутация и деньги, которых в одночасье может лишиться компания, не заметив инцидента, о котором сигнализировали средства защиты.

Оценка важности информационных активов также является начальным шагом обработки инцидентов ИБ.

Работа по определению ценности информационных активов в разрезе всей организации одновременно наиболее значима и сложна. Именно оценка информационных активов позволит начальнику отдела ИБ выбрать основные направления деятельности по обеспечению информационной безопасности. В первую очередь при проведении данной процедуры необходимо получить сведения об активах организации, используемых в ее повседневной деятельности. Ценность актива выражается величиной потерь, которые понесет организация в случае нарушения безопасности актива.

Целью процесса идентификации и оценки важности информационных активов является получение значений важности для выбранных активов организации. Результат этого процесса важен не только для проведения оценки рисков, но и для понимания руководством организации необходимости мероприятий в области ИБ.

В данной дипломной работе необходимо разработать методику идентификации и оценки важности информационных активов организации, которая позволяет автоматизировать действия по получению значений важности активов.

1 Анализ стандартов и практик в области оценки рисков ИБ, идентификации и оценки важности информационных активов

1.1 Общие сведения

Анализ отечественных и международных стандартов по информационной безопасности показывает, что в настоящее время оценка рисков занимает центральное место в системе управления информационной безопасностью. В российских и международных стандартах по информационной безопасности и нормативных документах государственных органов РФ определена необходимость проведения оценки рисков.

В стандарте ГОСТ Р ИСО/МЭК 27001 [2] определено, что организация должна создавать, внедрять, эксплуатировать и осуществлять мониторинг, анализировать, сопровождать и совершенствовать документированную систему управления ИБ в контексте общих бизнес активностей и рисков организации. А также: определять подход организации к оценке рисков, идентифицировать риски, анализировать и оценивать риски, идентифицировать и оценивать возможности по обработке рисков.

Однако методические указания по реализации процедур оценок не приведены, в связи с этим появляется необходимость каждому эксперту разрабатывать подход к решению поставленной задачи. В настоящее время существует достаточно большое количество нормативных документов по управлению рисками для предприятий. На основе лучших мировых практик создаются методики оценки рисков для различных областей применения, в том числе и для информационной безопасности. Данные методики позволяют правильно оценивать риски ИБ, что позволяет адекватно использовать ресурсы предприятия и настраивать защитные механизмы. Правильная и своевременная оценка рисков позволяет экономить материальные и физические ресурсы предприятия, что положительно сказывается на его деятельности.

Но при этом, нельзя не учитывать, что при построении системы информационной безопасности могут возникать проблемы, связанные с количеством рисков, которые необходимо минимизировать, так как перечень

рисков ИБ организации может оказаться довольно значительным. Для решения этой проблемы при идентификации и оценке рисков учитываются такие параметры, как угроза, уязвимости, а также инциденты ИБ, которые показывают негативные последствия угроз, которые были ранее реализованы. Угрозы могут исходить как от внешних источников, так и от внутренних. Уязвимости могут быть связаны с неэффективным управлением организацией, а также недостатками информационных систем. Оценивая риски таким образом можно получить перечень рисков, наиболее приоритетных при обработке, и вкладывать материальные и финансовые ресурсы в те процессы, где эти ресурсы действительно необходимы. Таким образом, только при помощи оценки рисков ИБ возможно спланировать и грамотно распределить ресурсы. Для обеспечения адекватности системы информационной безопасности текущему состоянию внешней среды необходимо производить периодическую переоценку рисков.

Важным источником информации при оценке рисков ИБ являются результаты обработки инцидентов ИБ. В ГОСТ Р ИСО/МЭК ТО 18044-2007 [3] отмечено, что анализ инцидентов ИБ повышает вероятность предотвращения будущих инцидентов, позволяет улучшить механизмы и процессы обеспечения информационной безопасности. В зависимости от серьезности инцидента ИБ, степени его воздействия, при оценке результатов анализа рисков ИБ и менеджмента ИБ, возможно, придется учитывать новые угрозы и уязвимости. В результате обновленного анализа рисков ИБ и анализа менеджмента ИБ может возникнуть необходимость внесения изменений в существующие защитные меры, а также необходимость применения новых защитных мер.

Взаимосвязь между процедурой обработки инцидентов, процессом анализа рисков может существенно повысить качество оценки рисков, угроз и уязвимостей и увеличить выгоду от использования процедуры обработки инцидентов. Информация о случаях возникновения угроз способна значительно улучшить качество оценки угрозы и, следовательно, качество оценки рисков. Процесс расследования инцидентов может предоставить новую

дополнительную информацию об уязвимостях и способах их устранения.

Применение результатов обработки инцидентов дает возможность пользователю идентифицировать и оценить уязвимости системы и предоставить полезные входные данные для оценки рисков.

Применение системы оценки рисков ИБ на основе результатов обработки инцидентов ИБ позволяет в некоторой степени автоматизировать процесс оценки рисков и учитывать новые угрозы и уязвимости, выявленные в процессе расследования инцидентов ИБ, сделать процесс оценки рисков ИБ наиболее эффективным и удобным при использовании. Именно поэтому возникает необходимость построения системы оценки рисков ИБ на основе результатов обработки инцидентов ИБ.

Анализ стандартов и лучших практик в области идентификации и оценки важности информационных активов организации позволяет разработать наиболее оптимальную методику оценки важности информационных активов организации. Для получения информации об идентификации и оценке важности информационных активов организации были рассмотрены следующие документы:

- международный стандарт ISO/IEC 27005: 2011: «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [4];

- международный стандарт ISO/IEC 27002: 2013: «Информационные технологии. Методы защиты. Свод рекомендуемых правил для управления информационной безопасностью» [5];

- стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» [6];

- рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [7];

- национальный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» [3].

1.2 Международный стандарт ISO/IEC 27005: 2011

Международный стандарт ISO/IEC 27005 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» предоставляет руководство по менеджменту риска информационной безопасности [4].

В вопросе об информационных активах организации данный стандарт представляет рекомендации по идентификации и определению ценности активов. В документе перечислены основные и вспомогательные активы, а также приведены их описания. Стандарт определяет общий порядок определения ценности активов в организации. Вначале должно быть принято решение о том, какую шкалу использовать: качественную или количественную. Данное решение является предпочтением организации. Далее выбираются критерии, используемые в качестве основы для присвоения ценности каждому активу. Критерии должны быть записаны в однозначных выражениях. Стандарт приводит примеры критериев, которые могут служить основой для определения ценности активов. После установления критериев для рассмотрения организация должна согласовать шкалу, которая будет использоваться в масштабах организации. Первым шагом является принятие решения о числе используемых уровней. Не существует правил, касающихся того, какое число уровней является наиболее уместным. Большее количество уровней обеспечивает больший уровень детализации, но иногда слишком тонкое разграничение затрудняет присвоение согласованных оценок в масштабе организации. Далее должны быть идентифицированы зависимости одних активов от других, поскольку это может влиять на ценность активов. Информация о зависимостях поможет в идентификации угроз и особенно уязвимостей. Кроме того, это поможет обеспечить уверенность в том, что

активам присваивается правильное значение ценности. Ценность активов, от которых зависят другие активы, может быть модифицирована. Окончательным результатом идентификации и определения ценности активов будет список активов и их ценности по отношению к раскрытию (сохранение конфиденциальности), модификации (сохранение целостности, подлинности, неотказуемости и учетности), недоступности и разрушению (сохранение доступности и надежности) и стоимости восстановления [4].

1.3 Международный стандарт ISO/IEC 27002: 2013

Международный стандарт ISO/IEC 27002 [5] предлагает практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности, определяет основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации.

В соответствии со стандартом оценка рисков должна включать в себя систематический анализ вероятного ущерба, наносимого бизнесу в результате нарушений информационной безопасности, вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также анализ внедренных мероприятий по управлению информационной безопасностью.

Результаты оценки рисков играют ключевую роль при определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрению мероприятий по управлению информационной безопасностью с целью минимизации этих рисков.

Также отмечено, что оценки рисков следует выполнять периодически, чтобы учитывать изменения в требованиях безопасности и в ситуации, связанной с риском, например, в отношении активов, угроз, уязвимостей, воздействий, оценивания рисков. Такие оценки рисков следует проводить методичным образом, способным обеспечивать воспроизводимые и сравнимые результаты.

1.4 Стандарт Банка России СТО БР ИББС-1.0-2014

Данный стандарт Банка России устанавливает требования для кредитных организаций, входящих в состав банковской системы Российской Федерации, к выбору и коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков нарушения информационной безопасности [6].

В организации БС РФ должны быть приняты, а также корректироваться в установленном порядке и по необходимости, методика оценки рисков нарушения ИБ и подход к оценке рисков нарушения ИБ. Кроме этого должны быть определены критерии принятия рисков и уровень допустимого риска нарушения информационной безопасности.

Методика оценки рисков и подход к оценке рисков нарушения информационной безопасности организации БС РФ должны определять и способ качественного или количественного оценивания рисков нарушения ИБ на основании оценивания:

- степени возможности реализации угроз ИБ выявленными или предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов организации БС РФ;
- степени тяжести последствий от потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности, для рассматриваемых информационных активов.

Полученные в результате оценивания рисков нарушения ИБ величины рисков должны быть соотнесены с уровнем допустимого риска, принятого в организации БС РФ. Результатом выполнения указанной процедуры является документально оформленный перечень недопустимых рисков нарушения ИБ.

В организации БС РФ должны быть документально определены роли по оценке рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

1.5 Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009

Данная методика устанавливает рекомендуемые способы и порядок проведения оценки рисков нарушения информационной безопасности организации банковской системы Российской Федерации, являющейся составной частью системы менеджмента ИБ организации БС РФ [7].

Настоящая методика рекомендована для применения путём использования устанавливаемых в ней положений при проведении оценки рисков нарушения информационной безопасности. В конкретной организации БС РФ для проведения оценки рисков нарушения информационной безопасности могут использоваться иные методики, соответствующие требованиям стандарта Банка России СТО БР ИББС-1.0-2014 [6].

Результаты использования методики РС БР ИББС-2.5-2014 и иных методик оценки рисков нарушения информационной безопасности имеют равное значение при построении системы обеспечения информационной безопасности организации банковской системы Российской Федерации.

1.6 Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007

В настоящем стандарте содержатся рекомендации по менеджменту инцидентов ИБ в организациях для руководителей подразделений по обеспечению информационной безопасности при применении информационных технологий, информационных систем, сервисов и сетей.

Менеджмент инцидентов ИБ подразделяют на четыре отдельных этапа: планирование и подготовка, использование, анализ и улучшение. В стандарте приведены подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса менеджмента инцидентов ИБ. Основное содержание этапов менеджмента инцидентов ИБ приведено на рисунке 1.1.

В данном стандарте определено, что на этапе улучшения осуществляется реализация рекомендаций по улучшению процессов обеспечения ИБ и реагирования на инцидент. Таким образом, что результаты обработки

инцидентов ИБ оказывают непосредственное влияние на оценку рисков, реализуемую в дальнейшем. Возникновение инцидентов ИБ обуславливает необходимость учитывать новые угрозы и уязвимости при повторной оценке рисков ИБ и, как следствие, в результате завершения обновленного анализа рисков ИБ и анализа менеджмента ИБ может возникнуть необходимость внесения изменений в существующие защитные меры.

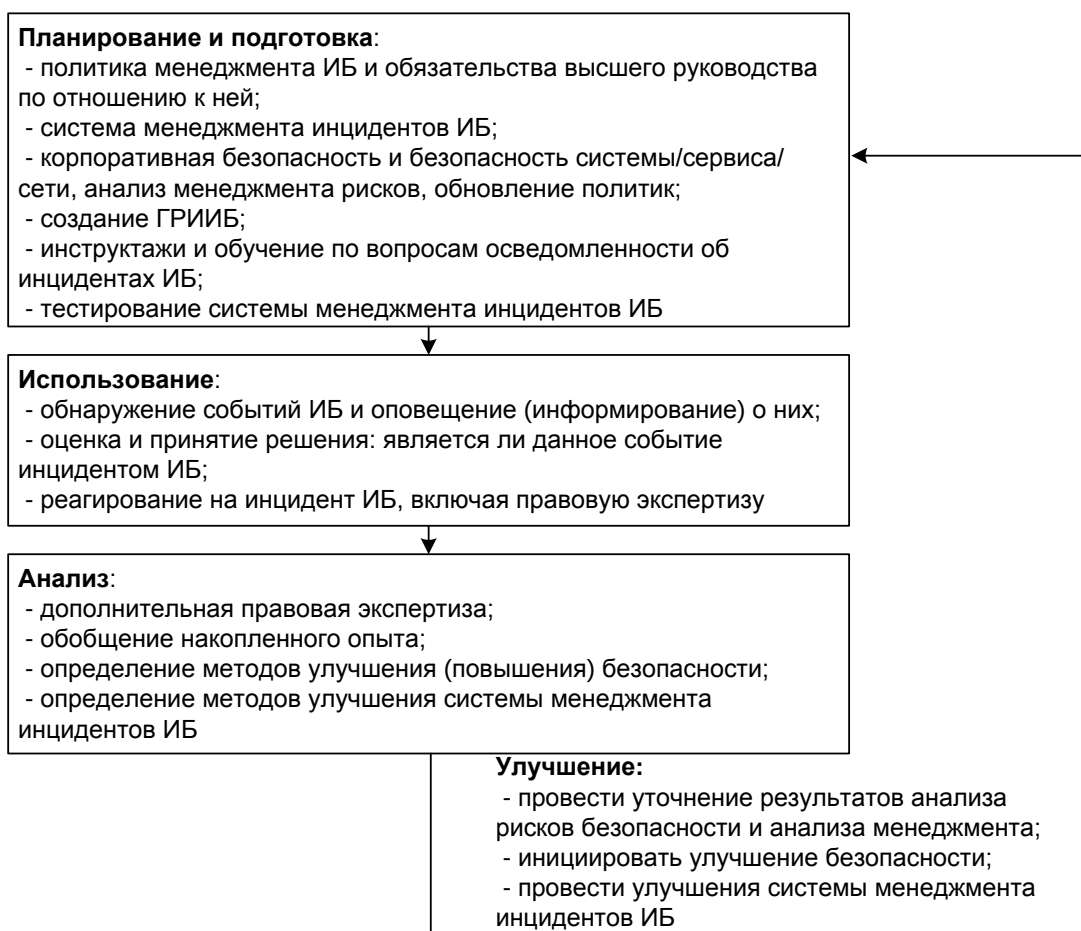


Рисунок 1.1 – Этапы менеджмента инцидентов информационной безопасности

1.7 Обзор существующих методик и лучших практик в области идентификации и оценки важности информационных активов организации

1.7.1 Общие подходы в области идентификации и оценки важности информационных активов организации

Во всех подходах к управлению рисками суть состоит в оценке их размера, выработке эффективных и экономичных мер их снижения, а также в

установлении приемлемых рамок для них. Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- оценка рисков;
- выбор эффективных и экономичных защитных средств.

Процесс управления рисками можно разделить на следующие этапы:

- выбор анализируемых объектов и уровня детализации их рассмотрения;
- выбор методологии оценки рисков;
- идентификация активов;
- анализ угроз и их последствий, выявление уязвимых мест в защите;
- оценка рисков;
- выбор ответных мер;
- реализация и проверка выбранных мер;
- оценка остаточного риска.

От последнего этапа в случае неприемлемости остаточного риска происходит возврат к началу [8].

Во многих методиках предлагаются различные способы сопоставления возможных последствий реализации угрозы с вероятностью ее реализации и получения соответствующих выводов, которые могут быть качественные, количественные и смешанные.

При этом количественные методы имеют такой недостаток, как недостаток точных данных, статистики инцидентов, но в отличие от качественных методов позволяют получить наиболее точную оценку рисков.

Классические вероятностно-статистические методы предназначены для описания повторяющихся экспериментов, проводимых в стабильных условиях. В большинстве методов количественной оценки риска используется среднее значение ущерба.

Конечной стадией оценки является принятие решения о достаточности используемых мер и средств защиты или об их недостаточности. В последнем случае, как было показано выше, предлагаются дополнительные меры, и оценка повторяется. В конечном счете, от процедуры оценки рисков требуется дать

ответ, является ли приемлемым остаточный риск, а не числовой параметр со сколькими-то значащими цифрами.

Существуют специализированные программные обеспечения, реализующие методики анализа рисков. Такое программное обеспечение должно быть в достаточной степени универсальным. Предлагаемое на рынке программное обеспечение ориентировано в основном на уровень информационной безопасности, несколько превышающий базовый уровень защищенности. Для решения задачи оценки рисков существуют комплексы анализа и контроля рисков информационной безопасности: CRAMM, FRAP, RiskWatch, ГРИФ.

Эти методики можно разделить на:

- методики, использующие оценку риска на качественном уровне. К таким методикам, в частности, относится FRAP;
- количественные методики, где риск оценивается через числовое значение, например размер ожидаемых годовых потерь. К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки, такой подход используется в CRAMM, методике ГРИФ [9].

В области обработки инцидентов ИБ основополагающей является необходимость реализовать комплексный подход к решению следующих задач:

- обнаружение, информирование и учет ИБ;
- реагирование на инциденты ИБ, применение необходимых средств для предотвращения, уменьшения и восстановления нанесенного ущерба;
- анализ произошедших инцидентов, целью которого является планирование превентивных мер защиты, улучшения процесса обеспечения ИБ в целом.

В настоящее время в международной практике разработано достаточное количество нормативных документов, регламентирующих вопросы управления инцидентами информационной безопасности. Согласно данным семейства международных стандартов под инцидентом понимается любое событие, не являющееся элементом нормального функционирования службы и при этом

оказывающее или способное оказать влияние на предоставление службы путем ее прерывания или снижения качества.

1.7.2 Методика CRAMM

Основу методики CRAMM составляет комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным, он подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний:

- коммерческий профиль;
- правительственный профиль.

Концептуальная схема проведения обследования по методу CRAMM показана на рисунке 1.2.

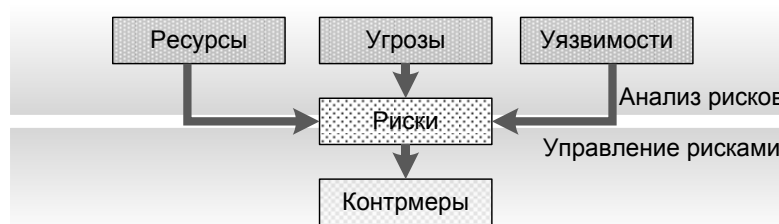


Рисунок 1.2 - Концептуальная схема проведения обследования по методу CRAMM

На первых этапах работы методики учитывается ценность ресурсов исследуемой системы, собираются первичные сведения о конфигурации системы. Проводится идентификация ресурсов: физических, программных и информационных, содержащихся внутри границ системы.

Результатом этого этапа является построение модели системы, с деревом связи ресурсов. Эта схема позволяет выделить критичные элементы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в следующих ситуациях:

- недоступность ресурса в течение определенного периода времени;

- разрушение ресурса;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация;
- ошибки, связанные с передачей информации [10].

Далее рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы. На этой стадии оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты.

Следующая стадия исследования заключается в поиске адекватных контрмер, представляющий собой поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

Таким образом, CRAMM является методикой расчета, при которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке.

К недостаткам метода CRAMM можно отнести следующее:

- аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;
- использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;
- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся;
- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;
- возможность внесения дополнений в базу знаний CRAMM недоступна

пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации;

- высокая стоимость лицензии.

1.7.3 Методика FRAP

В методике FRAP, обеспечение ИБ предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере ИБ – процесс, позволяющий компаниям найти баланс между затратами на средства защиты и получаемым эффектом.

Управление рисками начинается с оценки рисков. Результаты оценки являются основой для принятия решений в области повышения безопасности системы. После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта, который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня.

Составление списка угроз поможет использовать разные подходы:

- заранее подготовленные экспертами перечни угроз, из которых выбираются актуальные для данной системы;
- анализ статистики происшествий в данной ИС происходит оценка частоты их возникновения; по ряду угроз;
- «мозговой штурм», проводимый сотрудниками компании [11].

Когда список угроз закончен, каждой из них сопоставляют вероятность возникновения. После чего оценивают ущерб, который может быть нанесен данной угрозой. Исходя из полученных значений, оценивается уровень угрозы. Таким образом оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации.

После идентификации угроз и получения оценки риска, определяются контрмеры, позволяющие устранить риск или снизить его до приемлемого уровня. При этом должны приниматься во внимание законодательные ограничения, делающие невозможным или, наоборот, предписывающие в обязательном порядке использование тех или иных средств и механизмов

защиты. Если риск снижен недостаточно, следует, возможно, применить другую систему защиты информации. Вместе с определением средства защиты, надо определить какие затраты повлечет его приобретение и внедрение. Кроме того, необходимо оценить, безопасно ли само это средство, не создает ли оно новых уязвимостей в системе.

Нужно проводить анализ соотношения затрат и получаемого эффекта, чтобы использовать экономически эффективные средства защиты. При этом надо оценивать не только стоимость приобретения решения, но и стоимость поддержания его работы.

Заключительным этапом в этой методике является документирование. Когда оценка рисков закончена, ее результаты должны быть подробно документированы для дальнейшего использования или для проведения более глубокого анализа [12].

Таким образом, в методике производится анализ затрат и полученного эффекта от применения средства защиты информационной системы предприятия, она позволяет снизить риск до приемлемого уровня, таким образом, избежать максимальных затрат на обеспечение безопасности современными средствами ИБ. Принимаются законодательные ограничения, делающие невозможным или, наоборот, предписывающие в обязательном порядке, использование тех или иных средств и механизмов защиты.

1.7.4 Методика ГРИФ

Для проведения полного анализа информационных рисков, прежде всего, необходимо построить полную модель информационной системы с точки зрения ИБ это позволяет сделать методика ГРИФ. Основная задача методики ГРИФ – дать возможность оценить уровень рисков информационной безопасности в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании [13].

На первом этапе методики ГРИФ проводится опрос, определяющий полный список информационных ресурсов, представляющих ценность для компании.

На втором этапе определяются все виды информации, представляющие ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на ранее указанных на предыдущем этапе объектах хранения информации. Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

В начале третьего этапа проходит определение всех видов пользовательских групп. Затем определяется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды и права доступа пользователей ко всем ресурсам, содержащих ценную информацию.

На четвертом этапе проводится опрос, определяющий средства защиты информации, которыми защищена ценная информация на ресурсах. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также – ежегодные затраты на сопровождение системы информационной безопасности компании [14].

На завершающем этапе пользователь должен ответить на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

В результате выполнения всех действий по данным этапам, на выходе формируется полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета. Отчет представляет собой подробный, дающий полную картину возможного ущерба от инцидентов документ, готовый для представления руководству компании.

К недостаткам ГРИФ можно отнести:

- отсутствие привязки к бизнес-процессам;
- нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению безопасности;
- отсутствует возможность добавления специфичных для определенной компании требований политики безопасности.

1.7.5 Методика RiskWatch

Компания RiskWatch разработала собственную методику анализа рисков и семейство программных средств, в которых она в той либо иной мере реализуется. Семейство RiskWatch состоит из программных продуктов:

- RiskWatch for Physical Security - для анализа физической защиты ИС;
- RiskWatch for Information Systems - для информационных рисков;
- HIPAA-WATCH for Healthcare Industry - для оценки соответствия требованиям стандарта HIPAA, актуальных в основном для медицинских учреждений, работающих на территории США;
- RiskWatch RW17799 for ISO 17799 - для оценки соответствия ИС требованиям стандарта международного стандарта ISO 17799.

RiskWatch используется в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

Первый этап - определение предмета исследования. Здесь описываются параметры: как тип организации, состав исследуемой системы, базовые требования в области безопасности. Для облегчения работы аналитика, в шаблонах, соответствующих типу организации («коммерческая информационная система», «государственная / военная информационная система» и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз,

уязвимостей и мер защиты. И выбираются категории потерь, присутствующие в организации:

- задержки и отказ в обслуживании;
- раскрытие информации;
- прямые потери (например, от уничтожения оборудования огнем);
- жизнь и здоровье (персонала, заказчиков и т.д.);
- изменение данных;
- косвенные потери (например, затраты на восстановление);
- репутация.

Второй этап - ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. Подробнейшим образом описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Также задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Если для выбранного класса угроз в системе есть среднегодовые оценки возникновения, то используются они. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.

Третий этап - количественная оценка риска. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. SAFE (Standard Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в этой «части мира» (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Четвертый этап - генерация отчетов. Типы отчетов:

- краткие итоги;
- полные и краткие отчеты об элементах, описанных на стадиях 1 и 2;
- отчет от стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз;
- отчет об угрозах и мерах противодействия;
- отчет о ROI;
- отчет о результатах аудита безопасности.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Недостатки методики RiskWatch:

- методика RiskWatch подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов;
- полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций - метод не учитывает комплексный подход к информационной безопасности;
- программное обеспечение RiskWatch существует только на английском языке;
- высокая стоимость лицензии.

Методика RiskWatch позволяет разделить информационные системы на несколько профилей и уже использовать конкретизированную систему для учета рисков информационной безопасности предприятия, что очень удобно в современное время.

2 Рассмотрение подходов и способов идентификации и оценки важности информационных активов организации при оценке рисков ИБ

2.1 Идентификация и определение важности информационных активов

В результате идентификации активов должны быть рассмотрены все активы в рамках определённых на этапе установления контекста оценки границ и области оценки рисков ИБ. Для выполнения этой задачи целесообразно использовать описание объекта оценки, полученное при установлении границ и области оценки рисков ИБ, а также опись основных и вспомогательных активов организации.

Основной целью идентификации активов является определение наиболее важных с точки зрения целей деятельности организации информационных активов, а также вспомогательных активов, обеспечивающих надлежащие сбор, обработку и хранение таких активов, которые в свою очередь помимо собственной стоимости как имущества организации имеют ценность как средство обработки более ценного информационного актива. Оценка важности идентифицированных активов может проводиться в рамках процесса оценки рисков, однако часто рассматривается и реализуется как самостоятельный процесс, результаты которого несут ценную информацию для руководства и службы безопасности организации.

Для каждого информационного актива определяется его тип, бизнес-процесс, в котором он участвует, используемое техническое средство, подразделение, в котором данный актив обрабатывается. С помощью определения влияния различных факторов на информационных актив вычисляются соответствующие значения оценки важности.

Результатом организации данного процесса является сформированный перечень активов, оцененных с точки зрения их важности для организации и классифицированных по их возможным типам.

Прежде чем получить исходные данные для идентификации и оценки активов, необходимо определить границы рассмотрения. Место процесса

идентификации и оценки важности информационных активов в модели менеджмента рисков информационной безопасности можно увидеть на рисунке 2.1.

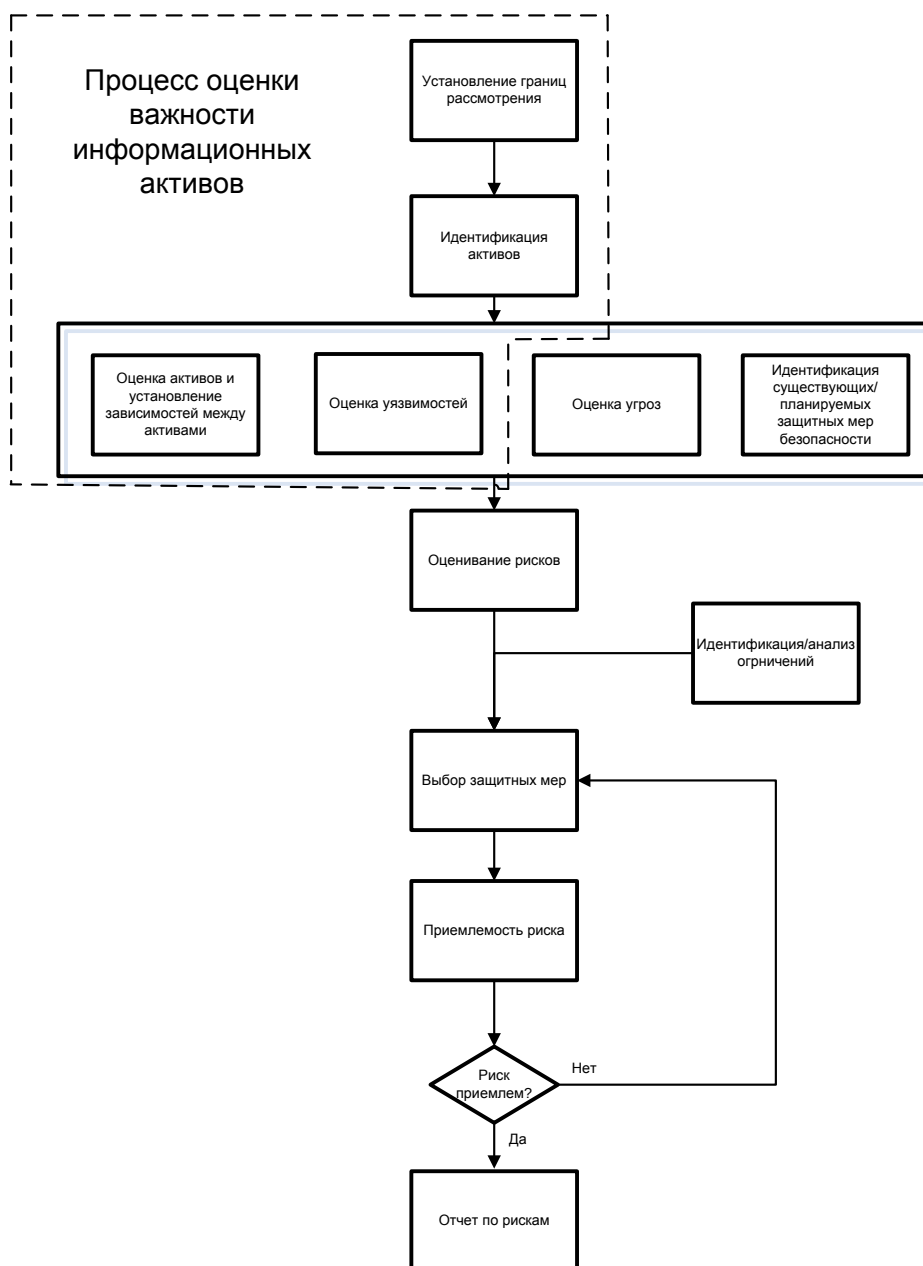


Рисунок 2.1 - Место оценки важности в модели менеджмента ИБ

Тщательное определение границ на этой стадии анализа риска позволяет избежать ненужных операций и повысить качество анализа риска. Установление границ рассмотрения должно четко определить, какие из перечисленных ниже ресурсов должны быть учтены при рассмотрении

результатов анализа риска. Для конкретной системы информационных технологий учитывают:

- активы информационных технологий (например, аппаратные средства, информационное обеспечение, информация);
- служащих (например, персонал организации, субподрядчики, персонал сторонних организаций);
- условия осуществления производственной деятельности (например здания, оборудование);
- деловую деятельность (операции)[15].

Оценка активов организации является важным этапом в общем процессе идентификации и оценки риска ИБ и вообще в системе менеджмента риска организации.

Для того, чтобы выполнить оценку активов организации, в первую очередь нужно определить область оценки важности информационных активов и идентифицировать все активы организации, а затем приступить к оцениванию важности. Графическое представление процесса оценки важности, представлено на рисунке 2.2.



Рисунок 2.2 - Процесс оценки важности информационных активов

Существует 4 разных подхода к оценке рисков ИБ:

- базовая ОР;
- неформальная ОР;

- детальная ОР;
- комбинированная ОР, состоящая из комбинации базовой, неформальной или детальной ОР.

При базовой оценке рисков используется единый подход ко всем системам и компонентам АС. Эта ОР используется в том случае, если организация не может или не считает нужным тратить время и средства к выбору защитных мер без предварительных оценок. Возможны 2 способа применения базовой ОР:

- выбор защитных мер в соответствии с типом и характеристиками рассматриваемой системы;
- выбор защитных мер в соответствии с целями, политиками и угрозами ИБ.

Базовые защитные меры могут быть определены в различных каталогах защитных мер.

Каталоги могут определять сами защитные меры или они могут определять множество требований ИБ которые должны быть выполнены с помощью каких-либо защитных мер подходящих для данной системы.

Достоинства: требуются минимальные ресурсы для выбора и реализации защитных мер.

Недостатки: если базовый уровень установлен слишком высоким, то для некоторых систем уровень может быть чрезмерным и соответственно наоборот.

Таким образом, если все активы имеют примерно одинаковые требования по значимости и по практичности воздействия угроз то базовый подход наиболее эффективен.

Неформальная оценка рисков основана на использовании знания и опыта отдельных лиц.

Достоинства: минимальный расход ресурсов и времени.

Недостатки: высокая вероятность того что не будут учтены некоторые аспекты обеспечения ИБ, возможность возникновения проблем по обеспечению ИБ, если лицо, проводившее оценку рисков, уходит из организации, на оценку

рисков ИБ сильно влияет субъективность подхода разработчика и его предпочтения.

Неформальная оценка рисков не является эффективным подходом для многих организаций и систем.

Детальная оценка рисков.

Достоинства: адекватность защитных мер защищаемым активам.

Недостатки: значительное время и ресурсы, затрачиваемые на реализацию.

Процессы детальной оценки рисков:

- определение области применения и границ оценки рисков ИБ;
- определение ценности активов;
- анализ и оценка угроз ИБ;
- анализ и оценка уязвимостей ИБ;
- анализ и оценка существующих защитных мер;
- качественное или количественное оценивание рисков ИБ.

Для определения границ оценки необходимо учитывать следующие элементы:

- особенности организации (опр. через цели особенности бизнеса и структуру организации);
- корпоративную политику;
- ограничения, влияющие на организацию (стратегические, территориальные экономические, структурные, функциональные, бюджетные);
- правовые, регулирующие и договорные требования;
- архитектура АС.

Для определения ценности активов необходимо определить критерии и шкалу. Критерии следующие:

- критерии оценивающие активы с точки зрения последствий и расходов, связанные с потерей конфиденциальности, целостности, доступности, неотказуемости;

- критерии на основе оценки исходной стоимости активов, стоимости замены активов, оценке абстрактной ценности (репутация).

Цель анализа и оценки угроз ИБ – источники случайных и преднамеренных угроз, сами угрозы. Должна быть определена вероятность их реализации и произведена оценка угроз.

Анализ и оценка уязвимостей ИБ включает определение слабостей в физической среде организации, уязвимостях сотрудников, уязвимостей в управлении, аппаратных и программных средств и т.д., которые могут быть использованы источниками угроз, чтобы причинить ущерб бизнесу или деятельности организации. Уязвимость, которая не имеет соответствующей угрозы, не требует реализации защитной меры, но должна быть идентифицирована и находиться под постоянным контролем [16].

Результатом этого этапа детальной оценки риска должны быть перечень уязвимости и оценки возможности их исполнения.

Анализ и оценка существующих защитных мер включает определение слабостей физической среды организации, АС, среды сотрудников, программных средств, которые могут быть использованы угрозами, в результате которых будет нанесен ущерб. Уязвимости, не имеющие соответствующих угроз, не требуют реализации защитных мер.

Защитные меры применяются для снижения риска ИБ до приемлемого уровня. Способы выбора защитных мер:

- предотвращение рисков. В этом случае отказываются от планируемой или существующей деятельности, если в ней есть риски;
- перенос рисков. Означает перенос риска на другие стороны (страховая компания, обработка информации в каком - либо центре информатизации);
- снижение рисков снижением угроз и уязвимостей. Межсетевые экраны.

При выборе защитных мер должны быть учтены функциональные характеристики защитных мер:

- простота применения защитных мер;
- прозрачность для пользователя;

- относительная стойкость защитных мер;
- типы выполняемых функций защитных мер.

Также необходимо учесть ограничения:

- временные, т.е. мера должна быть реализована в заданные временные рамки;
- финансовые, т.е. стоимость защитной меры не должна превышать ущерб;
- технические, т.е. меры должны быть связаны с совместимостью программных и аппаратных средств;
- социологические, т.е. необходимо учитывать уровень образования и специфику региона;
- юридические, т.е. необходимо учитывать текущие законы;
- ограничения среды, т.е. нужно учитывать климат, инфраструктуру и т.д.

Защитные меры будут выбираться по результатам ОР, как правило выбранные защитные меры являются дополнительными к уже существующим. Выбранные защитные меры не должны дублировать существующие. Если существующие неэффективны – их нужно заменить.

Оценка высокого уровня позволяет определять приоритеты и хронологию в действиях. По различным причинам, таким как бюджет, это может быть не возможным для одновременного осуществления всех контролей и только к самым критическим рискам можно обратиться через процесс обработки риска. Также, может быть преждевременным начало детализированного менеджмента рисков, если реализация предусмотрена только один или два года. Чтобы достигнуть этой цели, оценка высокого уровня может начаться с оценки последствий высокого уровня вместо того, чтобы начинать с систематического анализа угроз, уязвимости, активов и последствий [17].

Другая причина начинать с оценки высокого уровня состоит в том, чтобы синхронизироваться с другими планами, связанными с изменением менеджмента или непрерывностью бизнеса. Например, это не является нормой к полностью безопасной системе или приложению, если запланировано

произвести это на стороне в ближайшем будущем, хотя может все еще стоит делать оценку риска, чтобы определить производящийся на стороне контракт. Особенности итерации оценки риска высокого уровня описаны далее.

Оценка риска высокого уровня может обратиться к более глобальному представлению организации и ее информационных систем, рассматривая аспекты технологии как независимые от проблем бизнеса. Делая это, контекстный анализ концентрируется больше на эксплуатационной и бизнес среде, чем технологических элементах.

Оценка риска высокого уровня может обратиться к более ограниченному перечню угроз и уязвимостей, группированных в определенных доменах или ускорить процесс, она может сосредоточиться на риске или на сценарии вместо их элементов.

Риски, представленные в оценке рисков высокого уровня, часто являются более общими доменами риска, чем определенными идентифицированными рисками. Поскольку сценарии или угрозы группированы в доменах, обработка рисков предлагает перечни контролей в этом домене. Тогда сначала пытаются предложить действия обработки риска и выбрать общий менеджмент, который проходит через целую систему.

Тем не менее, наиболее соответствующее обеспечить менеджмент организационных и нетехнических контролей и технические аспекты менеджмента контролей, таких как резервное копирование и антивирусная защита для оценки риска высокого уровня или уровня общих технических гарантий, если это редко обращено к подробностям технологий.

Преимущества оценки риска высокого уровня следующие:

- начальное объединение простых подходов, вероятно, получит принятие программой оценки риска;
- это должно быть, возможно, чтобы построить организационно стратегический имидж программы информационной безопасности, то есть это будет действовать как хорошая помощь в планировании;

- могут быть применены ресурсы и деньги, где они, вероятно, самые выгодные, и к системам для обращения сначала к самым большим потребностям защиты.

Поскольку начальные исследования риска на высоком уровне потенциально менее точны, так как потенциальный недостаток – это то, что некоторые бизнес-процессы или требования системы не могут быть детально идентифицированы за короткое время оценкой риска. Этого можно избежать, если есть адекватная информация относительно всех аспектов организации ее информации и системы, включая информацию, полученную от оценки информационных инцидентов безопасности.

Оценка риска высокого уровня рассматривает бизнес значения информационных активов и риски с точки зрения бизнеса организации. Существует несколько критериев, которые помогают в определении, адекватна ли оценка высокого уровня в обработке риска; эти критерии могут включать следующее:

- бизнес цели, которые будут достигнуты при использовании различных информационных активов;

- уровень каждого информационного актива, от которого зависит бизнес организации, то есть, зависят функции, которые организация считает важным по отношению к ее выживанию или эффективному ведению бизнеса от каждого актива или от конфиденциальности, целостности, доступности, от возможности отказа от авторства, наблюдаемости, подлинности, надежности информации, хранящейся и обрабатываемой на этом активе;

- уровень инвестиций в каждом информационном активе в терминах разработки, поддержания или замены актива, и информационные активы, для которых организация непосредственно определяет значение.

Решение становится более простым, когда оценены эти критерии. Если цели актива чрезвычайно важны для поведения бизнеса организации или если активы находятся в области высокого риска, то должна быть проведена вторая итерация детальной оценки риска для специфического информационного

актива или части его. Применяется общее правило: если нехватка информационной безопасности может привести к существенным неблагоприятным последствиям в организации, ее бизнес-процессам или ее активам, то необходима вторая итеративная оценка риска на более детальном уровне, чтобы идентифицировать потенциальные риски.

Процесс подробной оценки риска информационной безопасности вовлекает всестороннюю идентификацию и оценку активов, оценку угроз этим активам и оценку уязвимости. Чтобы оценить риски и затем идентифицировать обработку риска используются следствия этих действий. Шаг детальной оценки обычно требует большого количества времени, усилия и экспертизы, и может, поэтому быть самым подходящим для информационных систем с высоким риском [18].

Конечная стадия оценки риска информационной безопасности должна подробно оценить полные риски, которые является основой этого приложения.

Последствия могут быть оценены несколькими способами, включая использование количественных, например денежно-кредитных и качественных мер, которые могут быть основаны на использовании таких прилагательных как умеренные или серьезные, или комбинации обоих. Чтобы оценить вероятность осуществления угрозы должен быть установлен период времени, в течение которого актив будет иметь определенное значение или должен быть защищен.

Вероятность появления определенной угрозы вызывается следующим:

- привлекательностью актива или возможностью применить воздействия, когда рассматривают преднамеренную человеческую угрозу;
- вероятностью преобразования уязвимости, эксплуатирующей актив, применимой к вознаграждению, если рассматривают преднамеренную человеческую угрозу;
- техническими возможностями агента угрозы, применяемого, чтобы обдумать человеческие угрозы, и восприимчивостью уязвимости к эксплуатации, применительно к технической и к нетехнической уязвимости.

Много методов используют таблицы и комбинируют субъективные и эмпирические меры. Важно, чтобы организация использовала метод, с которым удобно и в котором она уверена и что это приведет к ожидаемым результатам.

2.2 Анализ уязвимостей активов

Идентификация уязвимостей ИБ актуальных активов организации включает определение слабостей в физической среде организации, в автоматизированных системах, аппаратном и программном обеспечении, процедурах, слабостей персонала, управленческих ошибок.

Идентификация уязвимостей ИБ активов осуществляется на основе результатов обработки инцидентов ИБ. В процессе идентификации уязвимостей активов для каждого актива определяется перечень существующих уязвимостей. Источником данных о существующих уязвимостях являются результаты обработки инцидентов, в которых были определены уязвимости, использованные для реализации угрозы ИБ. На основании мнения экспертов это данные могут быть дополнены и другими, выявленными уязвимостями. Для каждого актива указывается одна или несколько характерных для него уязвимостей. В результате должен быть составлен перечень активов и их уязвимостей [19].

Оценка уязвимости зависит от наличия угрозы, которая могла бы использовать данную уязвимость для своей реализации, и от существующих защитных мер, направленных на устранение возможности использования уязвимости для реализации угрозы. Именно поэтому оценка уязвимости определяется совместно с процессом анализа угроз.

2.3 Анализ и оценка угроз информационной безопасности

Угроза обладает потенциалом причинения вреда активам, таким, как информация, процессы и системы, а, следовательно, и самой организации. Угрозы могут быть различного происхождения: природного, техногенного или антропогенного; могут носить преднамеренный или случайный характер. При идентификации должны быть учтены все возможные источники угроз активам.

Используемыми данными для идентификации угроз информационной

безопасности, актуальных для идентифицированных активов, являются:

- перечень активов, оцененных с точки зрения их важности для организации и классифицированных по их возможным типам;
- перечень типовых угроз информационной безопасности объекта защиты;
- перечень угроз, зафиксированный в результате обработки инцидентов ИБ;
- относительная частота реализации угроз, зафиксированных в результате обработки инцидентов;
- перечень уязвимостей, имеющих место у активов объекта оценки и являющихся для них потенциально опасными;
- информация о существующих защитных мерах;
- информация об источнике угрозы [20].

Эксперты совместно с владельцами и/или пользователями активов для идентификации угроз ИБ активов объекта оценки выполняют следующие действия:

- для каждого идентифицированного актива, входящего в состав объекта оценки указываются угрозы, которые могут нарушить актуальные свойства безопасности активов объекта оценки, то есть являются потенциально опасными для объекта оценки;
- для каждой угрозы определяется один или несколько потенциальных источников, причем, для источника антропогенного характера применяются формальная модель нарушителя;
- указывается метод реализации угрозы, доступный источнику угрозы и сложность обнаружения реализации угрозы;
- выбирается одна или несколько уязвимостей рассматриваемого актива, пригодных для реализации угрозы;
- указываются соответствующие защитные меры;

- для защитной меры указывается её влияние на возможность реализации угрозы и возможность использования соответствующей уязвимости.

При рассмотрении угрозы ИБ, выявленной на основании результатов обработки инцидентов ИБ, для неё рассчитывается относительная частота реализации. Для этого определяется общее количество инцидентов ИБ, в которых были выявлены все зафиксированные угрозы ИБ. Затем определяется количество инцидентов ИБ, в которых была зафиксирована рассматриваемая угроза. Относительная частота реализации рассматриваемой угрозы определяется соотношением количества инцидентов, соответствующих данной угрозе, к общему количеству инцидентов. Относительная частота реализации угрозы и результаты обработки инцидентов, соответствующих этой угрозе, позволяют определить актуальность рассматриваемой угрозы [21].

В процессе анализа угроз также осуществляется анализ и оценка защитных мер, а также оценка уязвимостей.

Для количественной оценки вероятности угроз необходимо иметь формальную модель нарушителя, предусматривающую различные возможности нарушителя по доступу к информационным ресурсам и по техническим возможностям реализации угроз. Источником угроз в формальной модели является внешний или внутренний субъект, получивший некоторые возможности доступа к сети со штатными средствами автоматизированной системы и средств вычислительной техники, имеющий определенный уровень знаний в области эксплуатации и защиты.

Представленная ниже формальная модель нарушителя предусматривает пять уровней этих возможностей.

Первый уровень – отсутствие полномочий доступа к ресурсам корпоративной сети. Нарушитель первого уровня не располагает именами зарегистрированных пользователей сети.

Второй уровень – у нарушителя имеются полномочия на запуск ряда задач (программ) из фиксированного набора, реализующего заранее

предусмотренные функции по обработке информации. Как правило, это пользователи сети, права которых определяются в принятой политике безопасности.

Третий уровень – определяется возможностью нарушителя создания и запуска собственных программ с новыми функциями по обработке информации. Пользователями третьего уровня полномочий наиболее часто являются внешние информационные посредники. Он может располагать любыми фрагментами информации о топологии и технических средствах обработки информации сети, любыми фрагментами конфиденциальных данных, к которым данный пользователь имеет доступ.

Четвертый уровень определяется возможностью управления функционированием автоматизированной системы, то есть воздействием на базовое программное обеспечение системы, на состав и конфигурацию оборудования сети. Пользователями четвертого уровня наиболее часто являются внутренние информационные посредники. Они обладают полномочиями системного администратора по отношению к части технических средств обработки информации, имеют полную информацию о сети, доступ ко всем техническим средствам обработки данных, кроме шифрования данных и средств протоколирования действий операторов.

Пятый уровень определяется возможностью доступа к средствам защиты информации и протоколирования действий операторов, к части криптографических ключей. Пользователями пятого уровня наиболее часто являются сотрудники службы информационной безопасности [22].

На основании полученных данных для указанных параметров выставляются оценки.

Так, например, если источник антропогенного характера то, в зависимости от его уровня, ему присваивается оценка от 0 до 2, таким образом:

- 0 – низкий – источник антропогенного характера первого уровня;
- 1 – средний – источник антропогенного характера второго и третьего уровня;

- 2 – высокий – источник антропогенного характера четвертого и пятого уровня.

В зависимости от сложности обнаружения реализации угрозы выставляются следующие оценки:

- 0 – низкая сложность обнаружения;
- 1 – средняя сложность обнаружения;
- 2 – высокая сложность обнаружения.

Для защитных мер, так же указываются следующие оценки:

- 0 – защитные меры предотвращают возможность реализации угрозы;
- 1 – защитные меры затрудняют возможность реализации угрозы;
- 2 – защитные меры направлены только на уменьшение ущерба в результате реализации угрозы и в случае, если они не влияют на реализации угрозы.

По совокупности этих оценок определяется возможность реализации угрозы данным источником для данного актива.

Для получения оценки возможности использования уязвимости для реализации угрозы учитываются такие параметры как: наличие уязвимости и наличие защитных мер. Если для рассматриваемой угрозы для данного актива нет уязвимости, которая могла бы быть использована, возможность использования уязвимости равна 0. Если уязвимость все же есть, то рассматриваются защитные меры и выставляются оценки:

- 0 – защитные меры предотвращают возможность использования уязвимости;
- 1 – защитные меры затрудняют возможность использования уязвимости;
- 2 – защитные меры не влияют на возможность использования уязвимости или защитных мер нет.

2.4 Оценивание рисков информационной безопасности

Исходными данными для оценивания рисков ИБ являются:

- перечень активов и соответствующие им оценки важности;

- оценка возможности реализации угрозы;
- оценка возможности использования уязвимости[23].

Оценивание рисков ИБ производится с помощью таблицы 2.1

Таблица 2.1 – Матрица рисков

Возможность реализации угрозы		Низкая			Средняя			Высокая		
Возможность использования уязвимости		Н	С	В	Н	С	В	Н	С	В
Значение ценности активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

Если в процессе анализа угроз для данной угрозы была зафиксирован защитная мера, то вычисляется начальный и остаточный риск. Начальный риск предполагает оценивание риска без учета защитных мер. Остаточный риск – риск, оставшийся после применения защитных мер. Такой подход к оценке риска позволяет определить эффективность предпринятых защитных мер [24].

При необходимости определения того, какой риск является допустимый, а какой нет, вводится граница допустимости риска и все значения выше указанного считаются недопустимыми. При этом следует учитывать, что риск равный 7 является максимальным, а 0 минимальный риск.

3 Разработка методики идентификации и оценки важности информационных активов

Определение важности информационного актива (далее – актива) на деятельность организации осуществляется посредством оценки уровня негативных последствий для деятельности организации в случае определенного воздействия на актив. В рамках разрабатываемой методики рассматриваются следующие виды воздействия на активы:

- искажение актива (A_1) – изменение актива с сохранением возможности его использования по назначению. Данному воздействию присваивается коэффициент 12;

- подмена актива (A_2) – целенаправленная злоумышленная замена актива с сохранением характеристик исходного актива. Коэффициент данного воздействия равен 14;

- раскрытие актива (A_3) – получение злоумышленником конфиденциальной информации в доступном для понимания виде. Присваивается коэффициент 16;

- блокирование актива (A_4) – изменение актива или его среды, приводящее к недоступности актива для законных пользователей и процессов. Для данного воздействия коэффициент равен 18;

- уничтожение актива (A_5) – преднамеренное или случайное уничтожение, хищение, утрата, стирание актива. Коэффициент – 20.

Оценка важности информационного актива осуществляется по двум направлениям: “влияние актива на деятельность организации” и “затраты, необходимые для ликвидации последствий”. По результатам оценки актива по двум данным направлениям, активу присваивается определенная степень важности в организации.

По направлению “влияние актива на деятельность организации” оценка проводится на основании заключений по следующим показателям:

- влияние на непрерывность деятельности организации (B_1);

- влияние на репутацию организации (B_2);
- нарушение законодательных требований или договоров (B_3);
- нарушение требований регулирующих или надзорных органов (B_4).

Далее рассматриваются все возможные значения показателя “влияние на непрерывность деятельности организации”:

- если вследствие воздействия на актив происходит нарушение деятельности отдельных сотрудников организации, то присваивается качественная величина показателя “низкая” и количественная – 3;

- если вследствие воздействия на актив происходит нарушение деятельности отдельных подразделений организации, то присваиваются величины “средняя” и 6;

- если вследствие воздействия на актив происходит нарушение деятельности организации, то присваивается качественная величина показателя “высокая” и соответствующая ему количественная величина 9.

Критерии определения показателя “влияние на непрерывность деятельности организации” представлены в таблице 3.1.

Далее рассматриваются возможные значения показателя “влияние на репутацию организации”:

- если вследствие воздействия на актив возможно появление отдельных негативных сообщений в местных или специализированных средствах массовой информации (СМИ) и/или поступление единичных жалоб со стороны клиентов, то качественная величина показателя “низкая”, а количественная – 3;

- если вследствие воздействия на актив возможно появление значительного количества негативных сообщений в местных или специализированных СМИ и/или поступление жалоб со стороны клиентов одновременно с отдельными случаями отказа от услуг организации, то присваивается качественная величина показателя “средняя” и количественная 6;

- если вследствие воздействия на актив возможно появление негативных сообщений в федеральных СМИ и/или поступление многочисленных жалоб со стороны клиентов одновременно со значительным оттоком клиентов организации, то качественной величине показателя присваивается значения “высокая”, а количественному – 9.

Таблица 3.1 – Критерии определения показателя “влияние на непрерывность деятельности организации”

Качественная величина	Количественная величина	Критерии
Низкая	3	Происходит нарушение деятельности отдельных сотрудников организации
Средняя	6	Происходит нарушение деятельности отдельных подразделений организации
Высокая	9	Происходит нарушение деятельности организации

Критерии определения показателя “влияние на репутацию организации” представлены в таблице 3.2.

Далее представлены возможные качественные и количественные значения показателя “нарушение законодательных требований или договоров”:

- если вследствие воздействия на актив возможны незначительные денежные выплаты клиентам и контрагентам, в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине организации, то показателям присваиваются величины “низкая” и 3;

- если вследствие воздействия на актив возможны значительные денежные выплаты клиентам и контрагентам, в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине организации, то присваивается качественная величина “средняя” и количественный – 6;

Таблица 3.2 – Критерии определения показателя “влияние на репутацию организации”

Качественная величина	Количественная величина	Критерии
Низкая	3	Появление отдельных негативных сообщений в местных или специализированных средствах массовой информации (СМИ)
		Поступление единичных жалоб со стороны клиентов
Средняя	6	Появление значительного количества негативных сообщений в местных или специализированных СМИ
		Поступление жалоб со стороны клиентов
		Отдельные случаи отказа от услуг организации
Высокая	9	Появление негативных сообщений в федеральных СМИ
		Поступление многочисленных жалоб со стороны клиентов
		Значительный отток клиентов организации

- если вследствие воздействия на актив возможны денежные выплаты на основании постановлений судов, решений органов, уполномоченных в соответствии с законодательством Российской Федерации, то качественному значению присваивается значение “высокая”, а количественному – 9.

Критерии определения показателя “нарушение законодательных требований или договоров” представлены в таблице 3.3.

В случае определения значения показателя “нарушение требований регулирующих и контролирующих органов” используются следующие критерии:

- если вследствие воздействия на актив возможно поступление писем/запросов от надзорных органов, то качественной величине присваивается значение “низкая”, а количественному – 3;

- если вследствие воздействия на актив возможно поступление официальных запросов или проведение официального расследования надзорными органами, то присваиваются значения “средняя” и 6;

- если в случае воздействия на актив возможно наложение санкций надзорными органами, носящих предупредительный характер, то по этому направлению оценки присваиваются показатели “высокая” и 9.

Критерии определения показателя “нарушение требований регулирующих и контролирующих органов” представлены в таблице 3.4.

После того, как заключение по всем трем показателям для каждого из пяти различных возможных воздействий данного направления оценки информационного актива были собраны, рассчитывается важность актива для организации по направлению “влияние актива на деятельность организации”. Расчет важности осуществляется по формуле:

$$S_1 = \sum_{i,j} A_i \cdot B_j,$$

где:

- A_i – коэффициент i -го воздействия на актив;
- i – индекс воздействия на актив;
- B_j – количественная величина j -го показателя оценки;
- j – индекс показателя оценки.

Значение S_1 важности актива по направлению “влияние актива на деятельность организации” после проведенных расчетов принимает количественное значение от 960 до 3121.

Определение важности актива по данному направлению осуществляется по следующим правилам:

- «низкая» – данная величина присваивается активу в том случае, когда количественное значение важности актива меньше или равно 1200;
- «средняя» – данная величина присваивается активу в том случае, когда количественное значение важности актива больше 1200 и меньше 2161;

- «высокая» – данная величина присваивается активу в том случае, когда количественное значение важности актива больше 2160 и меньше 3121.

Таблица 3.3 – Критерии определения показателя “нарушение законодательных требований или договоров”

Качественная величина	Количественная величина	Критерии
Низкая	3	Незначительные денежные выплаты клиентам и контрагентам, в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине организации
Средняя	6	Значительные денежные выплаты клиентам и контрагентам, в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине организации
Высокая	9	Денежные выплаты на основании постановлений судов, решений органов, уполномоченных в соответствии с законодательством Российской Федерации

Таблица 3.4 – Критерии определения показателя “нарушение требований регулирующих и контролирующих органов”

Качественная величина	Количественная величина	Критерии
Низкая	3	Поступление писем/запросов от надзорных органов
Средняя	6	Поступление официальных запросов
		Проведение официального расследования надзорными органами
Высокая	9	Наложение санкций надзорными органами, носящих предупредительный характер

По направлению “затраты, необходимые для ликвидации последствий” оценивание осуществляется на основании заключений по следующим показателям:

- объем финансовых и материальных затрат, необходимых для ликвидации последствий (C_1);
- объем дополнительных людских ресурсов, необходимых для ликвидации последствий (C_2);
- объем дополнительных временных затрат, необходимых для ликвидации последствий (C_3).

Рассмотрим все возможные значения показателя “объем финансовых и материальных затрат, необходимых для ликвидации последствий”:

- если для ликвидации последствий воздействия на актив могут потребоваться финансовые и материальные затраты, планируемые в рамках бюджета организации для ликвидации подобных нарушений, то присваивается качественное значение “низкая” и количественное значение 4;
- если для ликвидации последствий воздействия на актив могут потребоваться незначительные сверхплановые финансовые и материальные затраты из бюджета организации, то критерию присваиваются значения “средняя” и 8;
- если для ликвидации последствий воздействия на актив могут потребоваться значительные сверхплановые финансовые и материальные затраты из бюджета организации, то по этому направлению оценки присваивается качественное значение “высокая” и количественное – 12.

Критерии определения показателя “объем финансовых и материальных затрат, необходимых для ликвидации последствий” представлены в таблице 3.5

Качественные и количественные значения показателя “объем дополнительных временных затрат, необходимых для ликвидации последствий” представлены ниже:

- если ликвидация последствий воздействия на актив может потребовать дополнительных временных затрат от сотрудника организации, объем которых не наносит ущерба другим видам деятельности, выполняемым данным сотрудником, то данному показателю присваиваются значения “низкая” и 4;

- если ликвидация последствий воздействия на актив может потребовать дополнительных временных затрат от сотрудника организации, объем которых нанесет незначительный ущерб другим видам деятельности, выполняемым данным сотрудником, то активу по данному показателю присваивается качественная величина “средняя” и количественная 8;

- если ликвидация последствий воздействия на актив может потребовать дополнительных временных затрат от сотрудника организации, объем которых нанесет значительный ущерб другим видам деятельности, выполняемым данным сотрудником, то показателям присваиваются значения “высокая” и 12.

Таблица 3.5 – Критерии определения показателя “объем финансовых и материальных затрат, необходимых для ликвидации последствий”

Качественная величина	Количественная величина	Критерии
Низкая	4	Финансовые и материальные затраты, планируемые в рамках бюджета организации для ликвидации подобных нарушений
Средняя	8	Незначительные сверхплановые финансовые и материальные затраты из бюджета организации
Высокая	12	Значительные сверхплановые финансовые и материальные затраты из бюджета организации

Таблица 3.6 – Критерии определения показателя “объем дополнительных людских ресурсов, необходимых для ликвидации последствий”

Качественная величина	Количественная величина	Критерии
Низкая	4	Дополнительное привлечение сотрудников отдела организации, в компетенцию которого входит ликвидация данных последствий
Средняя	8	Привлечение сотрудников организации, действующих вне рамок своих должностных обязанностей и обладающих компетенцией и квалификацией для выполнения подобной деятельности
Высокая	12	Привлечение сторонних организаций в рамках существующих договорных обязательств

Критерии определения показателя “объем дополнительных временных затрат, необходимых для ликвидации последствий” представлены в таблице 3.7.

После того, как были собраны заключения по всем трем показателям для каждого из пяти различных возможных воздействий данного направления оценки информационного актива, можно приступить к расчету важности актива для организации по направлению “затраты, необходимые для ликвидации последствий”, который осуществляется по следующей формуле:

$$S_2 = \sum_{i,j} A_i \cdot C_j,$$

где:

- A_i – коэффициент i -го воздействия на актив;
- i – индекс воздействия на актив;
- C_j – количественная величина j -го показателя оценки;
- j – индекс показателя оценки.

Значение S_2 важности актива по направлению “затраты, необходимые для ликвидации последствий” после проведенных расчетов принимает количественное значение от 960 до 3121.

Определение важности актива по второму направлению осуществляется по следующим правилам:

- «низкая» – данная величина присваивается активу в том случае, когда количественное значение важности актива меньше или равно 1200;
- «средняя» – данная величина присваивается активу в том случае, когда количественное значение важности актива больше 1200 и меньше 2161;
- «высокая» – данная величина присваивается активу в том случае, когда количественное значение важности актива больше 2160 и меньше 3121.

Таблица 3.7 – Критерии определения показателя «объем дополнительных временных затрат, необходимых для ликвидации последствий»

Качественная величина	Количественная величина	Критерии
Низкая	4	Требуются дополнительные временные затраты от сотрудника организации, объем которых не наносит ущерба другим видам деятельности
Средняя	8	Требуются дополнительные временные затраты от сотрудника организации, объем которых нанесет незначительный ущерб другим видам деятельности, выполняемым данным сотрудником
Высокая	12	Требуются дополнительные временные затраты от сотрудника организации, объем которых нанесет значительный ущерб другим видам деятельности

После выявления оценки важности актива по обоим направлениям можно вывести интегральную оценку важности информационного актива. Интегральная оценка важности актива вычисляется по следующей формуле:

$$S = S_1 + S_2.$$

Значение S интегральной оценки важности актива после проведенных расчетов принимает количественное значение от 1920 до 6241.

Определение важности актива осуществляется применительно ко всем видам воздействия на актив по следующим правилам:

- «низкая» – данная величина присваивается активу в том случае, когда количественное значение важности актива меньше или равно 2400;
- «средняя» – данная величина присваивается активу в том случае, когда количественное значение важности актива больше 2400 и меньше 4321;
- «высокая» – данная величина присваивается активу в том случае, когда количественное значение важности актива больше 4320 и меньше 6241.

Таким образом, по результатам выполнения данной методики, информационному активу должна быть присвоена определенная степень его важности в организации для последующей оценке рисков информационной безопасности: низкая, средняя, высокая.

4 Процесс идентификации и оценки важности информационных активов

Под процессом понимается упорядоченная последовательность взаимосвязанных действий, выполняющихся с момента возникновения исходных данных до получения требуемого результата.

Целью процесса является идентификация и оценка важности информационных активов организации.

В данном процессе можно выделить следующие подпроцессы:

- определение границ оценки;
- определение области применения;
- формирование перечня информационных активов;
- идентификация информационных активов;
- определение важности информационных активов[25].

Первым шагом в процессе оценки важности информационных активов является определение границ оценки. В данном подпроцессе необходимо рассмотреть активы, людей, работающих с этими активами и среду, в которой эта работа происходит.

Для определения границ оценки необходимо учитывать корпоративную политику организации, так как она определяет способ оценки риска; особенности организации, которые определяются через ее цели бизнеса и структуру; различные ограничения и требования, влияющие на работу организации, как например, культурные, бюджетные, стратегические и так далее.

Таким образом, в данном подпроцессе будет следующая входная информация:

- корпоративная политика организации;
- ограничения и требования;
- особенности организации.

Управляющая информация: стандарты по информационной безопасности.

Роли:

- руководство организации;
- эксперты.

Выходная информация: границы оценки.

Структура подпроцесса определения границ оценки представлена на рисунке 4.1.

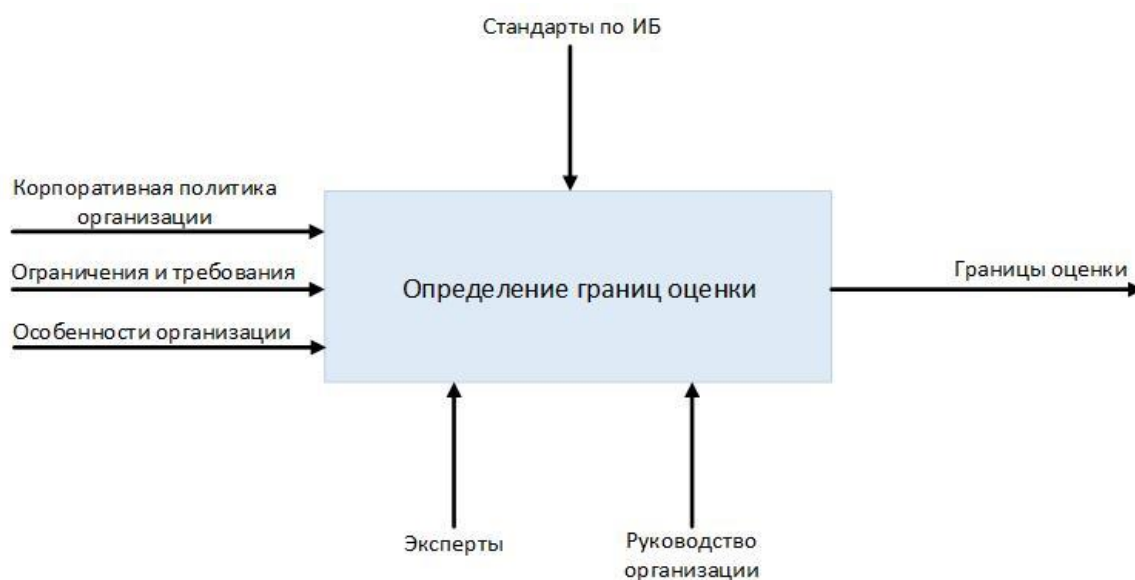


Рисунок 4.1 – Структура подпроцесса определения границ оценки

После определения границ оценки необходимо определить область применения оценки рисков ИБ. Определение области применения заключается в выяснении того, что будет подвергаться оценке в рамках границ оценки риска.

Входная информация:

- бизнес-процессы;
- границы оценки;

Управляющая информация: стандарты по ИБ.

Роли:

- руководство организации;
- эксперты.

Выходная информация: область применения.

Структура подпроцесса определения области применения представлена на рисунке 4.2.

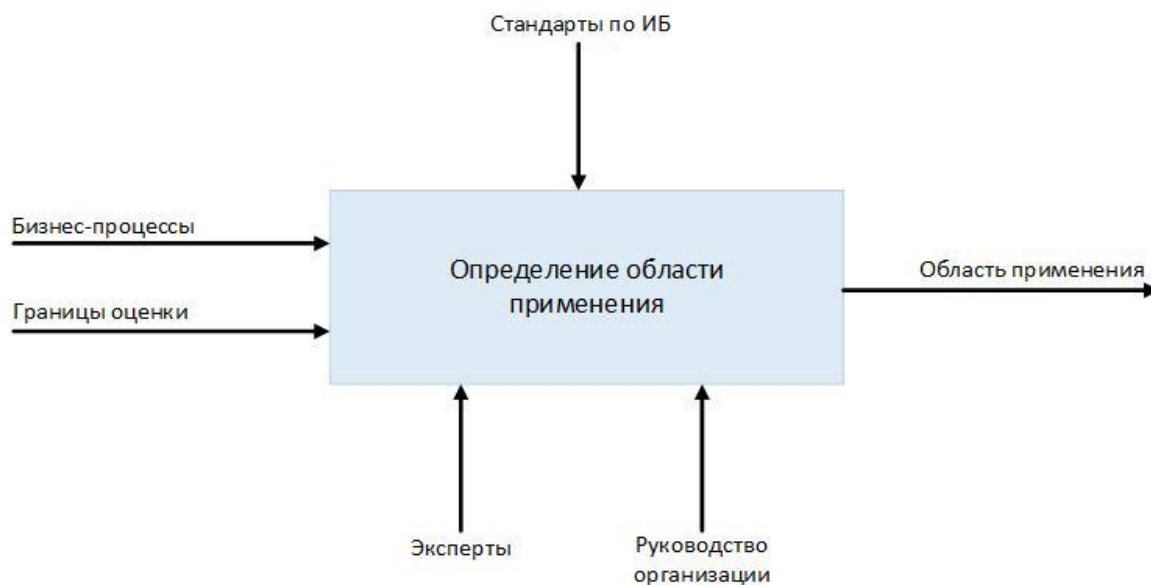


Рисунок 4.2 – Структура подпроцесса определения области применения

В рамках данного подпроцесса создается перечень имеющихся в организации информационных активов и полная информация о каждом из них. После этого необходимо произвести идентификацию информационных активов.

Происходит разделение информационных активов на основные и вспомогательные. К основным относят бизнес-процессы, то есть процессы, которые направлены на достижение целей деятельности организации, либо процессы, которые связаны с информацией ограниченного доступа. Также к основным активам относят информацию, которая необходима для достижения целей организации, информацию с высокой себестоимостью, и информацию, сбор и обработка которой связана с большими затратами.

К вспомогательным активам относят персонал, программное обеспечение, аппаратные средства и телекоммуникационное оборудование.

Входная информация:

- область применения;
- перечень информационных активов организации.

Управляющая информация: методика оценки важности информационных активов.

Роли:

- владельцы активов;
- эксперты.

Выходная информация: основные и вспомогательные активы, подлежащие оценке важности.

Структура подпроцесса идентификации информационных активов представлена на рисунке 4.3.

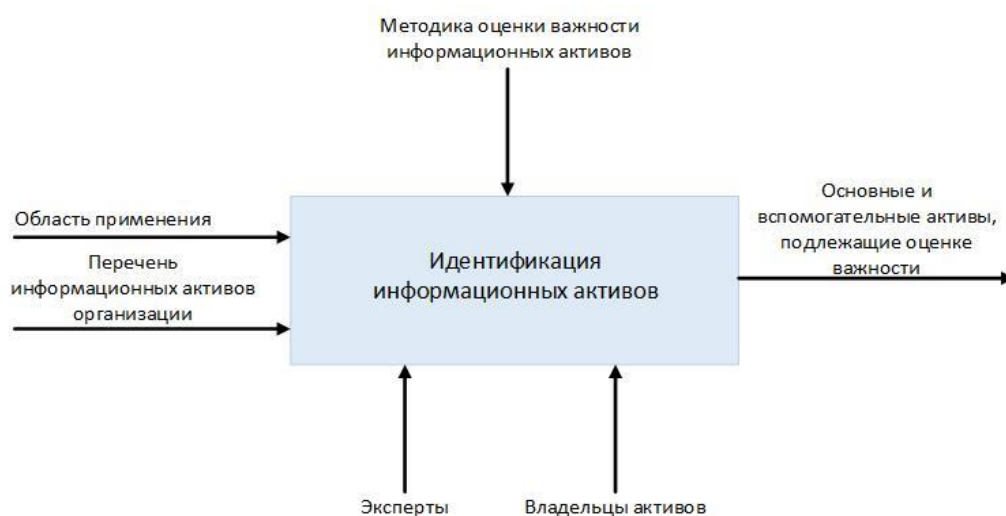


Рисунок 4.3 – Структура подпроцесса идентификации информационных активов

Последним подпроцессом является определение важности информационных активов. Определение важности актива на деятельность организации осуществляется посредством оценки уровня негативных последствий для деятельности организации в случае определенного воздействия на актив. Рассматриваются такие воздействия как: искажение актива, подмена, раскрытие, блокирование и уничтожение.

Важность информационного актива зависит от следующих критериев:

- влияние на непрерывность деятельности организации;
- влияние на репутацию организации;
- нарушение законодательных требований или договоров;

- нарушение требований регулирующих или надзорных органов;
- объем финансовых и материальных затрат, необходимых для ликвидации последствий;
- объем дополнительных людских ресурсов, необходимых для ликвидации последствий;
- объем дополнительных временных затрат, необходимых для ликвидации последствий.

Определение важности происходит с помощью методики оценки важности информационных активов, которая была реализована в рамках системы оценки важности.

Согласно данной методики по каждому из видов воздействия и для каждого из критериев активу выставляется определенная качественная и соответствующая ему количественная величина. После чего данные оценки суммируются, и активу присваивается определенная степень его важности в организации: низкая, средняя, высокая или критическая.

Входная информация: основные и вспомогательные активы, подлежащие оценке важности.

Управляющая информация: методика оценки важности информационных активов.

Роли:

- владельцы активов;
- эксперты.

Выходная информация: перечень информационных активов и их ценность.

Структура подпроцесса определения важности информационных активов представлена на рисунке 4.4.

Общая схема технологического процесса оценки важности информационных активов представлена на рисунке 4.5.



Рисунок 4.4 – Структура подпроцесса определения важности информационных активов

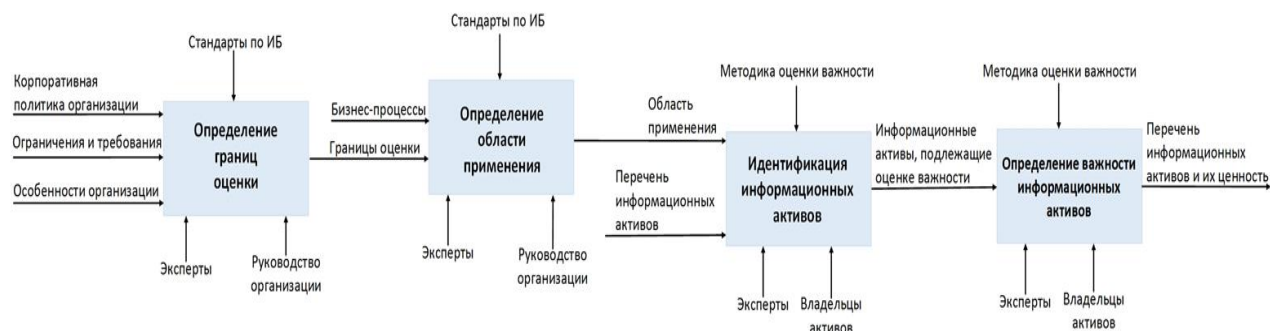


Рисунок 4.5 – Процесс оценки важности информационных активов

5 Выполнение проверки методики идентификации и оценки важности информационных активов организации

5.1 Описание бизнес-целей и бизнес-функций, основных бизнес-процессов организации

В качестве организации рассматривается поликлиника, основной целью (целевой функцией) поликлиники является оказание медицинских услуг населению.

Декомпозиция целевой функции позволяет определить основные информационные процессы, реализуемые информационной системой организации, необходимые для этого ресурсы, а также способы управления и преобразования информации.

Для реализации целевой функции в организации должны быть реализованы три процесса основной деятельности:

- регистрация пациентов;
- обследование пациентов;
- управление.

Указанные процессы реализуются основной функцией «Взаимодействие врачей находящихся на разных рабочих местах», при этом в составе этой основной функции можно выделить следующие функции:

- сохранение всех персональных и регистрационных данных, диагнозов, анализов на сервере организации;
- прием персональных данных от граждан, поступивших в поликлинику;
- печать оформленных отчетов и диагнозов.

Блок А0, соответствующий основной функции, показан на рисунке 5.1.

Декомпозиция блока А0 на составляющие функции представлена на рисунке 5.2.

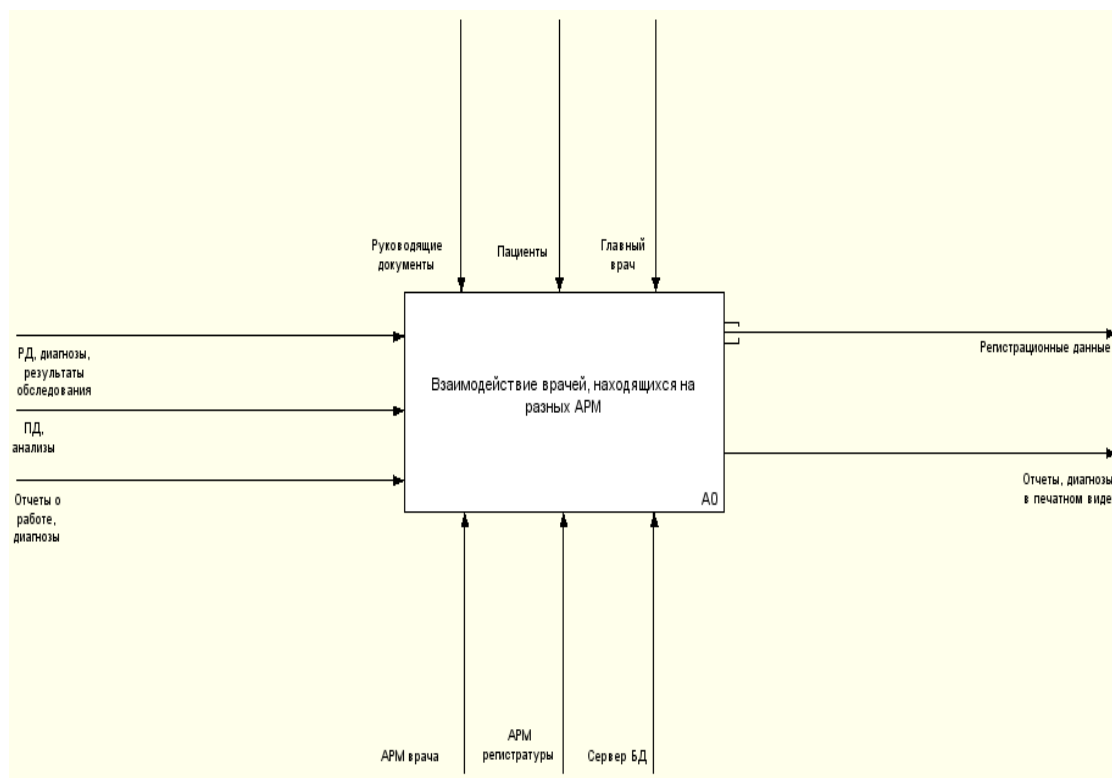


Рисунок 5.1- Диаграмма основной функции

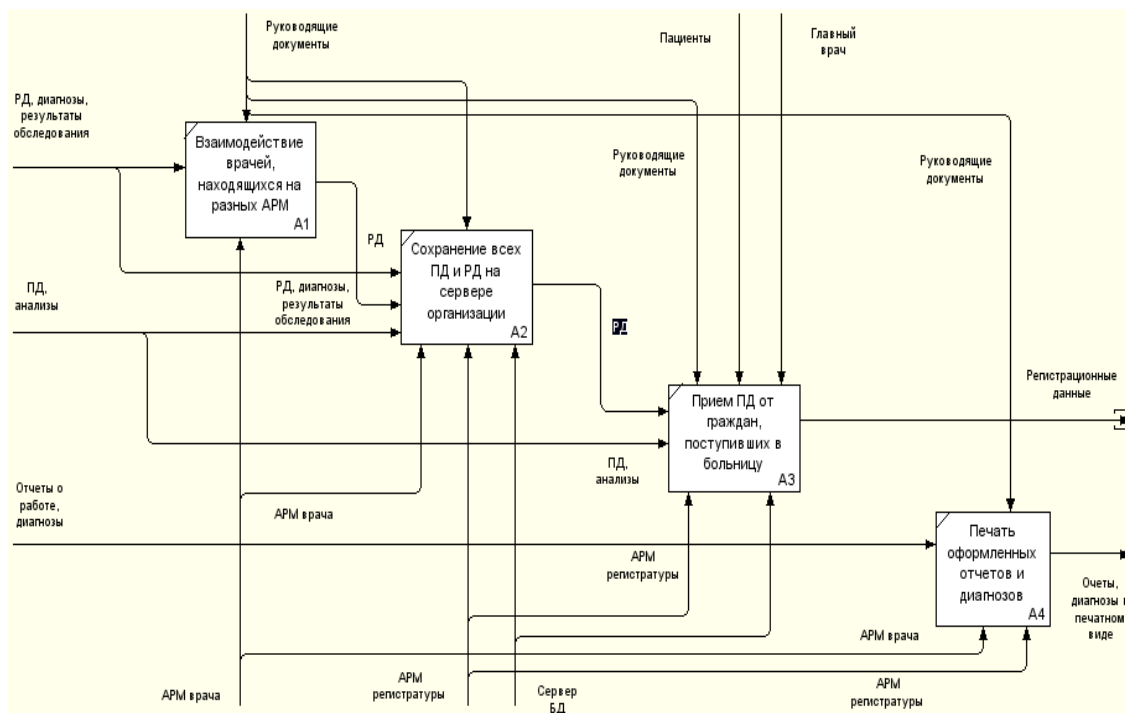


Рисунок 5.2 – Диаграмма составляющих функций

После определения основных информационных процессов в информационной системе организации была построена общая инфологическая модель, представляющая собой направленный граф.

Вершинами графа являются информационные компоненты, указанные в качестве ресурсов каждого процесса. Ребрами графа являются информационные потоки, связывающие информационные компоненты. Направление ребер определяет направление информационного потока. Для каждого ребра указываются:

- название информационного потока;
- критичность информационного потока;
- предполагаемый объем данных.

Критичность потока может быть обозначена как:

- В – высокая;
- С – средняя;
- Н – низкая.

Объем потока может быть обозначен как:

- 1 – малый;
- 2 – средний;
- 3 – большой.

Общая инфологическая модель информационной системы поликлиники приведена на рисунке 5.3.

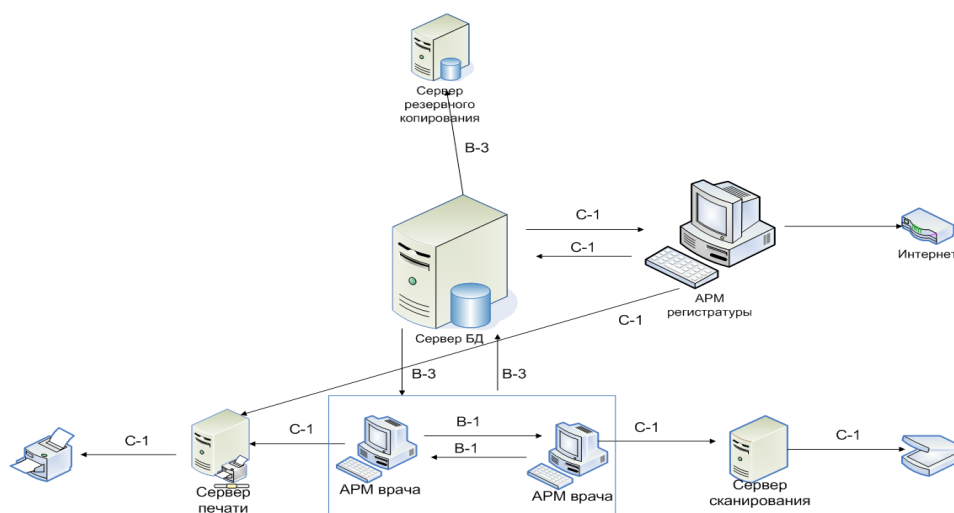


Рисунок 5.3 – Общая инфологическая модель

5. 2 Идентификация активов

Информационные активы организации включают информацию, необходимую для осуществления основной деятельности организации,

информацию с высокой себестоимостью, сбор, хранение, обработка и передача которой требует много времени и связана со значительными затратами на приобретение.

Перечень информационных активов:

- информация о руководящих документах;
- информация о пациентах;
- информация о регистрационных данных;
- информация о главном враче.

Далее идентифицированы вспомогательные активы и зависимости между ними и основными активами организации. Результат представлен в виде матрицы зависимостей в таблице 5.1.

Таблица 5.1 – Матрица зависимостей между активами организации

Зависимый актив	Актив				
	АРМ врача (BA1)	АРМ регистратуры (BA2)	Сервер БД (BA3)	Персонал (BA4)	Терминалы (BA5)
Информация о руководящих документах (ИА1)	+	+	+	-	-
Информация о пациентах (ИА2)	+	+	+	+	-
Информация о регистрационных данных (ИА3)	+	+	-	-	+
Информация о главном враче (ИА4)	+	+	+	+	-

5.3 Оценка важности информационных активов

Затем для каждого из информационных активов определены значимые свойства ИБ.

Документированный перечень информационных активов представлен в таблице 5.2.

Таблица 5.2 – Перечень информационных активов и их значимых свойств

Информационный актив	Значимые свойства информационной безопасности		
	Конфиденциальность	Целостность	Доступность
Информация о руководящих документах (ИА1)	-	+	+
Информация о пациентах (ИА2)	+	+	+
Информация о регистрационных данных (ИА3)	-	+	+
Информация о главном враче (ИА4)	+	+	+

Далее проведено оценивание величин ущерба от нарушения свойств ИБ активов по следующим направлениям:

- степень влияния на непрерывность деятельности организации;
- объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;
- объем дополнительных людских ресурсов, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;
- объем дополнительных временных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;
- степень нарушения законодательных требований и (или) договорных обязательств организации.

На основании результатов оценивания величины нарушений ИБ для каждого информационного актива определена обобщенная качественная оценка величины нарушения ИБ. Результаты оценивания представлены в таблице 5.3.

Таблица 5.3 – Результаты оценивания величии нарушения ИБ

Информационный актив	Свойства безопасности	Величины нарушения ИБ по направлениям оценивания					Обобщенная величина нарушения ИБ	Ценности актива
		1	2	3	4	5		
Информация о руководящих документах (ИА1)	Конфиденциальность	М	М	М	М	М	М	С
	Целостность	С	С	М	М	М	С	
	Доступность	С	С	М	М	М	С	
Информация о пациентах (ИА2)	Конфиденциальность	В	В	С	В	В	В	В
	Целостность	В	С	М	В	С	В	
	Доступность	В	С	М	В	С	В	
Информация о регистрационных данных (ИА3)	Конфиденциальность	М	М	М	М	М	М	С
	Целостность	С	С	М	М	М	С	
	Доступность	С	С	М	М	М	С	
Информация о главном враче (ИА4)	Конфиденциальность	В	В	С	В	В	В	В
	Целостность	В	С	М	С	С	В	
	Доступность	В	С	М	С	С	В	

Ценность вспомогательных активов была определена относительно их стоимости, а также ценности зависимых от них информационных активов. Результат оценивания представлен в таблице 5.4.

Таблица 5.4 – Определение ценности вспомогательных активов

Актив	Ценность актива без учета зависимостей	Зависимые активы		Ценность актива
		Актив	Ценность	
АРМ врача	С	Информация о руководящих документах	С	В
		Информация о пациентах	В	
		Информация о регистрационных данных	С	
		Информация о главном враче	В	
АРМ регистратуры	С	Информация о руководящих документах	С	В
		Информация о пациентах	В	
		Информация о регистрационных данных	С	
		Информация о главном враче	В	

Продолжение таблицы 5.4

Актив	Ценность актива без учета зависимостей	Зависимые активы		Ценность актива
		Актив	Ценность	
Сервер БД	С	Информация о руководящих документах	С	В
		Информация о пациентах	В	
		Информация о регистрационных данных	В	
Персонал	С	Информация о пациентах	В	В
		Информация о главном враче	В	
Терминалы	С	Информация о регистрационных данных	С	С

Далее рассчитывается важность активов по методике, разработанной в данной работе. Изначально потребуется оценить важность активов по такому виду воздействия на актив, как «искажение актива» или А1 с коэффициентом 12 по направлению – «влияние актива на деятельность организации». Влияние актива на деятельность организации для А1 представлено в таблице 5.5.

Таблица 5.5 – Влияние актива на деятельность организации для А1

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	3	3	3	3	144	576
	Информация о пациентах	3	3	3	3	144	

Продолжение таблицы 5.5

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о регистрационных данных	3	3	3	3	144	576
	Информация о главном враче	3	3	3	3	144	
АРМ регистратуры	Информация о руководящих документах	6	3	3	6	216	720
	Информация о пациентах	3	3	6	6	216	
	Информация о регистрационных данных	3	3	3	3	144	
	Информация о главном враче	3	3	3	3	144	
Сервер БД	Информация о руководящих документах	3	3	3	6	180	612
	Информация о пациентах	3	6	6	6	252	
	Информация о регистрационных данных	3	3	6	3	180	
Персонал	Информация о пациентах	3	3	6	3	180	324
	Информация о главном враче	3	3	3	3	144	
Терминалы	Информация о регистрационных данных	3	6	3	3	180	180

Таким образом, наивысшую оценку среди активов по такому виду воздействия, как «искажение актива» наибольшую важность представляет АРМ регистратуры, что связано с искажением данных для большого объема документов, которые печатает регистратура.

Далее необходимо оценить важность активов по такому виду воздействия на актив, как «подмена актива» или А2 с коэффициентом 14 по направлению – «влияние актива на деятельность организации». Влияние актива на деятельность организации для А2 представлено в таблице 5.6.

Таблица 5.6 – Влияние актива на деятельность организации для А2

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	3	3	6	3	210	714
	Информация о пациентах	3	3	3	3	168	
	Информация о регистрационных данных	3	3	3	3	168	
	Информация о главном враче	3	3	3	3	168	
АРМ регистратуры	Информация о руководящих документах	3	3	3	3	168	714
	Информация о пациентах	3	3	6	3	210	
	Информация о регистрационных данных	3	3	3	3	168	
	Информация о главном враче	3	3	3	3	168	

Продолжение таблицы 5.6

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
Сервер БД	Информация о руководящих документах	6	9	6	6	378	1050
	Информация о пациентах	3	9	9	6	378	
	Информация о регистрационных данных	3	6	6	6	294	
Персонал	Информация о пациентах	3	3	3	3	168	336
	Информация о главном враче	3	3	3	3	168	
Терминалы	Информация о регистрационных данных	3	6	6	3	252	252

Для данного вида воздействия на актив самую большую оценку важности актива получает Сервер БД, так как подмена данных на сервере оказывает самое большое влияние.

На следующем этапе необходимо оценить важность активов по такому виду воздействия на актив, как «раскрытие актива» или А3 с коэффициентом 16 по направлению – «влияние актива на деятельность организации». Влияние актива на деятельность организации для А3 представлено в таблице 5.7.

Для данного вида воздействия на активы самую большую важность имеет Сервер БД, так как раскрытие информации из базы данных о

пациентах может вызвать самые большие колебания общественность, может привести к крупным судебным разбирательствам и прочее.

Таблица 5.7 – Влияние актива на деятельность организации для А3

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	3	3	6	6	288	1008
	Информация о пациентах	3	3	6	6	288	
	Информация о регистрационных данных	3	3	6	3	240	
	Информация о главном враче	3	3	3	3	192	
АРМ регистратуры	Информация о руководящих документах	3	6	6	6	336	1008
	Информация о пациентах	3	6	6	3	288	
	Информация о регистрационных данных	3	3	3	3	192	
	Информация о главном враче	3	3	3	3	192	

Продолжение таблицы 5.7

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
Сервер БД	Информация о руководящих документах	3	9	9	9	480	1440
	Информация о пациентах	6	9	9	9	528	
	Информация о регистрационных данных	6	6	9	6	432	
Персонал	Информация о пациентах	3	3	6	3	240	432
	Информация о главном враче	3	3	3	3	192	
Терминалы	Информация о регистрационных данных	3	3	6	3	240	240

Далее необходимо оценить важность активов по такому виду воздействия на актив, как Блокирование актива или А4 с коэффициентом 18 по направлению – «влияние актива на деятельность организации». Влияние актива на деятельность организации для А4 представлено в таблице 5.8.

На данном этапе самую большую оценку важности получили АРМ Регистратуры и Сервер БД, что связано с самым большим влиянием на деятельность и работоспособность поликлиники при блокировании данных.

Таблица 5.8 – Влияние актива на деятельность организации для А4

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	3	3	3	3	216	864
	Информация о пациентах	3	3	3	3	216	
	Информация о регистрационных данных	3	3	3	3	216	
	Информация о главном враче	3	3	3	3	216	
АРМ регистратуры	Информация о руководящих документах	3	6	3	3	270	1134
	Информация о пациентах	3	6	3	3	270	
	Информация о регистрационных данных	3	6	6	3	324	
	Информация о главном враче	3	6	3	3	270	
Сервер БД	Информация о руководящих документах	3	6	6	6	378	1242
	Информация о пациентах	6	6	6	6	432	
	Информация о регистрационных данных	6	6	6	6	432	

Продолжение таблицы 5.8

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
Персонал	Информация о пациентах	3	3	3	3	216	432
	Информация о главном враче	3	3	3	3	216	
Терминалы	Информация о регистрационных данных	3	3	3	3	216	216

На последнем этапе необходимо оценить важность активов по такому виду воздействия на актив, как Уничтожение актива или А5 с коэффициентом 20 по направлению – «влияние актива на деятельность организации». Влияние актива на деятельность организации для А5 представлено в таблице 5.9.

Таблица 5.9 – Влияние актива на деятельность организации для А5

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	6	3	3	3	300	1140
	Информация о пациентах	6	3	3	3	300	

Продолжение таблицы 5.9

Наименование актива	Вспомогательный актив	Влияние на непрерывность деятельности организации В1	Влияние на репутацию организации В2	Нарушение законодательных требований или договоров В3	Нарушение требований регулирующих или надзорных органов В4	Итого	Важность актива
1	2	3	4	5	6	7	8
АРМ врача	Информация о регистрационных данных	6	3	3	3	300	1140
	Информация о главном враче	3	3	3	3	240	
АРМ регистратуры	Информация о руководящих документах	6	3	3	3	300	1440
	Информация о пациентах	6	6	6	6	480	
	Информация о регистрационных данных	6	3	6	6	420	
	Информация о главном враче	3	3	3	3	240	
Сервер БД	Информация о руководящих документах	6	6	9	9	600	1920
	Информация о пациентах	6	9	9	9	660	
	Информация о регистрационных данных	6	9	9	9	660	
Персонал	Информация о пациентах	3	3	6	6	360	600
	Информация о главном враче	3	3	3	3	240	
Терминалы	Информация о регистрационных данных	3	3	6	6	360	360

Таким образом, самую большую оценку важности имеет сервер данных, так как удаление данных на нем окажет самое большое влияние на деятельность поликлиники из-за потребности в восстановлении большого объема данных, что обязательно будет освещено на федеральном уровне.

После того, как заключение по всем трем показателям для каждого из пяти различных возможных воздействий данного направления оценки информационного актива были собраны, рассчитывается важность актива для организации по направлению «влияние актива на деятельность организации». Итоговое значение важности и промежуточные расчеты сведены в таблицу 5.10.

Таблица 5.10 – Итоговое значение важности

Наименование актива	Вспомогательный актив	A1	A2	A3	A4	A5	Итог	Важность актива
1	2		3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	144	210	288	216	300	1158	4302 (H)
	Информация о пациентах	144	168	288	216	300	1116	
	Информация о регистрационных данных	144	168	240	216	300	1068	
	Информация о главном враче	144	168	192	216	240	960	
АРМ регистратуры	Информация о руководящих документах	216	168	336	270	300	1290	5016 (C)
	Информация о пациентах	216	210	288	270	480	1464	
	Информация о регистрационных данных	144	168	192	324	420	1248	
	Информация о главном враче	144	168	192	270	240	1014	

Продолжение таблицы 5.10

Наименование актива	Вспомогательный актив	A1	A2	A3	A4	A5	Итог	Важность актива
1	2		3	4	5	6	7	8
Сервер БД	Информация о руководящих документах	180	378	480	378	600	2016	6264 (В)
	Информация о пациентах	252	378	528	432	660	2250	
	Информация о регистрационных данных	180	294	432	432	660	1998	
Персонал	Информация о пациентах	180	168	240	216	360	1164	2124 (Н)
	Информация о главном враче	144	168	192	216	240	960	
Терминалы	Информация о регистрационных данных	180	252	240	216	360	1248	1248 (Н)

Далее необходимо провести оценку важности активов поликлиники по направлению «затраты, необходимые для ликвидации последствий». Оценивание на данном этапе осуществляется на основании заключений по следующим показателям:

- объем финансовых и материальных затрат, необходимых для ликвидации последствий (С1);
- объем дополнительных людских ресурсов, необходимых для ликвидации последствий (С2);
- объем дополнительных временных затрат, необходимых для ликвидации последствий (С3).

Далее необходимо оценить важность активов по такому виду воздействия на актив, как «искажение актива» или А1 с коэффициентом 12 по направлению - «затраты для ликвидации последствий». Влияние актива на деятельность организации представлено в таблице 5.11.

Таблица 5.11 – Влияние актива на деятельность организации

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
АРМ врача	Информация о руководящих документах	4	4	4	144	576
	Информация о пациентах	4	4	4	144	
	Информация о регистрационных данных	4	4	4	144	
	Информация о главном враче	4	4	4	144	
АРМ регистратуры	Информация о руководящих документах	8	4	4	192	672
	Информация о пациентах	4	4	8	192	
	Информация о регистрационных данных	4	4	4	144	
	Информация о главном враче	4	4	4	144	
Сервер БД	Информация о руководящих документах	4	8	8	240	1104
	Информация о пациентах	12	12	12	432	
	Информация о регистрационных данных	12	12	12	432	

Продолжение таблицы 5.11

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
Персонал	Информация о пациентах	4	4	8	192	384
Терминалы	Информация о регистрационных данных	4	8	8	240	240

По данным оценки важности в таблице 5.11, можно сказать, что самую большую оценку получил сервер БД, в связи с самыми большими затратами по времени восстановления данных, так как потребуется поиск и анализ возникших ошибок в связи с изменением данных.

Далее необходимо оценить важность активов по такому виду воздействия на актив, как «подмена актива» или А2 с коэффициентом 14 по направлению – «затраты для ликвидации последствий» (см. таблицу 5.12).

Таблица 5.12 – Влияние актива на деятельность организации

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
АРМ врача	Информация о руководящих документах	4	4	4	168	672
	Информация о пациентах	4	4	4	168	
	Информация о регистрационных данных	4	4	4	168	

Продолжение таблицы 5.12

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итого	Важность актива
1	2	3	4	5	6	8
АРМ регистратуры	Информация о руководящих документах	4	4	4	168	728
	Информация о пациентах	4	4	8	224	
	Информация о регистрационных данных	4	4	4	168	
	Информация о главном враче	4	4	4	168	
Сервер БД	Информация о руководящих документах	4	8	8	280	896
	Информация о пациентах	4	8	12	336	
	Информация о регистрационных данных	4	8	8	280	
Персонал	Информация о пациентах	4	4	8	224	448
	Информация о главном враче	4	4	8	224	
Терминалы	Информация о регистрационных данных	4	4	8	224	224

Следующий этап – оценка важности активов по такому виду воздействия на актив, как «раскрытие актива» или А3 с коэффициентом 16 по направлению – «затраты для ликвидации последствий» (см. таблицу 5.13).

Таблица 5.13 – Влияние актива на деятельность организации

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
АРМ врача	Информация о руководящих документах	4	4	4	192	768
	Информация о пациентах	4	4	4	192	
	Информация о регистрационных данных	4	4	4	192	
	Информация о главном враче	4	4	4	192	
АРМ регистратуры	Информация о руководящих документах	4	4	4	192	832
	Информация о пациентах	4	4	8	256	
	Информация о регистрационных данных	4	4	4	192	
	Информация о главном враче	4	4	4	192	
Сервер БД	Информация о руководящих документах	4	8	8	320	960
	Информация о пациентах	4	8	8	320	
	Информация о регистрационных данных	4	8	8	320	
Персонал	Информация о пациентах	4	4	8	256	448
	Информация о главном враче	4	4	4	192	
Терминалы	Информация о регистрационных данных	4	4	4	192	192

При раскрытии данных самую большую важность имеет сервер БД, так как самая большая часть данных является конфиденциальной информацией, раскрытие которой приведет к судебным разбирательствам в большом объеме.

Следующий этап – оценка важности активов по такому виду воздействия на актив, как «блокирование актива» или А4 с коэффициентом 18 по направлению – «затраты для ликвидации последствий» (см. таблицу 5.14).

Таблица 5.14 – Влияние актива на деятельность организации

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
АРМ регистратуры	Информация о руководящих документах	8	4	4	288	1152
	Информация о пациентах	8	4	8	360	
	Информация о регистрационных данных	8	4	4	288	
	Информация о главном враче	4	4	4	216	
Сервер БД	Информация о руководящих документах	8	12	12	576	1800
	Информация о пациентах	12	12	12	648	
	Информация о регистрационных данных	8	12	12	576	
Персонал	Информация о пациентах	4	4	8	288	576
	Информация о главном враче	4	4	8	288	
Терминалы	Информация о регистрационных данных	4	4	4	216	216

При блокировании данных самые большие затраты понесет Сервер БД, так как персонал имеет возможность работать и на бумажных носителях, в то время как восстановление доступа необходимо для поликлиники в связи с большим объемом информации, которая необходима поликлинике в сжатые сроки.

Следующий этап – оценка важности активов по такому виду воздействия на актив, как Уничтожение актива или А5 с коэффициентом 20 по направлению – «затраты для ликвидации последствий» (см. таблицу 5.15).

Таблица 5.15 – Влияние актива на деятельность организации

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
АРМ врача	Информация о руководящих документах	4	4	4	240	960
	Информация о пациентах	4	4	4	240	
	Информация о регистрационных данных	4	4	4	240	
	Информация о главном враче	4	4	4	240	
АРМ регистратуры	Информация о руководящих документах	8	4	4	320	1280
	Информация о пациентах	8	4	8	400	
	Информация о регистрационных данных	8	4	4	320	
	Информация о главном враче	4	4	4	240	

Продолжение таблицы 5.15

Наименование актива	Вспомогательный актив	Объем финансовых и материальных затрат С1	Объем дополнительных людских ресурсов С2	Объем дополнительных временных затрат С3	Итог	Важность актива
1	2	3	4	5	6	8
Сервер БД	Информация о руководящих документах	12	12	12	720	2160
	Информация о пациентах	12	12	12	720	
	Информация о регистрационных данных	12	12	12	720	
Персонал	Информация о пациентах	4	4	8	320	640
	Информация о главном враче	4	4	8	320	
Терминалы	Информация о регистрационных данных	4	4	8	320	320

При уничтожении данных самые большие затраты понесет Сервер БД, в связи с тем, что потеря информации приведет к дополнительным временным, людским и материальным затратам по восстановлению данных. Если учесть, что данные были утеряны безвозвратно и потребуется восстановление всего объема данных с бумажных носителей, то один перенос данных в электронный вид данных пациентов обойдется в огромные временные затраты.

После того, как заключение по всем трем показателям для каждого из пяти различных возможных воздействий данного направления оценки информационного актива были собраны, рассчитывается важность актива для организации по направлению «затраты, необходимые для ликвидации последствий». Итоговое значение важности и промежуточные расчеты сведем в таблицу (см. таблицу 5.16).

Таблица 5.16 – Влияние актива на деятельность организации

Наименование актива	Вспомогательный актив	A1	A2	A3	A4	A5	Итог	Важность актива
1	2		3	4	5	6	7	8
АРМ врача	Информация о руководящих документах	144	168	192	288	240	1032	4056(Н)
	Информация о пациентах	144	168	192	288	240	1032	
	Информация о регистрационных данных	144	168	192	288	240	1032	
	Информация о главном враче	144	168	192	216	240	960	
АРМ регистратуры	Информация о руководящих документах	192	168	192	288	320	1160	4664(С)
	Информация о пациентах	192	224	256	360	400	1432	
	Информация о регистрационных данных	144	168	192	288	320	1112	
	Информация о главном враче	144	168	192	216	240	960	
Сервер БД	Информация о руководящих документах	240	280	320	576	720	2136	6920(В)
	Информация о пациентах	432	336	320	648	720	2456	
	Информация о регистрационных данных	432	280	320	576	720	2328	
Персонал	Информация о пациентах	192	224	256	288	320	1280	2496(Н)
	Информация о главном враче	192	224	192	288	320	1216	
Терминалы	Информация о регистрационных данных	240	224	192	216	320	1192	1192(Н)

Таким образом, подсчитаем итоговую оценку важности информационных активов поликлиники суммируя данные по направлению «затраты, необходимые для ликвидации последствий» и по направлению «влияние актива на деятельность организации» (см. таблицу 5.17).

Таблица 5.17 – Важность активов организации

Наименование актива	Вспомогательный актив	S1	S2	S	Итог
1	2	3	4	5	6
АРМ врача	Информация о руководящих документах	1158	1032	2190	Н
	Информация о пациентах	1116	1032	2148	Н
	Информация о регистрационных данных	1068	1032	2100	Н
	Информация о главном враче	960	960	1920	Н
АРМ регистратуры	Информация о руководящих документах	1290	1160	2450	С
	Информация о пациентах	1464	1432	2896	С
	Информация о регистрационных данных	1248	1112	2360	Н
	Информация о главном враче	1014	960	1974	Н
Сервер БД	Информация о руководящих документах	2016	2136	4152	С
	Информация о пациентах	2250	2456	4706	В
	Информация о регистрационных данных	1998	2328	4326	В

Продолжение таблицы 5.17

Наименование актива	Вспомогательный актив	S1	S2	S	Итог
1	2	3	4	5	6
Персонал	Информация о пациентах	1164	1280	2444	С
	Информация о главном враче	960	1216	2176	Н
Терминалы	Информация о регистрационных данных	1248	1192	2440	С

Таким образом, проведенная оценка важности показала важность таких информационных активов:

- сервер БД – высокая;
- терминалы – средняя;
- персонал – низкая;
- АРМ регистратуры – средняя;
- АРМ врача – низкая.

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломной работы был проведен анализ международных и отечественных стандартов и практик в области идентификации и оценки важности информационных активов организации, а также были рассмотрены подходы и способы идентификации и оценки важности информационных активов организации при оценке рисков информационной безопасности. По результатам выполненного анализа была разработана методика идентификации и оценки важности информационных активов организации.

Экспериментальная проверка разработанной методики и оценки важности информационных активов проведена на примере организации – поликлиника. При проведении экспериментальной проверки было выявлено, что наиболее ценный актив - сервер БД, на котором хранится информация о персонале и клиентах поликлиники. Результаты оценки важности могут быть использованы при оценке и обработки рисков для указанной организации.

Таким образом, цель дипломной работы была достигнута, задание на дипломную работу выполнено в полном объеме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Белов Е.Б, Лось В.П. Основы информационной безопасности – М.: Горячая линия - Телеком, 2006. — 544 С.
- 2 ГОСТ Р ИСО/МЭК 27001-2006 - Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
- 3 ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
- 4 ISO/IEC 27005:2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
- 5 ISO/IEC 27002:2013 «Информационные технологии. Свод норм и правил менеджмента информационной безопасности»
- 6 Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»
- 7 Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»
- 8 Питер Друкер. Практика менеджмента. — М.: Вильямс, 2007. – 400 С.
- 9 Шпак В.Ф. Методологические основы обеспечения информационной безопасности объекта – Конфидент. Защита информации. – №1. – 2000 – С. 75 – 86
- 10 Обзор системы анализа рисков ГРИФ [Электронный ресурс]: Режим доступа:<http://www.dsec.ru/products/grif/overview/start/>, свободный
- 11 Гладких А.А., В.Е. Дементьев. Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов; - Ульяновск: изд-во УлГТУ, 2009. - 168 С.

- 12 Кононов А.А. Автоматизация построения профилей защиты с использованием комплексной экспертной системы «АванГард»
- 13 Оголюк А.А., А.В. Щеглов. Технология и программный комплекс защиты рабочих станций. - М.: изд-во Финансы и статистика, 2007 г. - 280 С.
- 14 Обзор системы анализа рисков Microsoftexpert [Электронный ресурс]: Режим доступа: <http://www.microsoft.com>, свободный
- 15 Шумский А.А., Системный анализ в защите информации / А.А. Шумский, А.А. Шелупанов. - М.: Гелиос АРВ, 2008. - 224 С.
- 16 Щеглов А.Ю. / Защита информации от несанкционированного доступа. - М.: изд-во Гелиос АРВ, 2005. - 384 С.
- 17 Сидак А.А. Формирование требований безопасности сетевых информационных технологий. – М.: МГУЛ, 2001
- 18 Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003
- 19 Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации, 2014
- 20 Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009
- 21 Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. М.: Компания АйТи; ДМК Пресс, 2004
- 22 Формальная модель нарушителя информационной безопасности [Электронный ресурс]: Режим доступа: <http://www.eruditscity.ru/2543>, свободный
- 23 Процедуры оценки рисков нарушения ИБ [Электронный ресурс]: Режим доступа: <http://www.zakonprost.ru/content/base/part/648072>, свободный
- 24 Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 С.
- 25 Семенов М.И. Трубилин И.Т. и др. Автоматизированные информационные технологии в экономике: Учебник. - М., 2008

МИНОБРАЗОВАНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники
Выпускающая кафедра:
Информационная безопасность систем
и технологий
Учебная группа 11ПИ1

УТВЕРЖДАЮ

Зав. кафедрой ИБСТ

к.т.н., доцент С.Л. Зефирова

27 04 2016 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ
РАБОТУ**

студента группы 11ПИ1 Николиной Юлии Валерьевны

Специальность 100503 – Информационная безопасность
автоматизированных систем

Тема дипломного проекта: Методика идентификации и оценки важности
информационных активов организации

Руководитель ВКР

к.т.н., доцент

С.Н. Шумкин

Нормоконтролер

к.т.н., доцент

А. Г. Фатеев

1 Цели и задачи ВКР

Цель работы – разработка методики идентификации и оценки важности информационных активов организации.

Разрабатываемая методика предназначена для идентификации информационных активов организации и вычисления их оценок важности для последующей оценки рисков информационной безопасности.

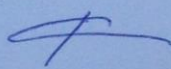
2 Тактико-технические требования к выполнению ВКР

Технические требования:

- должен быть выполнен обзор стандартов и практик по оценке рисков ИБ и определены роль и место процессов идентификации и оценки важности информационных активов;
- должен быть выполнен анализ подходов и способов идентификации и оценки важности информационных активов;
- должны быть сформированы предложения по идентификации информационных активов;
- должны быть сформированы критерии оценки важности информационных активов;
- должна быть разработана методика идентификации и оценки важности информационных активов;
- должны быть выполнены экспериментальные проверки разработанной методики идентификации и оценки важности информационных активов.

В ВКР должны быть рассмотрены следующие вопросы:

- анализ стандартов и практик в области оценки рисков ИБ, идентификации и оценки важности информационных активов;
- рассмотрение подходов и способов оценки важности информационных активов при оценке рисков ИБ;



- разработка предложений по идентификации информационных активов;
- определение критериев оценки важности информационных активов;
- разработка методики идентификации и оценки важности информационных активов;
- выполнение проверки методики идентификации и оценки важности информационных активов.

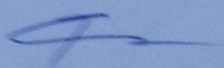
3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- стандарты и практики в области идентификации и оценки важности информационных активов – 1 л., ф. А1 (плакат);
- предложения по идентификации информационных активов – 1 л., ф. А1 (плакат);
- критерии оценки важности информационных активов – 1 л., ф. А1 (плакат);
- процесс оценки важности информационных активов – 1 л., ф. А1 (плакат);
- методика идентификации и оценки важности информационных активов – 1 л., ф. А1 (плакат);
- экспериментальная проверка методики идентификации и оценки важности информационных активов – 1 л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.



4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № 491/п от «15» 04 2016 г.

Дата выдачи задания «___» _____ 2016 г.

Время дипломного проектирования с _____ 2016 г. по _____ 2016 г.

Задание к исполнению принял «___» _____ 2016 г.

Исполнитель ВКР Мин



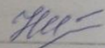
Ректору Пензенского
государственного университета
А. Д. Гулякову
студентки 5 курса ФПИТУ
очной формы обучения
Николиной Юлии Валерьевны

заявление.

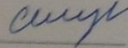
Я, Николина Юлия Валерьевна, студентка 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломной работы на тему «Методика идентификации и оценки важности информационных активов организации», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлена с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 /Ю. В. Николина/
2.06.2016г.

ВКР представлена на проверку 02.06.16г.

Руководитель ВКР  /С. Н. Шумкин/

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Методика идентификации и оценки важности информационных активов организации» студента 5 курса Ю. В. Николиной специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР к.т.н., доцент Шумкин Сергей Николаевич.

Отчет о проверке № 1

ФИО: Иванов Алексей Петрович
дата загрузки: 02.06.2016 22:23:15
пользователь: ap_ivanov@mail.ru / ID: 1267386
отчет предоставлен сервисом «Антиплагиат»
на сайте <http://www.antiplagiat.ru>

Информация о документе

№ документа: 28
Имя исходного файла: ВКР_Николина_ЮВ_11ПИ1.pdf
Размер текста: 1411 кБ
Тип документа: Не указано
Символов в тексте: 115227
Слов в тексте: 13208
Число предложений: 414

Информация об отчете

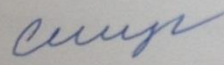
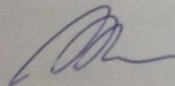
Дата: Отчет от 02.06.2016 22:23:16 - Последний готовый отчет
Комментарий: не указано
Оценка оригинальности: 75.42%
Занимательность: 24.58%
Цитирование: 0%



Оригинальность: 75.42%
Занимательность: 24.58%
Цитирование: 0%

10.06.2016 г.

Секретарь ГЭК

Шумкин С. Н.

А.П.Иванов

ОТЗЫВ

на дипломную работу студента

Николиной Юлии Валерьевны

(фамилия, имя, отчество)

Тема работы: Методика идентификации и оценки важности информационных активов организации

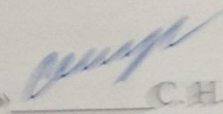
В рамках дипломной работы Николиной Ю.В. поставлена задача разработки методики идентификации и оценки важности информационных активов организации. Разработанная методика идентификации и оценки важности информационных активов может быть использована для оценки и обработки рисков ИБ, а также при обработке инцидентов ИБ организации, что обуславливает актуальность темы дипломной работы Николиной Ю.В.

Во время выполнения задания дипломником был выполнен анализ стандартов и практик в области идентификации и оценки важности информационных активов организации, а также были рассмотрены существующие практики в области идентификации и оценки важности информационных активов организации при оценке рисков ИБ. На основании полученных знаний была разработана методика идентификации и оценки важности информационных активов, которая определяет важность информационного актива на деятельность организации. Была проведена экспериментальная проверка, позволяющая оценить правильность подхода, заложенного в разработанной методике.

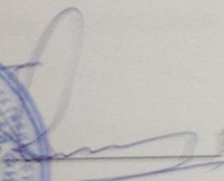
В ходе выполнения дипломной работы Николиной Ю.В. показала себя грамотным специалистом, умеющим самостоятельно принимать решения, ставить и решать технические задачи, а также продемонстрировал умение работать с научной и технической литературой.

Пояснительная записка и плакаты содержат необходимые сведения о проделанной работе и выполнены в соответствии с требованиями их отраслевых стандартов и рекомендациями методических указаний по диаграммному проектированию. Работы по всем пунктам ТЗ выполнены полностью. Считаю, что дипломный проект может быть допущен к защите в ГАК и заслуживает оценки «Хорошо», а Николина Ю.В. достойна присвоения квалификации специалиста по информационной безопасности по специальности 10.05.03 – «Информационная безопасность автоматизированных систем». Выполнение ВКР оценивается в 15 баллов.

Руководитель ВКР:

к.т.н., начальник управления ООО «НПО «Кристалл»  С.Н. Шумкин

Подпись С.Н. Шумкина заверяю:

генеральный директор ООО «НПО «Кристалл»  В.И. Шевченко



Рецензия на дипломный проект

Николиной Юлии Валерьевны

(фамилия, имя и отчество)

Тема работы: Методика идентификации и оценки важности информационных активов организации

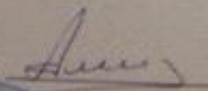
Дипломный проект Николиной Ю.В. посвящен разработке методики идентификации и оценки важности информационных активов организации.

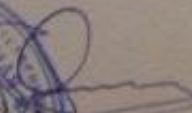
В процессе работы автором были рассмотрены существующие международные и национальные стандарты, изучены существующие методики и лучшие практики в области оценки рисков информационной безопасности, идентификации и оценки важности информационных активов. По результатам проведенного анализа была разработана методика идентификации и оценки важности информационных активов организации, выполнена ее проверка на тестовых данных.

Все пункты технического задания на дипломное проектирование выполнены в полном объеме. В ходе работы студентом продемонстрирован хороший уровень теоретических и практических знаний.

Недостатком дипломной работы является то, что экспериментальные проверки, подтверждающие правильность разработанной методики, выполнены на небольшом объеме тестовых данных.

Учитывая то, что все пункты технического задания выполнены, считаю, что выпускная квалификационная работа может быть допущена к защите в ГАК, а Николина Ю.В. достойна присвоения квалификации специалист по информационной безопасности по специальности «Информационная безопасность автоматизированных систем». С учетом актуальности ВКР, достоверности результатов ВКР, общая оценка ВКР составляет 9 баллов.

Начальник НИО-3 ООО «НПФ «Кристалл»  /Амиров А.И./

Подпись Амирова А.И. заверяю
генеральный директор ООО «НПФ «Кристалл»  /Шевченко В.И./

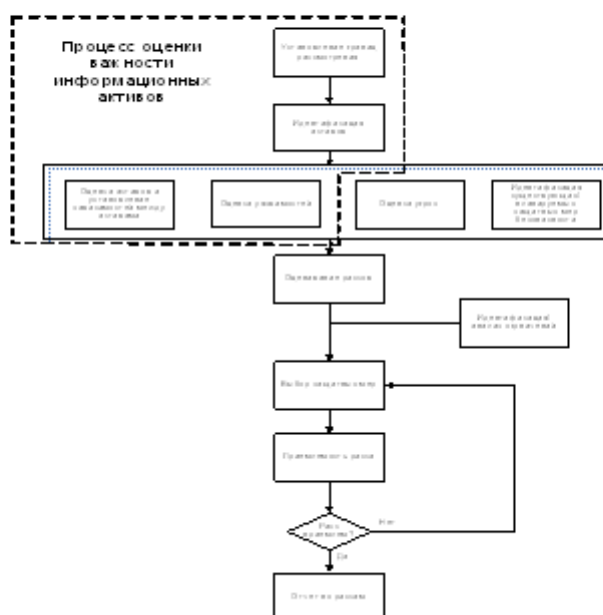


Плакат №1

Стандарты и практики в области идентификации и оценки важности информационных активов	
Международный стандарт ISO/IEC 27005:2011	Данный международный стандарт предоставляет руководство по менеджменту риска информационной безопасности. Стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001, и предполагает для содействия адекватному обеспечению информационной безопасности на основе подхода, связанного с немедленным риском.
Международный стандарт ISO/IEC 27002:2013	Международный стандарт ISO/IEC 27002 предлагает практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности, определяет основные принципы создания, реализации, поддержки и улучшения менеджмента информационной безопасности в организации.
Стандарт Банка России СТО БР ИББС-1.0-2014	Данный стандарт Банка России устанавливает требования для кредитных организаций, входящих в систему банковской системы Российской Федерации, к выбору и коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков нарушения информационной безопасности.
Рекомендации в области стандартизации Банка России РС БР ИББС-1.2-2009	Данная публикация устанавливает рекомендуемые способы и порядок проведения оценки рисков нарушения информационной безопасности и организации банковской системы Российской Федерации, являющейся составной частью системы менеджмента ИБ организации БС РФ.
Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007	В настоящем стандарте содержится рекомендации по менеджменту инцидентов ИБ в организациях для руководителей подразделений по обеспечению информационной безопасности при применении информационных технологий, информационных систем, сервисов и сетей.

Плакат №2

Предложения по идентификации информационных активов
Основной целью идентификации активов является определение наиболее важных с точки зрения целей деятельности организации информационных активов, а также вспомогательных активов, обеспечивающих надлежащие сбор, обработку и хранение таких активов, которые в свою очередь помимо собственной стоимости как имущества организации имеют ценность как средство обработки более ценного информационного актива. Прежде чем получить исходные данные для идентификации и оценки активов, необходимо определить границы рассмотрения.



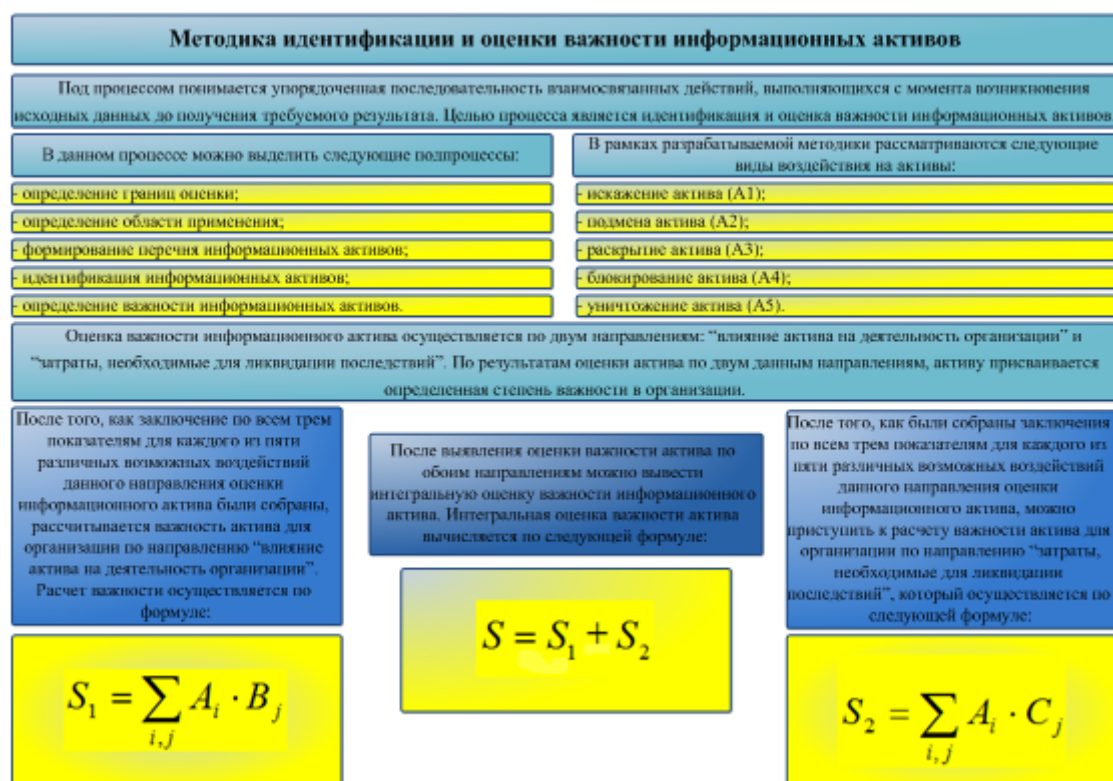
Плакаты №3



Плакаты №4

Критерии оценки важности информационных активов																	
Для определения ценности активов необходимо определить критерии и шкалу. Критерии следующие:																	
<table><tr><th colspan="3">Критерий: определение политики "защиты от инцидентов деятельности организации"</th></tr><tr><th>Качественная оценка</th><th>Количественная оценка</th><th>Критерий</th></tr><tr><td>Высокая</td><td>3</td><td>Принципы управления деятельностью, позволяющие организации</td></tr><tr><td>Средняя</td><td>6</td><td>Принципы управления деятельностью, позволяющие организации</td></tr><tr><td>Низкая</td><td>9</td><td>Принципы управления деятельностью, позволяющие организации</td></tr></table>			Критерий: определение политики "защиты от инцидентов деятельности организации"			Качественная оценка	Количественная оценка	Критерий	Высокая	3	Принципы управления деятельностью, позволяющие организации	Средняя	6	Принципы управления деятельностью, позволяющие организации	Низкая	9	Принципы управления деятельностью, позволяющие организации
Критерий: определение политики "защиты от инцидентов деятельности организации"																	
Качественная оценка	Количественная оценка	Критерий															
Высокая	3	Принципы управления деятельностью, позволяющие организации															
Средняя	6	Принципы управления деятельностью, позволяющие организации															
Низкая	9	Принципы управления деятельностью, позволяющие организации															
<table><tr><th colspan="3">Критерий: определение политики "управления критическими процессами и ресурсами"</th></tr><tr><th>Качественная оценка</th><th>Количественная оценка</th><th>Критерий</th></tr><tr><td>Высокая</td><td>3</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Средняя</td><td>6</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Низкая</td><td>9</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr></table>			Критерий: определение политики "управления критическими процессами и ресурсами"			Качественная оценка	Количественная оценка	Критерий	Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации
Критерий: определение политики "управления критическими процессами и ресурсами"																	
Качественная оценка	Количественная оценка	Критерий															
Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
<table><tr><th colspan="3">Критерий: определение политики "обеспечения безопасности информации"</th></tr><tr><th>Качественная оценка</th><th>Количественная оценка</th><th>Критерий</th></tr><tr><td>Высокая</td><td>3</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Средняя</td><td>6</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Низкая</td><td>9</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr></table>			Критерий: определение политики "обеспечения безопасности информации"			Качественная оценка	Количественная оценка	Критерий	Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации
Критерий: определение политики "обеспечения безопасности информации"																	
Качественная оценка	Количественная оценка	Критерий															
Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
<table><tr><th colspan="3">Критерий: определение политики "обеспечения безопасности информации"</th></tr><tr><th>Качественная оценка</th><th>Количественная оценка</th><th>Критерий</th></tr><tr><td>Высокая</td><td>3</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Средняя</td><td>6</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Низкая</td><td>9</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr></table>			Критерий: определение политики "обеспечения безопасности информации"			Качественная оценка	Количественная оценка	Критерий	Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации
Критерий: определение политики "обеспечения безопасности информации"																	
Качественная оценка	Количественная оценка	Критерий															
Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
<table><tr><th colspan="3">Критерий: определение политики "обеспечения безопасности информации"</th></tr><tr><th>Качественная оценка</th><th>Количественная оценка</th><th>Критерий</th></tr><tr><td>Высокая</td><td>3</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Средняя</td><td>6</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Низкая</td><td>9</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr></table>			Критерий: определение политики "обеспечения безопасности информации"			Качественная оценка	Количественная оценка	Критерий	Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации
Критерий: определение политики "обеспечения безопасности информации"																	
Качественная оценка	Количественная оценка	Критерий															
Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
<table><tr><th colspan="3">Критерий: определение политики "обеспечения безопасности информации"</th></tr><tr><th>Качественная оценка</th><th>Количественная оценка</th><th>Критерий</th></tr><tr><td>Высокая</td><td>3</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Средняя</td><td>6</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr><tr><td>Низкая</td><td>9</td><td>Внедрение политики управления критическими процессами и ресурсами, позволяющее организации</td></tr></table>			Критерий: определение политики "обеспечения безопасности информации"			Качественная оценка	Количественная оценка	Критерий	Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации	Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации
Критерий: определение политики "обеспечения безопасности информации"																	
Качественная оценка	Количественная оценка	Критерий															
Высокая	3	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Средняя	6	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															
Низкая	9	Внедрение политики управления критическими процессами и ресурсами, позволяющее организации															

Плакаты №5



Плакаты №6

Экспериментальная проверка методики идентификации и оценки важности информационных активов

После того, как заключение по всем трем показателям для каждого из пяти возможных воздействий данного направления оценки информационного актива были собраны, подсчитывается итоговая оценка важности информационных активов поликлиники. Суммируются данные по направлению «затраты, необходимые для ликвидации последствий» и по направлению «влияние актива на деятельность организации»

Наименование	Всесоответствующий актив	S1	S2	S	Итог
АРМ врача	Информация о руководящих документах	1158	1032	2190	Н
	Информация о пациентах	1116	1032	2148	Н
	Информация о регистрационных данных	1068	1032	2100	Н
	Информация о главном враче	960	960	1920	Н
АРМ регистратуры	Информация о руководящих документах	1290	1160	2450	С
	Информация о пациентах	1464	1432	2896	С
	Информация о регистрационных данных	1248	1112	2360	Н
	Информация о главном враче	1014	960	1974	Н
Сервер БД	Информация о руководящих документах	2016	2136	4152	С
	Информация о пациентах	2250	2456	4706	В
	Информация о регистрационных данных	1998	2328	4326	В
Персонал	Информация о пациентах	1164	1280	2444	С
	Информация о главном враче	960	1216	2176	Н
Терминалы	Информация о регистрационных данных	1248	1192	2440	С