МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №51 «Безопасность информационных систем

На правах рукописи

Мошак Н.Н.

Безопасность информационных систем

Учебно-методическое пособие к практическим работам

основная профессиональная образовательная программа:
09.04.02 – Информационные системы и технологии

Квалификация: бакалавр

Профиль **– Информационная безопасность**

Санкт-Петербург

2020

УДК 004.056

Мошак Н.Н. Безопасность информационных систем: учеб. метод. пособ. / ГУАП. – СПб, 2020.

Утверждено в качестве учебно-методического пособия редакционно-издательским советом университета.

Излагаются методические указания к практическим работам по курсу «Безопасность информационных систем», выполнение которых будет способствовать усвоению и закреплению пройденного теоретического курса. Пособие содержит задания к практическим работам, методические рекомендации по их выполнению. Практикум сопровождается кратким теоретическим материалом и справочной информацией. Структура практикумаотражает последовательность изложения материала в учебной программе и в учебном пособии Мошак Н.Н. Безопасность информационных систем: Учеб. пособие/ Н.Н. Мошак – СПб.: ГУАП, 2019. – 169 с. ISBN 978-5-8088-1414-1. Основное внимание в практических работах уделяется методикам расчета рисков раздела рабочей программы «Разработка модели нарушителя и угроз в информационной системе (ИС)».

Предназначено для подготовки бакалавров по профессиональной образовательной программе 10.04.01 Информационная безопасность. Профиль – Безопасность компьютерных систем.

Ответственный редактор – В.В. Овчинников.

Рецензенты – д-р.техн.наук., проф. В.А. Богатырев, д-р.техн.наук, проф. А.Н, Молдовян

Общие рекомендации по выполнению практических работ

1. Методическиеуказания по выполнению практических работ

Входевыполненияпрактических работобучающийсядолженуглубитьизакрепить знания,практическиенавыки,овладетьсовременнойметодикойитехникойэкспериментав соответствиисквалификационнойхарактеристикойобучающегося.Выполнение практических работсостоитизэкспериментально-практической,расчетно-аналитической частей и контрольных мероприятий.

Выполнениепрактических работобучающимсяявляетсянеотъемлемойчастью изучениядисциплины «Безопасность информационных систем»,определяемойучебнымпланомиотноситсяксредствам, обеспечивающимрешение следующихосновныхзадачуобучающегося:

- приобретениенавыковисследованияпроцессов,явленийиобъектов,изучаемыхв рамкахданной дисциплины;
- закрепление, развитиеи детализация теоретическихзнаний,полученныхналекциях;
- получениеновой информации поизучаемой дисциплине;
- приобретениенавыковсамостоятельнойработыслабораторнымоборудованиеми приборами.

2. Заданияитребованияк проведениюпрактических работ

Вариантзаданияпокаждойпрактической работеобучающийсяполучаетв соответствиисномеромвспискегруппы.Передпроведениемпрактической работы обучающемусяследуетвнимательноознакомиться*сметодическимиуказаниям ипоее выполнению.*Всоответствиисзаданиемобучающийсядолженподготовитьнеобходимые данные,получитьотпреподавателядопускквыполнениюпрактической работы,выполнить указаннуюпоследовательностьдействий,получитьтребуемыерезультаты,оформитьи защитить отчет попрактической работе.

3. Оформление, структура и форма отчета по практической работе

Покаждойпрактической работевыполняетсяотдельныйотчет.Титульныйлист оформляетсявсоответствиисшаблоном(образцом)приведеннымнасайтеГУАП (www.guap.ru)вразделе«Секторнормативнойдокументации».Текстовыеиграфические материалыоформляютсявсоответствиисдействующимиГОСТамиитребованиями,

приведеннымина сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

Отчет о практической работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении практической и/или лабораторной работы, описание процесса выполнения работы, полученные результаты и выводы.

Практическая работа 1

Оценка риска информационной системы на основе модели угроз и уязвимостей

1. Цель работы

Рассчитать риск информационной безопасности корпоративной информационной системы (ИС) на основе модели угроз и уязвимостей. Оценить эффективность предложенных контрмер.

2. Задание к практической работе

2.1. Разработать структурную схему «закрытого» и «открытого» контура ИС, с указанием защищаемых ресурсов.

2.2. Идентифицировать активы, которые определяют функциональность ИС.

2.3. Определить отделы, к которым относятся ресурсы (закрытого и открытого контура) и задать уровень приоритетов базовых услуг информационной безопасности («конфиденциальность», «целостность» и «доступность».

2.4. Построить модель угроз и уязвимостей для информационной системы организации. Задать вероятность реализации угрозы через данную уязвимость.

2.5. Задать критичность реализации угрозы через данную уязвимость.

2.6. Задать уровень приемлемого риска.

2.7. Рассчитать уровень угрозы по уязвимости Th с учетом критичности и вероятности реализации угрозы через данную уязвимость, а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами

2.8. Рассчитать уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами;

2.9. Рассчитать общий уровень угроз по ресурсу $CThR$ а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами;

2.10. Рассчитать риск ресурса R_{old} а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами;

2.11. Рассчитать риск по информационной системе CR с учетом рисков по всем N ресурсам: а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами;

2.12. Задать контрмеры;

2.13. Выполнить цикл алгоритма п.4.10-п.4.14;

2.14. Рассчитать и оценить эффективность принятых контрмер E. При необходимости усилить контрмеры и пересчитать риск ресурса R_{new}

3. Краткие теоретические сведения

3.1. *Описание объекта защиты*

Современные ИС строятся, как правило, на архитектуре «клиент-сервер» с применением технологии виртуальных серверов и предусматривают «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре, который может иметь различные классы защищенности, обрабатывается конфиденциальная информация с различным грифом секретности, а в «открытом» контуре - открытая информация. При этом сертифицированными средствами однонаправленной передачи информации (межсетевыми экранами (МЭ)) обеспечивается только односторонняя передача информации из «открытого» контура в «закрытый». Типовая схема организации взаимодействия контуров ИС приведена на рис.1. Вешнее взаимодействие «закрытых» контуров корпоративной ИС с осуществляется с применением сертифицированных средств криптографической защиты информации (СКЗИ) по арендованным каналам связи. Вешнее взаимодействие «открытых» контуров между собой и с другими ИС осуществляется с применением сертифицированных МЭ. Для этого могут быть использованы публичные сети общего пользования, в том числе Интернет, LTE и др. с организацией виртуальных частных сетей (VirtualPrivateNetwork, VPN).

В качестве базового сетевого протокола используется IP-протокол.

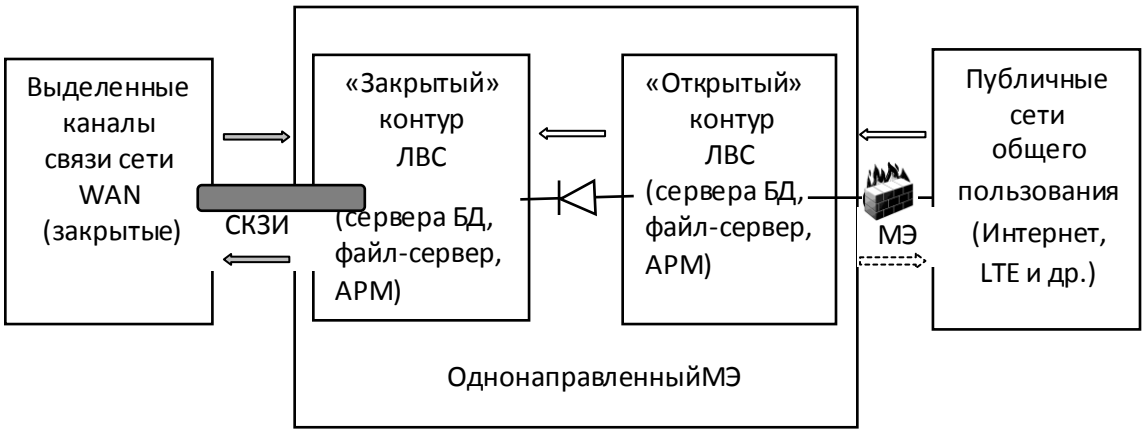

Рис. 1 - Обобщенная схема информационных потоков в ИС

В общем случае корпоративная ИС на технологии «клиент-сервер» включает в себя следующие функциональные компоненты:

- сервера СУБД и файл-сервера, осуществляющие обработку и хранение информации;

- автоматизированные рабочие места (АРМ) - оконечное абонентскоеоборудование ИС;
- корпоративная мультисервисная сеть связи на основе IP-QoS технологий, включающая в себя ЛВС центрального офиса организации и ее филиалов, «закрытую» WAN-компоненту, обеспечивающую связь территориально удаленных «закрытых» контуров ЛВС ИС организации. Связь территориально удаленных «открытых» контуров ЛВС ИС организации осуществляется по сетям общего пользования (Интернет, мобильные сети). Компоненты корпоративной сетивключают в себя оборудование ЛВС, оборудование структурированной кабельной системы ЛВС, сетевое оборудование(концентраторы, коммутаторы, маршрутизаторы, мультиплексоры, межсетевые экраны и т. д.), внешние арендованные каналы связи, а также системы и средства защиты информации.

3.2. *Анализ рисков в ИС*

Анализ рисков — это то, с чего должно начинаться построение политики информационной безопасности (ИБ) ИС. Он включает в себя мероприятия по обследованию безопасности ИС, целью которых является определение того, какие активы ИС и от каких угроз надо защищать, а также, в какой степени те или иные активы нуждаются в защите. В процессе анализа рисков проводятся следующие работы:

– идентификация и определение ценности всех активов в рамках выбранной области деятельности;

– идентификация угроз и уязвимостей для идентифицированных активов;

– оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;

– выбор критериев принятия рисков;

– подготовка плана обработки рисков.

3.2.1. Идентификация и определение ценности активов

Необходимо идентифицировать только те активы, которые определяют функциональность ИС и существенны с точки зрения обеспечения безопасности. Важность (или стоимость) актива определяется величиной ущерба, наносимого в случае нарушения его конфиденциальности, целостности или доступности. В ходе оценки стоимости активов определяется величина возможного ущерба для каждой его категории при успешном осуществлении угрозы. В ИС организации хранятся и обрабатываются различные виды открытой и служебной конфиденциальной информации. Прежде всего, следует определить**,** что является*ценным активом*организации с точки зрения информационной безопасности.

В процессе категорирования активов необходимо оценить ихважность для бизнес-процессов организации или, другими словами, определить,какой ущерб понесет компания в случае нарушения

информационнойбезопасностиактивов. Данный процесс вызывает наибольшую сложность, так как *ценностьактивовопределяетсянаосновеэкспертныхоценокихвладельцев*.В процесседанного этапа часто проводятся обсуждения между консультантами поразработкесистемыуправленияивладельцамиактивов.Этопомогаетпослед нимпонять, каким образом следует определять ценность активов с точкизренияинформационной безопасности (как правило, процесс определениякритичности активов является для владельца новым и нетривиальным). Следует определить, нарушение информационной безопасностикакихактивов может нанести ущерб организации. В этом случае актив будетсчитатьсяценным, и его необходимо будет учитывать при оценкеинформационныхрисков. Инвентаризация заключается в составлении перечня ценныхактивоворганизации. Как правило, данный процесс выполняют владельцыактивов.

Кроме этого,длявладельцев активов разрабатываются различные методики оценки. В частности, такие методики могут содержать конкретные критерии (актуальныедляданной организации), которые следует учитывать при оценкекритичности: конфиденциальность, целостность и доступность (следует оценить ущерб,которыйпонесет компания при нарушении конфиденциальности, целостности илидоступностиактивов).

Оценку критичности активов можно выполнять в денежных единицах ивуровнях. Однако, учитывая тот факт, что для анализа информационныхрисковнеобходимы значения в денежных единицах, в случае оценки критичностиактивов в уровнях, следует определить оценку каждого уровня в деньгах.Например,длябазовойоценкирисковдостаточно3-уровневойшкалыоценкикритичности:низкий,среднийивысокийуровни.При выборе шкалы важно учитыватьследующее:

– чем меньше количество уровней, тем ниже точностьоценки;

– чем больше количество уровней, тем выше сложность оценки (сложно определить разницу между, скажем, 7-м и 8-м уровнем 10-уровневой шкалы).

Кроме этого, следует иметь в виду, что для расчетаинформационныхрисков достаточно примерных значений критичности активов: необязательнооценивать их с точностью до денежной единицы. Однако денежноевыражениекритичности все равнонеобходимо.

Стандарт ISO 17799,подробно описывающий процедуры системы управления ИБ, выделяетследующиевидыактивов:

– *информационные ресурсы* (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, техническая документация, обучающие материалы и пр.);

– *программное обеспечение*;

– *материальные активы* (компьютерное оборудование, средства телекоммуникаций и пр.);

– *сервисы* (поддерживающая инфраструктура);

– *сотрудники организации*, их квалификация и опыт;

– *нематериальные ресурсы* (репутация и имидж организации).

Информационные ресурсы. Различаются следующие категории информационных ресурсов, подлежащих защите:

– *информация, составляющая государственную тайну;*

– *конфиденциальная информация ограниченного доступа (включая коммерческую тайну, служебную тайну и персональные данные), принадлежащая третьей стороне;*

– *данные, критичные для функционирования ИС и работы бизнес подразделений.*

Для первых двух категорий информационных ресурсов в качестве основной угрозы безопасности рассматривается нарушение *конфиденциальности* информации путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

К последней категории относятся информационные ресурсы предприятия, нарушение *целостности или доступности* которых может привести к сбоям функционирования ИС либо бизнес-подразделений.

Информационные активы (или виды информации) оцениваются сточки зрения нанесения организации ущерба от их раскрытия, модификацииилинедоступности в течение определенноговремени.

Программное обеспечение,материальные ресурсы и сервисы.Программное обеспечение, материальные ресурсы и сервисыоцениваются, как правило, с точки зрения *их доступности* илиработоспособности,т. е. требуется определить, какой ущерб понесет компания принарушениифункционирования данных активов. Например, нарушение системыкондиционирования в течение трех суток приведет к отказу серверов организациикним будет нарушен доступ и вследствие этого компания понесет убытки.

Сотрудники организации. Сотрудники организации с точки зрения конфиденциальности ицелостности оцениваются, учитывая их доступ к информационным ресурсам справами на чтение и на модификацию. Оценивается,какой ущерб понесет компания при отсутствии сотрудника в течениеопределенного периода времени. Здесь важно учесть опыт сотрудника, егоквалификацию, выполнение им каких-либо специфическихопераций.

Репутация организации. Репутация организации оценивается в связи с информационнымиресурсами: какой ущерб репутации организации будет нанесен в случаенарушениябезопасности информацииорганизации.

Заметим, что процесс категорирования активов должен подчинятьсячетким документированным процедурам организации. Аудиторамсертификационного органа будет недостаточно формального документа, отражающегорезультаты категорирования. От владельцев активов требуется, чтобы они моглиобъяснить,какиеметодикионииспользовалиприоценке,наоснованииика кихданных были получены результатыоценки.

3.2.2. Определениеугроз и уязвимостей для идентифицированных активов

Очевидно, что для анализа информационных рисков необходимо оценить не только критичность активов, но и уровень их защищенности. В процессе оценки защищенности информационной системыопределяютсяугрозы,действующиенаактивы,атакжеуязвимостиинф ормационнойсистемы, в которой обрабатываются активы и которые могут привести креализации угроз. *Угрозы и уязвимости рассматриваются только во взаимосвязидруг с другом*, так как ***инцидент***–событие, указывающее на действительную, мнимую или вероятную реализацию угрозы, возникает в случае появления комплементарной пары «угроза-уязвимость»). Уязвимость, через которую невозможно реализовать ни однуизугроз, не имеет смысла. Аналогично, угроза, которую невозможнореализоватьввиду отсутствия уязвимости, такженеактуальна.

Невызываетсомнения,чторазличныеугрозыиуязвимостиимеютразное значение (разный вес) для информационной системы. Следовательно, необходимо определить, какие угрозы и уязвимости наиболее актуальны,или, другими словами, определить вероятностьреализации угрозы через уязвимость. *Под уровнем угрозы понимается вероятность ее осуществления.* Оценка угроз включает в себя:

–определение уязвимых мест системы;

–анализ вероятности угроз, направленных на использование этих уязвимых мест;

–оценка последствий успешной реализации каждой угрозы;

–оценка стоимости возможных мер противодействия;

–выбор оправданных механизмов защиты (возможно, с использованием стоимостного анализа).

Оценка уязвимостей активов ИС, обусловленных слабостями их защиты, предполагает определение вероятности успешного осуществления угроз безопасности.

Угрозы и уязвимости, а также их вероятность определяются врезультатепроведения технологического аудита защищенности информационнойсистемыорганизации. Такой аудит может быть выполнен как специалистамиорганизации(так называемый, внутренний аудит), так и стороннимиконсультантами(внешнийаудит).

3.2.3. Оценка рисков для возможных случаев успешной реализации угроз информационной безопасности

Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей. Величина риска определяется на основе стоимости актива, уровня угрозы и величины уязвимости. С их увеличением возрастает и величина риска. Оценка рисков состоит в том, чтобы выявить существующие риски и оценить их величину, т. е. дать им количественную оценку.Классическая формула оценки информационного риска:

$$R=P(V)\,D,$$

где R– информационный риск; D– величина возможного ущерба; $P(V)$– вероятность реализации определенной угрозы через некоторые уязвимости.

Разработка методики оценки риска – достаточно трудоемкая задача. Во-первых, такая методика должна всесторонне описывать информационную систему, ее ресурсы, угрозы и уязвимости. Задача заключается в том, чтобы построить максимально гибкую модель информационной системы, которую можно было бы настраивать в соответствии с реальной системой. Во-вторых, методика оценки рисков должна быть предельно прозрачна, чтобы владелец информации, использующий ее, мог адекватно оценить ее эффективность и применимость к своей конкретной системе. На сегодняшний день существует два основных метода оценки рисков информационной безопасности, основанных на построении: модели угроз и уязвимостей и модели информационных потоков.

3.2.4. Выбор критерия принятия рисков

Выбор критериев принятия рисков лежит в основе этапа обработки информационных рисков, в процессе которого определяется какие действия по отношению к рискам требуется выполнить в организации. Основные критерии обработки рисков:

– принятие рисков;
– уклонение от рисков;
– передача рисков;
– снижение рисков.

Принятие рисков осуществляется в том случае, если уровень рисковпризнается приемлемым, т. е. компания не считает целесообразнымприменятькакие-либо меры по отношению к этим рискам и готова понестиущерб.

Уклонение от рисков —полное устранение источникариска.

Передача рисков — перенесение ответственности за риск на третьилица(например, поставщика оборудования или страховую компанию) безустранения источникариска.

Снижение рисков — выбор и внедрение мер по снижениювероятностинанесенияущерба.

В процессе обработки рисков сначала требуется определить, какие изнихтребуют дальнейшей обработки, а какие можно принять. Как правило, эторешается с помощью оценки приемлемого уровня риска. Риски, равные илинижеприемлемого, можно принять. Очевидно, что для рисков, превышающихприемлемый уровень, требуется выбрать дальнейшие меры по обработке.Приемлемый уровень риска определяется руководством организации илиспециальнойгруппой, в которую входят руководители и главные финансистыорганизации.Например, если руководство организации декларирует, что низкий уровеньрискасчитается приемлемым, то дальнейшие действия по обработке рисковопределяются только для средних и высоких уровней риска, причем средний ивысокий уровни риска требуется снизить до низкого (приемлемого)уровня.

В случае, когда в организации наблюдается большой разброс значенийриска(какправило,этоможетвозникнуть,есликритичностьактивовбылаопределена в денежных единицах, а не уровнях), информационные рискиможноразбить на категории и определять приемлемый уровень для каждой из нихотдельно.Этовызванотем,чтоснижатьразличныезначениярисковдоодногозаданного значения не всегда целесообразно (часто для снижениявысокихрисков до заданного уровня необходимы неоправданно большиезатраты).

3.2.5. Подготовка плана обработки рисков

По результатам этапа «Выбор критериев принятия рисков» составляется «*Отчет об обработке информационных рисков организации*», который подробно описывает методы обработки рисков. Кроме этого, составляется «*План снижения рисков*», где четко описываются конкретные меры по снижению рисков, сотрудники, ответственные за выполнение каждого положения плана, сроки выполнения плана. *Данный документ содержит перечень первоочередных мероприятий по снижению уровней рисков, а также цели и средства управления, направленные на снижение рисков, с указанием:*

– лиц, ответственных за реализацию данных мероприятий и средств;

– сроков реализации мероприятий и приоритетов их выполнения;

– ресурсов для реализации таких мероприятий;

– уровней остаточных рисков после внедрения мероприятий и средств управления.

Определение набора адекватных контрмер осуществляется в ходе построения подсистемы ИБ ИС и управления рисками. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть тем больше, чем меньше вероятность причинения ущерба. Контрмеры могут способствовать уменьшению величины рисков различными способами:

– уменьшая вероятность осуществления угроз безопасности;

– ликвидируя уязвимости или уменьшая их величину;

– уменьшая величину возможного ущерба;

– выявляя атаки и другие нарушения безопасности;

– способствуя восстановлению ресурсов ИС, которым был нанесен ущерб.

4. Последовательность выполнения работы

Основные понятия и допущениямодели

Базовые угрозы информационной безопасности – нарушениеконфиденциальности, нарушение целостности и отказ вобслуживании.

Ресурс – любой контейнер, предназначенный для хранения информации,подверженный угрозам информационной безопасности (сервер, рабочаястанция,переноснойкомпьютер).

Свойствами ресурса являются: перечень угроз, воздействующих на него, икритичностьресурса.

Угроза–

действие,котороепотенциальноможетпривестикнарушениюбезопасности.

Свойством угрозы является перечень уязвимостей, при помощи которыхможетбыть реализованаугроза.

Уязвимость – это слабое место в информационной системе, котороеможетпривести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализацииугрозычерез данную уязвимость и критичность реализации угрозы через даннуюуязвимость.

***Критичностьресурса*(D)**–ущерб,которыйпонесеткомпанияотпотериресурса. Задается в уровнях (количество уровней может быть в диапазоне от 2до 100 или в деньгах. В зависимости от выбранного режима работы, можетсостоять из критичности ресурса по конфиденциальности, целостности идоступности (D_c , D_i, D_a).

Критичность реализации угрозы **(*ER*)** – степень влияния реализацииугрозына ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса.Задается в процентах. Состоит из критичности реализации угрозы поконфиденциальности, целостности и доступности (ER_c , ER_i, ER_a).

***Вероятность реализации угрозы через данную уязвимость в течениегода*(P(V))** – степень возможности реализации угрозы через данную уязвимостьвтех или иных условиях. Указывается впроцентах.

Максимальное критичное время простоя **(**T_{max}**)** – значение временимаксимального простоя, которое является критичным для организации. Т.е. ущерб, нанесенныйорганизации при простаивании ресурса в течение критичного временипростоя,максимальный. При простаивании ресурса в течение времени,превышающегокритичное, ущерб, нанесенный организации, неувеличивается.

4.1. Разработать структурную схему «закрытого» и «открытого» контура ИС, с указанием защищаемых ресурсов;

4.2. Идентифицировать активы, которые определяют функциональность

ИС и существенны с точки зрения обеспечения безопасности и определить их ценность

–аппаратные ресурсы «закрытого» (сервер БД, СКЗИ, однонаправленный МЭ, оборудование ЛВС, АРМ пользователей) контура и «открытого» контура (сервер БД, Proxy-сервер, внешний МЭ, оборудование ЛВС, АРМ пользователей);

–информационные ресурсы «закрытого» и «открытого» контура (БД);

–программные ресурсы «закрытого» и «открытого» контура (ОС, СУБД, прикладное ПО);

–людские ресурсы;

–имидж организации.

4.3. Определить отделы, к которым относятсяресурсы (закрытого и открытого контура).

4.4. Задать уровень приоритетов базовых услуг информационной безопасности («конфиденциальность», «целостность» и «доступность» с учетом уровня конфиденциальности обрабатываемой информации в «закрытом» и «открытом» контуре. Сточкизрениябазовыхугрозинформационнойбезопасностисуществуетдварежима работыалгоритма, реализующего метод оценки рисков, основанный на модели угроз и уязвимостей

а) одна базовая угроза (суммарная);

б) три базовые угрозы.

4.5. Задать критичностьресурса (величина ущерба D).

4.6. Определить угрозы, действующие наресурсы (сформулировать самостоятельно с учетом лекционного материала) и уязвимости, через которые реализуютсяугрозы (сформулировать самостоятельно с учетом лекционного материала); Построить модель угроз и уязвимостей для информационной системы организации (анализируются угрозы, действующие на каждый ресурс информационной системы, и уязвимости, через которые возможна реализация угроз).

4.7. Задать вероятность реализации угрозы через данную уязвимость (на основе полученной модели проводится анализ вероятности реализации угроз информационной безопасности на каждый ресурс).

4.8. Задать критичность реализации угрозы через даннуюуязвимость (задать самостоятельно).

4.9. Задать уровень приемлемого риска (например, 10% от предполагаемого ущерба), которым оцениваются принятые контрмеры.

4.10. Рассчитать уровень угрозы по уязвимости Th с учетом критичности и вероятности ее реализации через конкретную уязвимость. Уровень угрозы показывает, насколько критичным являетсявоздействиеданной угрозы на ресурс с учетом вероятности

ереализации. Вычисляется одно значение (для суммарной угрозы). Получается значение уровня угрозы по уязвимости в интервале от 0 до 1.

а)для режима с одной базовойугрозой

$$Th = \frac{ER}{100} \times \frac{P(V)}{100},$$

гдеER (%) - критичность реализации угрозы,

$P(V)$ (%) – вероятность реализации угрозы через данную уязвимость

б) для режима с тремя базовымиугрозами:

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где$ER_{c,i,a}$ (%) - критичность реализации угрозы для каждой базовой услуги безопасности,

$P(V)_{c,i,a}$ (%) – вероятность реализации угрозы через данную уязвимостьдля каждой базовой услуги безопасности.

4.11. Рассчитать уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh

а)для режима с одной базовойугрозой

$$CTh = 1 - \prod_{n=1}^{N} (1 - Th)$$

б) для режима с тремя базовымиугрозами$CThc, i, a$(%)

$$CTh_c = 1 - \prod_{n=1}^{N} (1 - Th_c)$$

$$CTh_i = 1 - \prod_{i=1}^{n} (1 - Th_i)$$

$$CTh_a = 1 - \prod_{n=1}^{N} (1 - Th_a)$$

Значения *уровня угрозы по всем пуязвимостям (n=1,2,…,N)* получаются в интервале от 0 до1.

4.12. Рассчитать общий уровень угроз по ресурсу $CThR$

а)для режима с одной базовойугрозой

$$CThR = 1 - \prod_{n=1}^{N} (1 - Th)$$

б) для режима с тремя базовымиугрозами$CThc, i, aRc, i, a$(%)

$$CTh_cR_c = 1 - \prod_{n=1}^{N} (1 - Th_c)$$

$$CTh_iR_i = 1 - \prod_{n=1}^{N} (1 - Th_i)$$

$$CTh_aR_a = 1 - \prod_{n=1}^{N} (1 - Th_a)$$

Значение *общего уровня угрозы по ресурсу* получается в интервале от 0 до1.

4.13. Рассчитать риск ресурса R

а)для режима с одной базовойугрозой

$$R_{old} = CThR \times D$$

где D – критичность ресурса для одной базовой угрозы. Задается в деньгах илиуровнях.

б) для режима с тремя базовымиугрозами

$$R_c = CTh_c R_c \times D_c$$
$$R_i = CTh_i R_i \times D_i$$
$$R_a = CTh_a R_a \times D_a$$
$$R_{old\,(c,i,a)} = (1 - \prod_{n=1}^{3} \left(1 - 1 - \frac{R_n}{100}\right)) \times 100$$

$R_{old\,(c,i,a)}$ – суммарный риск по трем угрозам

D_c, D_i, D_a – критичность ресурса по трем базовым угрозам. Задается в деньгах илиуровнях.В случае угрозы *доступность* (отказ в обслуживании) критичность ресурса вгодвычисляется по следующейформуле:

$$D_{a\,/yer} = D_{a\,/oure} \times T$$

Для остальных угроз критичность ресурса задается вгод.

4.14. Рассчитать риск по информационной системе CR с учетом рисков по всем N ресурсам

а) для режима с одной базовойугрозой:

-для режима работы вденьгах:

$$CR = \sum_{n=1}^{N} R_n$$

- для режима работы вуровнях:

$$CR = (1 - \prod_{n=1}^{N} \left(1 - \frac{R_n}{100}\right)) \times 100$$

б) для режима работы с тремяугрозами:

- для режима работы вденьгах:

$$CR_{c,i,a} = \sum_{n=1}^{N} R_n$$
$$CR = \sum_{n=1}^{N} CR_{c,i,a}$$

$CR_{c,i,a}$- риск по системе по каждому видубазовыхугроз

CR- риск по системе суммарно по трем видамугроз

- для режима работы вуровнях:

$$CR_{c,i,a} = (1 - \prod_{n=1}^{N} \left(1 - \frac{R_n}{100}\right)) \times 100$$

$$CR = (1 - \prod_{n=1}^{3} \left(1 - \frac{R_{c,i,a}}{100}\right)) \times 100$$

4.15. Задание контрмер для угроз и/или уязвимостей (пересмотреть модель угроз и уязвимостей).

4.16. Для расчета эффективности введенной контрмеры необходимо

пройти последовательно по всему алгоритму п.4.10-п.4.14 с учетом заданной контрмеры. Таким образом, на выходе пользователь получает значение двух рисков – значение риска без учета контрмеры (R_{old}) и значение риска с учетом заданной контрмеры (R_{new}) (т.е. с учетом того, что уязвимость или угроза закрыта).

4.17. Рассчитать эффективность (E) введения контрмеры рассчитывается по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

4.18. Принять или отклонить R_{new} (если эффективность введенных контрмер недостаточна, т.е. рассчитанный уровень ущерба превышает заданный уровень (например, 10%), то необходимо усилить контрмеры и пересчитать R_{new}).

5. Методические рекомендации по выполнению работы

(Расчет рисков приведен только для одной угрозы информационнойбезопасности и одного ресурса (аппаратного), т. к. для остальных ресурсов риск рассчитываетсяаналогично).

5.1. Модель угроз и уязвимостей аппаратных ресурсов ИС

Уровень приемлемого риска принимаем равным 10% от предполагаемого ущерба по ресурсу.

Модель угроз и уязвимостей приведена в табл.5.1:

Таблица 5.1

Ресурс	*Угрозы*	*Уязвимости*
1.Сервер закрытого контура (критичность ресурса 100у.е)	1.Неавторизованное проникновение нарушителявнутрьохраняемогопериметра	1.Отсутствиерегламента доступа впомещения с ресурсами, содержащими ценнуюинформацию 2. Отсутствиесистемы видеонаблюдения
	2.Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе	1.Отсутствиеавторизации для внесения изменений в системуэлектроннойпочты 2.Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции
	3. Разглашение конфиденциальной информации сотрудниками организации	1.Отсутствиесоглашений оконфиденциальности 2. Распределение атрибутов безопасности (ключи доступа,

		шифрования) между несколькими доверенными сотрудниками
2.Сервер открытого контура (критичность ресурса 120у.е)	1. Угроза некорректного использования функционала программного и аппаратного обеспечения	1. Отсутствие настроек авторизации пользователей 2. Слабая система хранения паролей
	2.Угроза доступа неавторизированных пользователей к файловой системе	1. Отсутствие настроек авторизации пользователей 2.Слабая технология защиты файловой системы
	3 Угроза длительного удержания вычислительных ресурсов пользователями	1.Слабый механизм балансировки нагрузки 2. Отсутствие настроек авторизации пользователей
3.МЭ открытого контура (критичность ресурса 80у.е)	1. Отказ в обслуживании	1.Отсутствиерезервного межсетевого экрана 2.Низкая пропускная способность межсетевого экрана
	2. Разглашение текущей конфигурации устройства	1. Отсутствиесоглашений оконфиденциальности 2. Отсутствие системы аутентификации
	3 Неавторизованный доступ к настройке МЭ	1. Отсутствие настроек авторизации пользователей 2. Использование устаревших алгоритмов аутентификации для хранения паролей
4.СКЗИ закрытого контура (критичность ресурса 50у.е)	1.Отказ в обслуживании	1.Отсутствиемежсетевого экрана 2. Отсутствие аутентификации при подключении к зашифрованному каналу
	2.Угроза анализа криптографических алгоритмов и их реализации	1. Использование слабых криптографических алгоритмов 2.Наличие ошибок в программном коде криптографических средств

	3.Неограниченный доступ нарушителя к информации	1.Использование слабых или устаревших криптографических алгоритмов 2. Отсутствие соглашения о конфиденциальности
5. Однонаправленный МЭ (критичность ресурса 73у.е)	1.Отказ в обслуживании	1.Отсутствие резервный межсетевой экран 2.Низкая пропускная способность шлюза
	2.Реализацияатаки «ManintheMiddle» путем возможного подключения к закрытому каналу	1. Отсутствие криптографических средств, применяемых к передаваемой информации 2.Отсутствие контроля доступа к закрытому каналу
	3.Угроза перехвата привилегированного потока	1. Наличие ошибок в программном коде криптографических средств 2. Отсутствие аутентификации при подключении к закрытому каналу
6. Оборудование ЛВС открытого контура (критичность ресурса 99 у.е)	1. Перехват передаваемых сообщений	1.Неправильная конфигурация средств криптографических средств защиты информации 2.Использование алгоритмов шифрования с недостаточной длиной ключа
	2.Модификация и удаление передаваемых сообщений	1. Отсутствие алгоритмов аутентификации 2. Использование устаревшего алгоритма аутентификации
	3.Прослушивание привилегированного трафика	1.Отсутствие криптографической защиты, применяемой к пакетам данных 2.Отсутствие контроля доступа к защищенному каналу
7. Оборудование ЛВС закрытого контура (критичность ресурса 85у.е)	1. Прослушивание привилегированного трафика	1. Отсутствие криптографической защиты, применяемой к пакетам данных 2. Отсутствие контроля

	доступа к защищенному каналу
2.Модификация и удаление передаваемых сообщений	1. Отсутствие алгоритмов аутентификации 2. Использование устаревшего алгоритма аутентификации
3.Перехват передаваемых сообщений	1. Неправильная конфигурация средств криптографических средств защиты информации 2. Отсутствие регламента смены пароля

5.2. Расчет вероятности и критичности для каждой угрозы для аппаратных ресурсов приведен в табл.5.2.

Таблица 5.2

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через уязвимость (%), ER
	Сервер закрытого контура	
Угроза1/Уязвимость 1	95	70
Угроза1/Уязвимость 2	75	50
Угроза2/Уязвимость 1	70	50
Угроза2/Уязвимость 2	85	70
Угроза3/Уязвимость 1	70	20
Угроза3/Уязвимость 2	55	20
	Сервер открытого контура	
Угроза1/Уязвимость 1	50	50
Угроза1/Уязвимость 2	80	70
Угроза2/Уязвимость 1	20	20
Угроза2/Уязвимость 2	15	10
Угроза3/Уязвимость 1	70	60
Угроза3/Уязвимость 2	40	20
	МЭ открытого контура	
Угроза1/Уязвимость 1	70	30
Угроза1/Уязвимость 2	60	50
Угроза2/Уязвимость 1	80	50
Угроза2/Уязвимость 2	45	50
Угроза3/Уязвимость 1	35	30
Угроза3/Уязвимость 2	50	60
	СКЗИ закрытого контура	
Угроза1/Уязвимость 1	30	20
Угроза1/Уязвимость 2	90	70
Угроза2/Уязвимость 1	30	10
Угроза2/Уязвимость 2	40	30
Угроза3/Уязвимость 1	30	30
Угроза3/Уязвимость 2	50	60
	Однонаправленный шлюз	
Угроза1/Уязвимость 1	70	70

Угроза1/Уязвимость 2	90	50
Угроза2/Уязвимость 1	40	50
Угроза2/Уязвимость 2	60	30
Угроза3/Уязвимость 1	50	30
Угроза3/Уязвимость 2	40	30
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	20	40
Угроза1/Уязвимость 2	60	40
Угроза2/Уязвимость 1	70	50
Угроза2/Уязвимость 2	40	20
Угроза3/Уязвимость 1	20	10
Угроза3/Уязвимость 2	50	30
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	70	50
Угроза1/Уязвимость 2	50	30
Угроза2/Уязвимость 1	90	70
Угроза2/Уязвимость 2	95	70
Угроза3/Уязвимость 1	55	40
Угроза3/Уязвимость 2	60	40

5.3. Расчёт уровня угрозы по уязвимости Th и уровня угрозы по всем уязвимостям, через которые реализуется данная угроза CTh

Результаты расчета приведены в табл. 5.3.

Таблица5.3

Угроза/Уязвимость	Уровень угрозы (%), Th $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$
Сервер закрытого контура		
Угроза1/Уязвимость 1	0,665	0,791
Угроза1/Уязвимость 2	0,375	
Угроза2/Уязвимость 1	0,35	0,737
Угроза2/Уязвимость 2	0,595	
Угроза3/Уязвимость 1	0,14	0,235
Угроза3/Уязвимость 2	0,11	
Сервер открытого контура		
Угроза1/Уязвимость 1	0,25	0,67
Угроза1/Уязвимость 2	0,56	
Угроза2/Уязвимость 1	0,04	0,054
Угроза2/Уязвимость 2	0,015	
Угроза3/Уязвимость 1	0,42	0,466
Угроза3/Уязвимость 2	0,08	
МЭ открытого контура		
Угроза1/Уязвимость 1	0,21	0,447
Угроза1/Уязвимость 2	0,3	
Угроза2/Уязвимость 1	0,4	0,535
Угроза2/Уязвимость 2	0,225	

Угроза3/Уязвимость 1	0,105	0,374
Угроза3/Уязвимость 2	0,3	
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	0,06	0,652
Угроза1/Уязвимость 2	0,63	
Угроза2/Уязвимость 1	0,03	0,146
Угроза2/Уязвимость 2	0,12	
Угроза3/Уязвимость 1	0,09	0,363
Угроза3/Уязвимость 2	0,3	
Однонаправленный шлюз		
Угроза1/Уязвимость 1	0,49	0,72
Угроза1/Уязвимость 2	0,45	
Угроза2/Уязвимость 1	0,2	0,344
Угроза2/Уязвимость 2	0,18	
Угроза3/Уязвимость 1	0,15	0,252
Угроза3/Уязвимость 2	0,12	
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	0,08	0,301
Угроза1/Уязвимость 2	0,24	
Угроза2/Уязвимость 1	0,35	0,402
Угроза2/Уязвимость 2	0,08	
Угроза3/Уязвимость 1	0,02	0,167
Угроза3/Уязвимость 2	0,15	
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	0,35	0,448
Угроза1/Уязвимость 2	0,15	
Угроза2/Уязвимость 1	0,63	0,876
Угроза2/Уязвимость 2	0,665	
Угроза3/Уязвимость 1	0,22	0,407
Угроза3/Уязвимость 2	0,24	

5.4. Расчет общего уровня угроз, действующих на ресурс, а также вычислим риск каждого ресурса. Результаты приведены в табл.5.4:

Таблица5.4

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), $CThR$ $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	Риск ресурса для режима с одной общейугрозой (%), R_{old} $R_{old} = CThR \cdot D$
Сервер закрытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,958	0,958x150=143,70
Сервер открытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2	0,833	120x0,833=99,96

Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2		
МЭ открытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,839	80x0,839=67,12
СКЗИ закрытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,811	40,55
Однонаправленный шлюз		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,863	62,999
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,652	64,548
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,959	81,515

5.5. Контрмеры:

- Ввести систему видеонаблюдения в серверных;
- Составить соглашение о конфиденциальностидля сотрудников;
- Ввести ролевую систему доступа на сервере;
- Установить резервный межсетевой экран в открытой зоне;
- Настроить аутентификацию при удаленном и консольном подключении ко всем устройствам;
- Поставить межсетевой экран на защищенный канал;
- Настроить аутентификацию при подключении к зашифрованному каналу;

- Повысить пропускную способность шлюза;
- Настроить более современные алгоритмы шифрования;
- Увеличить длину ключей шифрования.

5.6. Расчет вероятности реализации угрозы с учетом контрмер. Результаты приведены в табл.5.5:

Таблица5.5

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), $P(V$	Критичность реализации угрозы через уязвимость (%), ER
	Сервер закрытого контура	
Угроза1/Уязвимость 1	5	70
Угроза1/Уязвимость 2	7	50
Угроза2/Уязвимость 1	11	50
Угроза2/Уязвимость 2	8	70
Угроза3/Уязвимость 1	5	20
Угроза3/Уязвимость 2	7	20
	Сервер открытого контура	
Угроза1/Уязвимость 1	10	50
Угроза1/Уязвимость 2	10	70
Угроза2/Уязвимость 1	7	20
Угроза2/Уязвимость 2	5	10
Угроза3/Уязвимость 1	11	60
Угроза3/Уязвимость 2	9	20
	МЭ открытого контура	
Угроза1/Уязвимость 1	5	30
Угроза1/Уязвимость 2	8	50
Угроза2/Уязвимость 1	9	50
Угроза2/Уязвимость 2	10	50
Угроза3/Уязвимость 1	5	30
Угроза3/Уязвимость 2	5	60
	СКЗИ закрытого контура	
Угроза1/Уязвимость 1	5	20
Угроза1/Уязвимость 2	10	70
Угроза2/Уязвимость 1	5	10
Угроза2/Уязвимость 2	5	30
Угроза3/Уязвимость 1	5	30
Угроза3/Уязвимость 2	7	60
	Однонаправленный шлюз	
Угроза1/Уязвимость 1	10	70
Угроза1/Уязвимость 2	9	50
Угроза2/Уязвимость 1	5	50
Угроза2/Уязвимость 2	3	30
Угроза3/Уязвимость 1	5	30
Угроза3/Уязвимость 2	3	30
	Оборудование ЛВС открытого контура	
Угроза1/Уязвимость 1	5	40
Угроза1/Уязвимость 2	10	40
Угроза2/Уязвимость 1	10	50
Угроза2/Уязвимость 2	7	20
Угроза3/Уязвимость 1	5	10

Угроза3/Уязвимость 2	5	30
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	8	50
Угроза1/Уязвимость 2	10	30
Угроза2/Уязвимость 1	5	70
Угроза2/Уязвимость 2	6	70
Угроза3/Уязвимость 1	3	40
Угроза3/Уязвимость 2	5	40

5.7. Расчёт уровня угрозы по уязвимости Th и уровня угрозы по всем уязвимостям, через которые реализуется данная угроза CTh с учетом контрмер.

Результаты расчета приведены в табл.5.6.

Таблица5.6

Угроза/Уязвимость	Уровень угрозы (%),Th $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%),CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$
Сервер закрытого контура		
Угроза1/Уязвимость 1	0,035	0,069
Угроза1/Уязвимость 2	0,035	
Угроза2/Уязвимость 1	0,055	0,108
Угроза2/Уязвимость 2	0,056	
Угроза3/Уязвимость 1	0,01	0,024
Угроза3/Уязвимость 2	0,014	
Сервер открытого контура		
Угроза1/Уязвимость 1	0,05	0,117
Угроза1/Уязвимость 2	0,07	
Угроза2/Уязвимость 1	0,014	0,019
Угроза2/Уязвимость 2	0,005	
Угроза3/Уязвимость 1	0,066	0,083
Угроза3/Уязвимость 2	0,018	
МЭ открытого контура		
Угроза1/Уязвимость 1	0,015	0,054
Угроза1/Уязвимость 2	0,04	
Угроза2/Уязвимость 1	0,045	0,093
Угроза2/Уязвимость 2	0,05	
Угроза3/Уязвимость 1	0,015	0,045
Угроза3/Уязвимость 2	0,03	
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	0,01	0,079
Угроза1/Уязвимость 2	0,07	
Угроза2/Уязвимость 1	0,005	0,02
Угроза2/Уязвимость 2	0,015	
Угроза3/Уязвимость 1	0,015	0,056
Угроза3/Уязвимость 2	0,042	
Однонаправленный шлюз		
Угроза1/Уязвимость 1	0,07	0,112

Угроза1/Уязвимость 2	0,045	
Угроза2/Уязвимость 1	0,025	0,034
Угроза2/Уязвимость 2	0,009	
Угроза3/Уязвимость 1	0,015	0,024
Угроза3/Уязвимость 2	0,009	
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	0,02	0,059
Угроза1/Уязвимость 2	0,04	
Угроза2/Уязвимость 1	0,05	0,063
Угроза2/Уязвимость 2	0,014	
Угроза3/Уязвимость 1	0,005	0,02
Угроза3/Уязвимость 2	0,015	
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	0,04	0,069
Угроза1/Уязвимость 2	0,03	
Угроза2/Уязвимость 1	0,035	0,076
Угроза2/Уязвимость 2	0,042	
Угроза3/Уязвимость 1	0,012	0,032
Угроза3/Уязвимость 2	0,02	

5.8. Расчет общего уровня угроз, действующих на ресурс и риск ресурса для режима с одной общей угрозой с учетом контрмер. Результаты приведены в табл.5.7.

Таблица5.7

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), $CThR$ $CThR = 1 - \prod_{n=1}^{N}(1 - CTh)$	Риск ресурса для режима с одной общейугрозой (%), R_{new} $R_{new} = CThR \cdot D$
Сервер закрытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,189	28,35
Сервер открытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,206	24,72
МЭ открытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,181	14,48

СКЗИ закрытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,148	7,4
Однонаправленный шлюз		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,163	11,899
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,136	13,464
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1 Угроза1/Уязвимость 2 Угроза2/Уязвимость 1 Угроза2/Уязвимость 2 Угроза3/Уязвимость 1 Угроза3/Уязвимость 2	0,167	14,195

5.9. Расчет эффективности введения контрмер.

Результат представлен в табл.5.8.

Таблица 5.8

Ресурс	Эффективность $E = \frac{R_{old} - R_{new}}{R_{old}}$
Сервер закрытого контура	0.844
Сервер открытого контура	0.753
МЭ открытого контура	0.784
СКЗИ закрытого контура	0.818
Однонаправленный шлюз	0.811
Оборудование ЛВС открытого контура	0.791
Оборудование ЛВС закрытого контура	0.826

Выводы

Построена модель угроз и нарушителя для аппаратного ресурса ИС. Проведена оценка риска по аппаратному ресурсуR_{old}. После принятия контрмер уровень рискаR_{new} по аппаратному ресурсузаметно снизился.Однако заданный уровень эффективности E снижения риска до приемлемого уровня 10% не достигнут. Необходимо усилить контрмеры и пересчитать значение нового рискаR_{new}

6. Содержание отчета

1. Цель работы
2. Теоретические положения
3. Структурная схема«закрытого» и «открытого» контура ИС, с указанием защищаемых ресурсов.
4. Описание процесса выполнения работы
5. Полученные результаты расчетов (по каждому виду ресурса)
   5.1. Уровни угроз $Th, CTh,\ CThR$а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами
   5.2. Риск ресурса R_{old} а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами;
   5.3. Риск ресурса R_{new} с учетом заданных контрмер а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами
   5.4. Рассчитать и оценить эффективность принятых контрмер E.
   5.5. Риск по информационной системе CR с учетом рисков по всем N ресурсам:а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами;
6. Выводы

7. Контрольные вопросы

7.1. Какие структурные элементы входят в объект защиты?
7.2. Какая основная цель проведения анализа рисков в ИС?
7.3. Какие активы определяют функциональность ИС и существенны с точки зрения обеспечения безопасности?
7.4. Чем определяется важность (или стоимость) актива?
7.5. Какие видыактивов ИС вы знаете?
7.6. Как оцениваются сточки зрения нанесения ущерба организации информационные активы, программное обеспечение, материальные ресурсы и сервисы, а также сотрудники организации (их квалификация и опыт) и нематериальные ресурсы (репутация и имидж организации)?
7.7. Как определить вероятностьреализации угрозы через уязвимость или хи актуальность?
7.8. В чем заключается оценка информационных рисков? Приведите классическую формулу для оценки информационных рисков.
7.9. Какие основные критерии обработки рисков вы знаете?
7.10. Что описывает «Отчет об обработке информационных рисков организации»?
7.11. Как рассчитать уровень угрозы по уязвимости Th с учетом критичности и вероятности реализации угрозы через

данную уязвимость,а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами?

7.12. Как рассчитать уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CThа) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами?

7.13. Как рассчитать общий уровень угроз по ресурсу $CThR$а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами?

7.14. Как рассчитать риск ресурса R_{old} а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами?

7.15. Как рассчитать риск по информационной системе CR с учетом рисков по всем N ресурсам а) для режима с одной базовой угрозой; б) для режима работы с тремя угрозами?

7.16. Как задать контрмеры?

7.17. Как оценить эффективность принятых контрмер E?

Практическая работа 2

Оценки рисков информационной системы на основе модели информационныхпотоков (*"Методика оценки рисков информационнойбезопасностиорганизацииDigitalSecurity"*)

1. **Цель работы.** Рассчитать риск информационной системы (ИС) на основе модели информационныхпотоков.
2. **Задание к практической работе**

2.1. ***Описать архитектуру ИС***.

2.1.1. Составить структурно-функциональную схему ИС

2.1.2. Описать в виде таблиц средства защиты каждого аппаратного ресурса, средства защиты каждого вида информации, хранящемся на нем с указанием веса каждого средства.

2.1.3. Описать в виде таблицы вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а также наличие соединения через VPN, количество человек в группе для каждого информационного потока.

2.1.4. Указать наличие у пользователей выхода в Интернет.

2.1.5. Указать ущерб организации от реализации угроз ИБ для каждого информационного потока.

2.2. ***Рассчитать риски для каждого вида информации в ИС***

2.2.1. Рассчитать риски для каждого вида информации по угрозе

нарушение «конфиденциальности».

2.2.2. Рассчитать риски для каждого вида информациипо угрозе нарушение «целостности».

2.2.3. Рассчитать риски для каждого вида информациипо угрозе нарушение «доступности».

2.2.4. Оценить рискидля каждого вида информации по угрозе нарушение «конфиденциальности», «целостности» и«доступности».

3. Краткие теоретические сведения

Метод оценки рисков информационной системы на основе модели информационных потоков позволяет оценить защищенность каждого вида информации.

Метод оценки рисков базируется на построении модели ИС организации. Для этого необходимо проанализировать защищенность и архитектуру ИС. Специалист по ИБ, привлекая владельца (менеджера) ИС (используя вопросники, интервью, документацию, инструменты автоматического сканирования), должен подробно описать архитектуру сети:

– все аппаратные (компьютерные) ресурсы, на которых хранится ценная информация;

– сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);

– отделы, к которым относятся ресурсы;

– виды ценной информации;

– ущерб для каждого вида ценной информации по трем видам угроз;

–бизнес-процессы, в которых обрабатывается информация;

–пользователей (группы пользователей), имеющих доступ к ценной информации;

– класс группы пользователей;

– доступ группы пользователей к информации;

– характеристики этого доступа (вид и права);

– средства защиты информации;

– средства защиты рабочего места группы пользователей.

Исходя из полученных данных строится полная модель ИС организации на основе которой проводитсяоценки рисков для каждого ресурса по угрозе нарушения «конфиденциальности», «целостности» и «доступности».Алгоритм оценки рисков позволяет получить следующие данные:

– реестр ресурсов;

– значения риска для каждого ценного ресурса организации;

– значения риска для ресурсов после задания контрмер (остаточный риск);

– эффективность контрмер;

– рекомендации экспертов.

4. Последовательность выполнения практической работы

4.1. *Построить архитектуру ИС*

4.1.1. Составить структурно-функциональную схему ИС на которой отобразить (пример схемы приведен на рис.4.1):

- все ресурсы (сервер, АРМ, ПО, БД ит.д.) «закрытого» и «открытого» контура ИС;
- отделы, к которым относятсяресурсы «закрытого» и «открытого» контура ИС;
- сетевыегруппы«открытого» контура,физическиесвязиресурсовмеждусобой и их подключения кИнтернет и/или к мобильным сетям;
- виды ценной информации, хранящейся наресурсах;
- пользователей (группы пользователей), имеющих доступ кценной(конфиденциальной)информации.

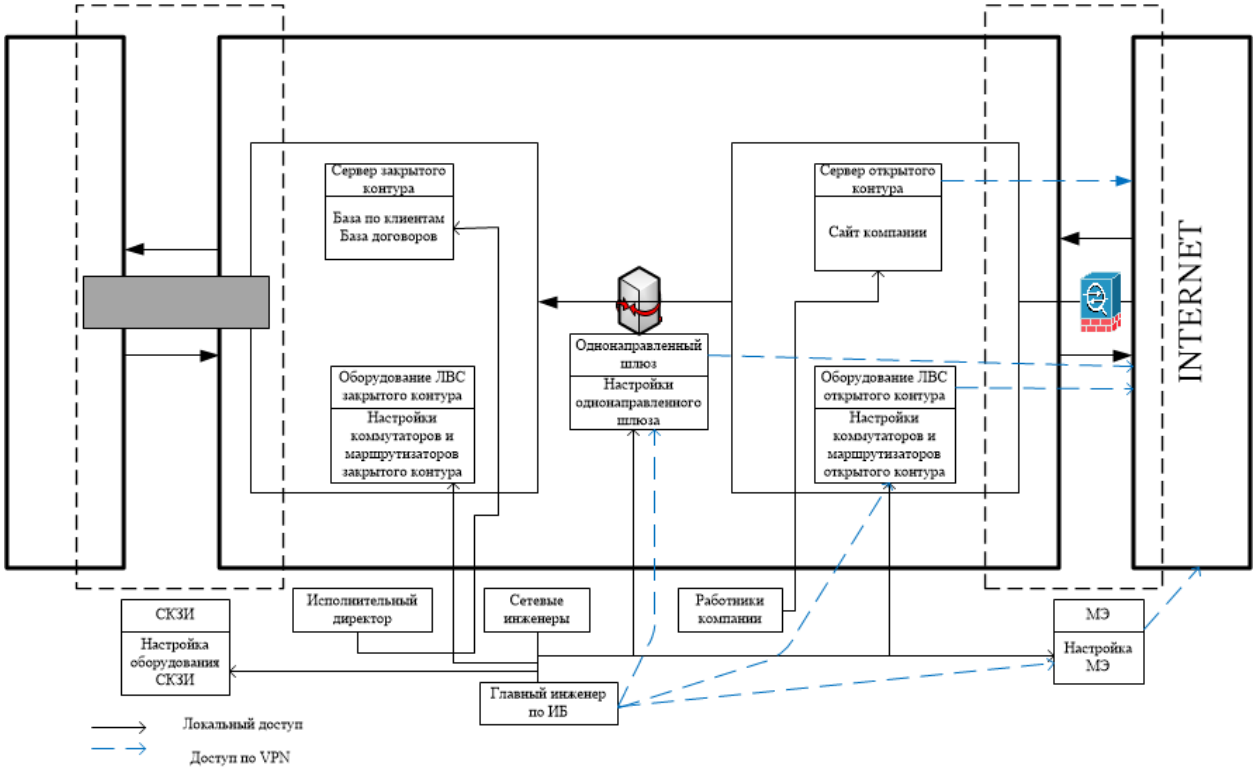

Рис.4.1. Структурно-функциональная схема ИС

4.1.2. Определить вес средств защиты каждого аппаратного ресурса, средств защиты каждого вида информации, хранящемся на нем, а также ПО с указанием веса каждого средства (табл.4.1). Веса выбирать самостоятельно.

Таблица 4.1

Средства защиты сервера	Вес
Средства физическойзащиты	

Контроль доступа в помещение, где расположен ресурс(физическаяохрана, дверь с замком, специальный пропускной режим впомеще-ние)	
Средства локальнойзащиты	
Отсутствие дисководов и USB портов10	
Средства корпоративной сетевойзащиты	
Межсетевойэкран	
Обманнаясистема	
Система антивирусной защиты насервере	
Средства резервирования и контроляцелостности	
Аппаратная система контроляцелостности	
Средства защиты информации (информация№1)	Вес
Средства локальнойзащиты	
Средства криптографической защиты (криптозащита данных наАРМ)	
Средства резервирования и контроляцелостности	
Резервноекопирование	
Программная система контроляцелостности	
Средства защиты рабочейстанции	Вес
Средство физическойзащиты	
Контроль доступа в помещение, где расположен ресурс (дверьсзамком,видеонаблюдение)	
Средства локальнойзащиты	
Средства антивирусной защиты (антивирусныймонитор)	
Отсутствие дисководов и USBпортов	
Средства персональной сетевойзащиты	
Наличие персонального межсетевогоэкрана	
Система криптозащиты электроннойпочты	

4.1.3. Определить вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а также наличие соединения через VPN, количество человек в группе для каждого информационного потока (табл. 4.2)

Таблица 4.2

Информационный поток	Виддоступа	Правадоступа	Наличие VPN-соединения	Количество человекв группе
(Наименование)	(Локальный, удаленный)	(Чтение,за-пись,удале-ние)	(Да,нет)	(1,2,….n)

4.1.4. Указать наличие у пользователей выхода в Интернет(табл.4.3)

Таблица 4.3

Пользователь(группапользователей)	Доступ вИнтернет

(Наименование)	(Есть, нет, неанализируется)

4.1.5. Определить ущерб организации от реализации угроз ИБ для каждого информационного потока (табл. 4.4)

Таблица 4.4

Информационный поток	Конфиденциальность	Целостность	Доступность
(Наименование)	(у.е. в год)	(у.е. в год)	(у.е. вчас)

Ущерб определяется с участием владельца ИС, либо им самимнепосредственно.На этом описание архитектуры ИСзавершается.

4.2. Расчет рисков для каждого вида ценной информации по угрозе нарушения «конфиденциальности», «целостности» и «доступности».

4.2.1. Расчет рисков по угрозе нарушение «конфиденциальности»

4.2.1.1. Расчет коэффициентовзащищенности.

Для каждого информационного потока рассчитывается коэффициентлокальной либо удаленной защищенности информации, хранящейся на ресурсе,взависимости от типа доступа. Если доступ локальный, то рассчитываетсятолько коэффициент локальной защищенности информации. Если доступудаленный, то рассчитывается коэффициент удаленной защищенностиинформации,хранящейся на ресурсе и коэффициент локальной защищенности рабочегоместапользователя.

*Коэффициент локальной защищенности информации*рассчитывается,еслидоступкинформациивданноминформационномпотоке***локальный***.Онравен сумме весов средств физической и локальной защитыинформации.Учитываютсявсесредствафизическойзащитыисредствалокальнойзащиты информации, обеспечивающие защиту информации по угрозе***конфиденциальность***:

- средства физической защиты: охрана, замок, пропускной режим в помещение(например, 25);
- средства локальнойзащиты:
- отсутствие дисководов и USB портов(например, 10);
- криптозащита данных на АРМ(например, 20).

*Коэффициент удаленной защищенности информации на ресурсе*рассчитывается, если доступ к информации в данном информационномпотоке*удаленный*. Он необходим для того, чтобы учесть сетевые средства защиты,иравен сумме весов средств корпоративной сетевой защиты информации. Эти средства (межсетевой экран, серверная антивирусная защита) находятся**насервере.**

*Коэффициент локальной защищенности рабочего места*пользователя(группы пользователей) рассчитывается только при удаленном доступе кинформации. Он равен сумме весов средств *физической, локальной* и*персональной сетевой защиты*информации.

- Средства физической защиты – теже.
- Средствалокальнойзащиты:антивирус,отсутствиедисководовиUSB-портов.
- Средства персональной сетевой защиты: межсетевой экран (firewall),средства криптозащиты электроннойпочты.

Эти средства (персональный межсетевой экран, средства криптозащиты электронной почты) находятся на АРМ, подключенном к ЛВС.

Этот коэффициент не определяется для анонимных и авторизованных Интернет-пользователей, т. к. АРМ пользователя в данном случае не является частью ИС.

Для дальнейших расчетов *по каждому потоку из трех коэффициентов выбирается наименьший коэффициент защищенности (НК)*.

Полученные значения коэффициентов сводятся в табл.4.5.

Таблица 4.5

Информационнй поток	Коэф.локальн.защищен-ти информации	Коэффициент удаленной защищен-тиинформации	Коэффициент локальной защищен-тиАРМ	Наименьший коэффициент
(Наименование)	(Ф+Л)	(СКСЗ)	(Ф+Л+ПСЗ)	(НК)min

4.2.1.2. Учет наличия доступа при помощи VPN

При локальном доступе VPN не учитывается, поскольку ЛВС не используется для передачиинформации.

При удаленном доступе через VPN к наименьшему коэффициентузащищенности потока прибавляется вес VPN шлюза (МЭ) и вычисляется результирующий коэффициент**:***РК=НК+вес VPN шлюза (или+0)*. Расчеты сводятся в табл.4.6

Таблица4.6.

Информационный поток	Наименьший коэффициент	Вес VPNсоединения	Результирующий коэффициент
(Наименование)	(НК)	(20 либо0)	(РК)

4.2.2. Расчет итогового коэффициента (ИК) защищенности

Если количество пользователей 1, и у группы нет доступа в Интернет, то:*ИК=1/РК*.

Учет количества человек N в группе пользователей:*ИК=N/РК*.

Если группа пользователей имеет доступ в Интернет, то ИКувеличивается в 2 раза:*ИК=2 N/РК*.

Если при удаленном доступе Интернет-пользователейVPN-

соединениенеиспользуется(Интернетзаведеннакомпьютер,аненасервер),то дляних итоговый коэффициентзащищенности(ИК)умножаетсяна4, в силу отсутствия зашиты шлюза *ИК= (4 N)/РК*. Результаты расчетов сводятся втабл.4.7.

Таблица 4.7

Информационный поток	Результир.коэффициент	Количествочеловекв группе	Наличие Интернет	Итоговыйкоэффициент
Гл. бухгалтер–бухгалтерскийотчет	(РК)	(N)	I=2,1	ИК=(NI)/РК

4.2.3. Расчет итоговой вероятности (ИВ)

Чтобы получить итоговую вероятность ИВ, необходимо сначала определить базовую вероятность (БВ) реализации угрозы нарушения конфиденциальности и умножитьеена ИК: *ИВ=БВ·ИК*.

Базоваявероятность БВ реализации *k*-ой угрозыопределяется на основе методаэкспертныхоценок. Группа экспертов определяет БВ для каждой информации (длякаждогопотока). Базовую вероятность БВ может задать владелецинформации.Результаты расчетов сводятся втабл.4.8.

Таблица 4.8

Информационный поток	Базоваявероятн.(БВ)	Итоговая базоваявероятн.(ИБВ)	Итоговый коэф.(ИК)	Промежуточ. вероятн.(ПВ)	Итоговаявероятн.(ИВ)

Если на ресурсе расположены несколько видов информации, причем кнекоторымиз них осуществляется доступ через Интернет (группами анонимных,авторизованных или мобильных Интернет-пользователей), то угрозы, исходящие отэтихгрупп пользователей, могут повлиять и на другие виды информации.Следовательно,этонеобходимоучесть.Еслинаодномизресурсов,находящемсявсетевой группе, хранится информация, к которой осуществляют доступуказанныегруппыпользователей,тоэтоучитываетсяаналогичнодлявсехвидов информации, хранящихся на всех ресурсах, входящих в сетевую группу. Вреальной информационной системе все ресурсы, взаимосвязанные между собой,оказывают друг на друга влияние. Т.е. злоумышленник, проникнув на одинресурсинформационной системы (например, получив доступ к информацииресурса),можетбезтрудаполучитьдоступкресурсам,физическисвязаннымсовзломанным.

4.2.4. Расчет риска по угрозе нарушение «конфиденциальности» для каждого вида информации

Риск по угрозе конфиденциальность для каждого вида информации рассчитывается, какпроизведение итоговой вероятности наущерб:

$$Rк=ИВi \cdot Di.$$

где*Di*–ущерб для каждого *i*-ого вида информации от реализациюугрозы.

4.2.5. Расчет риска по угрозе нарушение «конфиденциальности» для ресурса

Риск для ресурса, на котором хранится несколько видов информаций(несколько БД) *равенсумме рисковпо всем видаминформации*.

P.S.Расчеты рисков по угрозенарушения «целостности» и «доступности» выполняются аналогичным образом

5. Методические рекомендации повыполнения работы

5.2. Описание архитектуры ИС

5.2.1. Построение структурно-функциональной схемы «закрытого» и «открытого» контуров ИС

На рис.5.1 показана структурно-функциональная схема ИС организации, отображающая основные технические средства, функционирующие в сети, физические линии связи между оборудованием и логические (информационные) связи сотрудников (их АРМ) с ресурсами серверов «открытого» и «закрытого» контуров.Современные ИС строятся, как правило, на архитектуре «клиент-сервер» с применением технологии виртуальных серверов и предусматривают «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре, который может иметь различные классы защищённости, обрабатывается конфиденциальная информация с различным грифом секретности, а в «открытом» контуре – открытая информация. При этом сертифицированными средствами однонаправленной передачи информации обеспечивается только односторонняя передача информации из «открытого» контура в «закрытый», т.е. передача информации в «закрытый» контуриз«открытого» осуществляется через однонаправленный межсетевой экран (МЭ).

Внешнее взаимодействие ИС с корпоративными системами осуществляется через «закрытый» контур с применением сертифицированных средств криптографической защиты информации (СКЗИ) с шифрованием информации. Взаимодействие «открытого» контура с «открытыми» контурамикорпоративной ИС осуществляется через Интернет (LTE) с применением сертифицированного внешнего МЭ.

С логической точки зрения структуру сети можно представить в виде трех отделов, технического, финансового и управляющего (руководство организации), каждый из которых имеет доступ к серверам как «открытого», так и к «закрытого»контура. Также в организации имеется несколько сотрудников, работающих удаленно – соответственно, эти пользователи

имеют доступ к обоим контурам, а также к сети Интернет по VPN. Следует понимать, что во всех трех отделах также имеется несколько сотрудников, и их группировка произведена для удобства восприятия схемы.

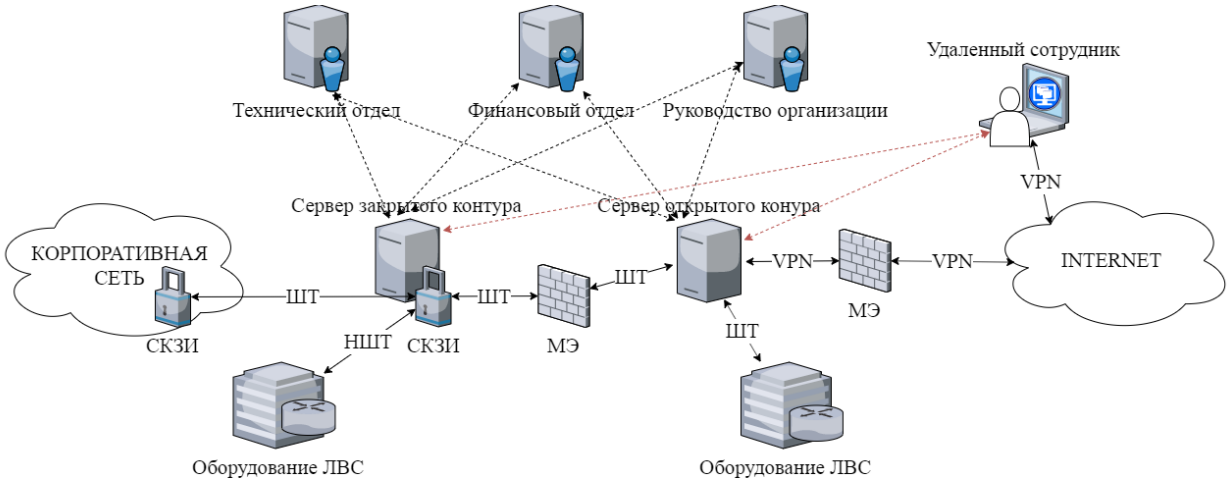

Рис.5.1. Структурно-функциональная схема ИС организации

Обозначения на структурной схеме соответствуют:

- ШТ – шифрованный с помощью средства криптографической защиты информации трафик
- НШТ – нешифрованный трафик
- VPN (Virtual Private Network) – технология организации защищенного канала для подключения удалённого сотрудника к ресурсам серверов «открытого»контура через сеть общего пользования (например, сеть Интернет и/или мобильные сети).

Пунктирными линиями обозначены логические связи, показывающие работу отделов организации с ресурсами серверов«открытого и «закрытого» контура, а также доступ к ним удалённого сотрудника.

5.2.2. Описание средств защиты аппаратных и информационных ресурсов

Для дальнейшего выполнения практической работы приведем сводную таблицу с описанием средств защиты каждого аппаратного ресурса, средств защиты каждого вида информации, хранящейся на нём, с указанием веса каждого средства (табл.5.1).

Таблица5.1

Тип средства защиты	Средство защиты	Вес средства защиты
Средства защиты закрытого сервера		
Средства физической защиты	[Д, К] Контроль доступа в помещение, где расположен ресурс(физическаяохрана, дверь с замком, специальный пропускной режим впомещение)	28
	[К] Система наблюдения(видеонаблюдение, сенсоры ит.д.)за	28

	объектом	
Средства локальной защиты	[Ц] Настроенная политика аудита (учет всех действий на сервере, в т.ч. авторизация, выход из учетной записи, модификации данных)	20
	[К, Ц] Отсутствие дисководов и USB-портов (исключение возможности использования внешних носителей с предположительно вредоносным кодом и/или выгрузки информации)	10
Средства корпоративной сетевой защиты	[Д]Межсетевой экран	20
	[К, Ц] Система антивирусной защиты	25
	[Ц] Система обнаружения и предотвращения утечек (DLP-система)	28
Средства резервирования и контроля целостности	[Д, Ц] Средства создания резервной копии (резервная копия создается каждые три дня в соответствии с политикой безопасности организации)	28
	[Ц] Аппаратная система контроляцелостности	25
Средства защиты открытого сервера		
Средства физической защиты	[К, Д] Контроль доступа в помещение, где расположен ресурс(физическаяохрана, дверь с замком, специальный пропускной режим впомещение)	22
	[К] Система наблюдения(видеонаблюдение, сенсоры ит.д.)за объектом	16
Средства локальной защиты	[Ц] Настроенная политика аудита (учет всех действий на сервере, в т.ч. авторизация, выход из учетной записи, модификации данных)	12
	[К, Ц] Отсутствие дисководов и USB-портов (исключение возможности использования внешних носителей с предположительно вредоносным кодом и/или выгрузки информации)	10
Средства корпоративной сетевой защиты	[Д]Межсетевой экран	15
	[К, Ц] Система антивирусной защиты	15
	[Ц] Система обнаружения и предотвращения утечек (DLP-система)	24
Средства резервирования и контроля целостности	[Д, Ц] Средства создания резервной копии (резервная копия создается каждые три дня в соответствии с политикой безопасности организации)	22
	[Ц] Аппаратная система контроляцелостности	18
Средства защиты информации		
Средство локальной защиты	[Ц] Использование средств криптографической защиты информации	25
	[Д] Распределение прав доступа к информации в соответствии с матрицей доступа	16
	[К, Ц] Наличие соглашений оконфиденциальности (исключение разглашениякон фиденциальнойинформациисотрудникамиорган изации)	20
Средства резервирования и контроля целостности	[Д, Ц] Средства создания резервной копии (резервная копия создается каждые три дня в соответствии с политикой безопасности организации)	20
	[Ц] Аппаратная система контроляцелостности	18
Средства защиты рабочих мест		

Средства физической защиты	[К, Д] Контроль доступа в помещение, где расположен ресурс(физическаяохрана, дверь с замком)	16
	[К] Система наблюдения(видеонаблюдение, сенсоры ит.д.)за объектом	16
Средства локальной защиты	[К, Ц] Наличие соглашений оконфиденциальности (исключение разглашенияконфиденциальнойинформациисотрудникамиорганизации)	20
	[Д] Настроенная локальная политика безопасности на каждом рабочем месте (распределение прав доступа, парольная политика, аудит действий пользователя)	15
	[К, Ц] Отсутствие дисководов и USB-портов	10
	[Ц] Средства антивирусной защиты (антивирусный монитор)	10
Средства персональной сетевойзащиты	[К, Ц] Система криптозащиты электронной почты	5
	[Д, К] Наличие персонального межсетевого экрана на каждом АРМ	5

В квадратных скобках отмечено, какой тип угрозы закрывает каждое средство, сокращения соответствуют:

- Д – угрозе Доступности;
- К – угрозе Конфиденциальности;
- Ц – угрозе Целостности.

5.2.3. Описание типов и прав доступа сотрудников

Для дальнейшего выполнения практической работы приведем сводную таблицу (табл. 5.2) с описанием видов доступа (локальный или удаленный) и прав доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей, если речь идет об отделах). Также добавим отдельную графу, в которую вынесем нужно или нет конкретному пользователю (отделам) VPN-соединение.

Предположим, что управляющий отдел (руководство организации) периодически контролирует деятельность других отделов – необходимо наличие двух информационных потоков от руководства к открытому и закрытому контурам. Удаленному сотруднику по роду деятельности требуется доступ к открытому и закрытому серверам. Технический и финансовый отделы собирают информацию о работе организации, каждый свою, поэтому и им необходимо взаимодействовать с обоими контурами.

В целях безопасности запретим информационным потокам право на удаление, а для всех потоков, что идут через закрытый сервер – еще и запись, во избежание уничтожения и модификации информации (что может привести к торможению рабочего процесса организации и к финансовым и человек/часовым потерям).

Таблица 5.2

Информационный поток	Вид доступа	Права доступа	VPN-соединение	Количество человек

Руководство организации – Сервер закрытого контура	Локальный	Чтение, запись,	Не требуется	10
Руководство организации – Сервер открытого контура	Локальный	Чтение, запись,	Не требуется	
Технический отдел – Сервер закрытого контура	Локальный	Чтение, запись,	Не требуется	13
Технический отдел – Сервер открытого контура	Локальный	Чтение, запись,	Не требуется	
Финансовый отдел – Сервер закрытого контура	Локальный	Чтение	Не требуется	17
Финансовый отдел – Сервер открытого контура	Локальный	Чтение, запись	Не требуется	
Удалённый сотрудник – Сервер закрытого контура	Удалённый	Чтение	Да	6
Удалённый сотрудник – Сервер открытого контура	Удалённый	Чтение, запись	Да	

5.2.4. Доступ к сети Интернет для сотрудников

Для дальнейшего выполнения практической работы приведем сводную таблицу для трех имеющихся отделов организации (управляющий, технический, финансовый), в которой определим необходимость (или ее отсутствие) доступа к сети интернет для всех пользователей этих групп (табл. 5.3).

Предположим, что управляющий отдел (руководство организации) периодически контролирует деятельность других отделов, а также осуществляет решение различных вопросов, связанных с деятельностью организации в целом – следовательно, данному отделу требуется доступ к сети Интернет. Технический отдел контролирует работоспособность системы в целом, а также имеет возможность связываться с руководством организации при необходимости (посредством электронной почты), поэтому данному отделу также требуется доступ к сети Интернет. Финансовый отдел, ввиду особой ценности, обрабатываемой им информации, в целях повышения безопасности доступа к сети интернет не имеет.

Таблица 5.3

Отдел	Доступ к сети Интернет
Руководство организации	Есть
Технический отдел	Есть
Финансовый отдел	Отсутствует

5.2.5. Определение ущерба организации при реализации угроз ИБ для каждого информационного потока

Для дальнейшего выполнения практической работы приведем сводную таблицу, в которой перечислим ущерб организации, который возникнет в случае реализации угроз ИБ для каждого информационного потока (табл.5.4).

Таблица 5.4

Информационный поток	Конфиденциальность (у.е. в год)	Доступность (у.е. в час)	Целостность (у.е. в год)

Руководство организации – Сервер закрытого контура	100	55	50
Руководство организации – Сервер открытого контура	85	30	40
Технический отдел – Сервер закрытого контура	90	50	40
Технический отдел – Сервер открытого контура	70	25	25
Финансовый отдел – Сервер закрытого контура	90	30	40
Финансовый отдел – Сервер открытого контура	65	30	40
Удалённый сотрудник – Сервер закрытого контура	85	25	30
Удалённый сотрудник – Сервер открытого контура	60	25	25

5.3. Расчет рисков по угрозе нарушение «конфиденциальности»

Для каждого информационного потока рассчитывается коэффициентлокальной либо удаленной защищенности информации, хранящейся на ресурсе,взависимости от типа доступа. Если доступ локальный, то рассчитываетсятолько коэффициент локальной защищенности информации. Если доступудаленный, то рассчитывается коэффициент удаленной защищенностиинформации,хранящейся на ресурсе и коэффициент локальной защищенности рабочегоместапользователя.

5.3.1. *Расчет коэффициентов защищенности*.

Коэффициент локальной защищенности информациирассчитывается,еслидоступкинформациивданноминформационномпотоке*локальный*.Онравен сумме весов средств *физической* и *локальной* защитыинформации.Учитываютсявсесредствафизическойзащитыисредства локальнойзащиты информации, обеспечивающие защиту информации по угрозе*«конфиденциальность»*.

Рассмотрим пример расчета для «открытого» сервера:

- средства физической защиты: контроль доступа в помещение, где расположен ресурс(физическаяохрана, дверь с замком, специальный пропускной режим впомещение) (22), система видеонаблюдения (16);
- средства локальнойзащиты: отсутствие дисководов и USB-портов(10), наличие соглашений оконфиденциальности (20).

Коэффициент удаленной защищенности информации на ресурсерассчитывается, если доступ к информации в данном информационномпотоке*удаленный*. Он необходим для того, чтобы учесть *сетевые средства* защиты,иравен сумме весов средств корпоративной

сетевой защиты информации(межсетевой экран, серверная антивирусная защита)**.**

Рассмотрим пример расчета для «открытого» сервера:

- средства корпоративной сетевой защиты информации на сервере: DLP-система (24).

Коэффициент локальной защищенности рабочего места пользователя (группы пользователей) рассчитывается только при удаленном доступе к информации. Он равен сумме весов средств *физической, локальной и персональной сетевой защиты информации*.

Рассмотрим пример расчета для «открытого» сервера:

- средства физической защиты: контроль доступа в помещение, где расположен ресурс(физическаяохрана, дверь с замком, специальный пропускной режим впомещение) (22), система видеонаблюдения (16);
- средства локальной защиты: отсутствие дисководов и USB-портов(10), наличие соглашений оконфиденциальности (20), средства антивирусной защиты (10);
- средства персональной защиты: межсетевой экран (5), система криптозащиты электронной почты (5).

Для дальнейших расчетов по каждому потоку из трех коэффициентов выбирается *наименьший коэффициент защищенности (НК)*. Расчёт результирующих коэффициентов для информационных потоков представлен в табл.5.5.

Таблица 5.5

Информационный поток	Коэффициент локальной защищенности информации	Коэффициент удаленной защищенности информации	Коэффициент локальной защищенности рабочего места	НК
Руководство организации – Сервер закрытого контура	86	–	106	86
Руководство организации – Сервер открытого контура	68	–	88	68
Технический отдел – Сервер закрытого контура	80	–	70	70
Технический отдел – Сервер открытого контура	60	–	62	60
Финансовый отдел – Сервер закрытого контура	82	–	76	76
Финансовый отдел – Сервер открытого контура	65	–	64	64
Удалённый сотрудник – Сервер закрытого контура	50	28	34	28
Удалённый сотрудник – Сервер открытого контура	45	24	22	22

5.3.2. Учет наличия доступа через VPN

При локальном доступе VPN не учитывается, поскольку локальная сеть не используется для передачи информации.

При удалённом доступе через VPN к наименьшему коэффициенту защищенности потока прибавляется вес VPN шлюза (20). Это сетевое устройство повышает защищённость информации. При этом от наименьшего коэффициента переходят к результирующему: РК = НК + 20 или РК = НК + 0. Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.6.

Таблица 5.6

Информационный поток	Наименьший коэффициент защищенности	Вес VPN-соединения	Результирующий коэффициент
Руководство организации – Сервер закрытого контура	86	0	86
Руководство организации – Сервер открытого контура	68	0	68
Технический отдел – Сервер закрытого контура	70	0	70
Технический отдел – Сервер открытого контура	60	0	60
Финансовый отдел – Сервер закрытого контура	76	0	76
Финансовый отдел – Сервер открытого контура	64	0	64
Удалённый сотрудник – Сервер закрытого контура	28	20	48
Удалённый сотрудник – Сервер открытого контура	22	20	42

5.3.3. Расчёт итогового коэффициента защищённости

Далее от результирующего коэффициента (РК) переходят к итоговому коэффициенту (ИК) защищенности. Рассчитывается он следующим образом:

- если количество пользователей 1, и у группы нет доступа в Интернет, то*ИК=1/РК*;
- если количество человек *N* и у группы пользователей нет доступа в Интернет, то *ИК=N/РК*;
- если группа пользователей имеет доступ в Интернет, то ИКувеличивается в 2 раза: *ИК=2N/РК*.

Если при удаленном доступе к Интернет-пользователей VPN-соединение не используется (Интернет заведен на компьютер, а не на сервер), то для них итоговый коэффициент защищенности (ИК) умножается на 4, в силу отсутствия зашиты шлюза*ИК=4N/РК*. Расчёт итоговых коэффициентов для информационных потоков представлен в табл. 5.7.

Таблица 5.7

Информационный поток	Результирующий коэффициент защищенный	Количество человек в группе	Наличие Интернет-соединения	Итоговый коэффициент защищенности
Руководство организации – Сервер	86	10	Есть (*2N/РК*)	0,233

закрытого контура				
Руководство организации – Сервер открытого контура	68			0,294
Технический отдел – Сервер закрытого контура	70	13	Есть (*2N/PK*)	0,371
Технический отдел – Сервер открытого контура	60			0,433
Финансовый отдел – Сервер закрытого контура	76	17	Нет (*N/PK*)	0,224
Финансовый отдел – Сервер открытого контура	64			0,266
Удалённый сотрудник – Сервер закрытого контура	48	6	Есть (*2N/PK*)	0,25
Удалённый сотрудник – Сервер открытого контура	42			0,286

5.3.4. Расчёт итоговой вероятности

Чтобы получить итоговую вероятность (ИВ), необходимо сначала определить базовую вероятность (БВ) реализации угрозы нарушения конфиденциальности и умножить её на ИК: $ИВ = БВ \cdot ИК$. БВ реализации угрозы «К» определяется на основе метода экспертных оценок. Группа экспертов определяет БВ для каждой информации (для каждого потока). БВ может задать владелец информации.

Промежуточная вероятность (ПВ) вычисляется как: $ПВ = ИБВ \cdot ИК$. Итоговая вероятность $ИВ = 1 - ((1 - ПВ_1) \cdot (1 - ПВ_2) \cdot \ldots \cdot (1 - ПВ_N))$, как суммарная по нескольким группам пользователей.

Расчёт итоговой вероятности показан в табл.5.8. Для удобства разобьем расчет итоговой вероятности для серверов закрытого и открытого контуров.

Таблица 5.8

Информационный поток	БВ	ИБВ	ИК	ПВ	ИВ
Руководство организации – Сервер закрытого контура	0,01	0,2	0,233	0.047	0.199
Технический отдел – Сервер закрытого контура	0,03	0,2	0,371	0.074	
Финансовый отдел – Сервер закрытого контура	0,01	0,2	0,224	0.045	
Удалённый сотрудник – Сервер закрытого контура	0,03	0,2	0,25	0.05	
Руководство организации – Сервер открытого контура	0,02	0,32	0,294	0.059	0.233
Технический отдел – Сервер открытого контура	0,04	0,32	0,433	0.087	
Финансовый отдел – Сервер открытого контура	0,02	0,32	0,266	0.053	
Удалённый сотрудник – Сервер открытого контура	0,04	0,32	0,286	0.057	

Итоговая базовая вероятность (ИБВ) одинакова для всех потоков, поскольку к информации имеется доступ через Интернет. Если на ресурсе

расположены несколько видов информации, причем к некоторым из них осуществляется доступ через Интернет (группами анонимных, авторизованных или мобильных Интернет-пользователей), то угрозы, исходящие от этих групп пользователей, могут повлиять и на другие виды информации. Следовательно, это необходимо учесть. Если на одном из ресурсов, находящемся в сетевой группе, хранится информация, к которой осуществляют доступ указанные группы пользователей, то это учитывается аналогично для всех видов информации, хранящихся на всех ресурсах, входящих в сетевую группу. В реальной информационной системе все ресурсы, взаимосвязанные между собой, оказывают друг на друга влияние. Т.е. злоумышленник, проникнув на один ресурс информационной системы (например, получив доступ к информации ресурса), может без труда получить доступ к ресурсам, физически связанным со взломанным.

5.3.5. Расчёт риска по угрозе нарушение «конфиденциальности» для каждой информации

Риск по угрозе «конфиденциальность» для каждой информации рассчитывается как произведение итоговой вероятности на ущерб. Расчёт риска по угрозе «конфиденциальность» приведен в табл. 5.9.

Таблица 5.9

Информационный поток	ИВ	Ущерб	Значение риска
Руководство организации – Сервер закрытого контура	0.199	100	20
Технический отдел – Сервер закрытого контура		90	18
Финансовый отдел – Сервер закрытого контура		90	18
Удалённый сотрудник – Сервер закрытого контура		85	17
Руководство организации – Сервер открытого контура	0.233	85	20
Технический отдел – Сервер открытого контура		70	16
Финансовый отдел – Сервер открытого контура		65	15
Удалённый сотрудник – Сервер открытого контура		60	14

5.3.6. Расчёт риска по угрозе нарушение «конфиденциальности» для ресурса

Риск для ресурса, на котором хранится несколько видов информаций равен сумме рисков по всем видам информации. Так как основными ресурсами в организации являются сервер закрытого контура и сервер открытого контура, то риски для данных ресурсов рассчитываются как сумма рисков по всем информационным потокам к этому ресурсу. Расчёт риска по угрозе «конфиденциальность» для ресурса показана в табл. 5.10.

Таблица 5.10

Информационный поток	Значение риска для информации	Значение риска для ресурса
Руководство организации – Сервер закрытого контура	20	73
Технический отдел – Сервер закрытого контура	18	
Финансовый отдел – Сервер закрытого контура	18	
Удалённый сотрудник – Сервер закрытого контура	17	

Руководство организации – Сервер открытого контура	20	65
Технический отдел – Сервер открытого контура	16	
Финансовый отдел – Сервер открытого контура	15	
Удалённый сотрудник – Сервер открытого контура	14	

На этом расчет рисков по угрозе нарушение «конфиденциальности» закончен.

5.4. Расчет рисков по угрозе нарушение «доступности»

5.4.1. Расчет коэффициентов защищенности

Расчеты производятся аналогичным образом, однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл.5.11.

Таблица 5.11

Информационный поток	Коэффициент локальной защищенности информации	Коэффициент удаленной защищенности информации	Коэффициент локальной защищенности рабочего места	НК
Руководство организации – Сервер закрытого контура	64	–	48	48
Руководство организации – Сервер открытого контура	58	–	42	42
Технический отдел – Сервер закрытого контура	55	–	46	46
Технический отдел – Сервер открытого контура	43	–	45	43
Финансовый отдел – Сервер закрытого контура	50	–	38	38
Финансовый отдел – Сервер открытого контура	46	–	36	36
Удалённый сотрудник – Сервер закрытого контура	44	20	30	20
Удалённый сотрудник – Сервер открытого контура	38	15	28	15

5.4.2. Учет наличия доступа через VPN

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.12.

Таблица 5.12

Информационный поток	Наименьший коэффициент защищенности	Вес VPN-соединения	Результирующий коэффициент
Руководство организации – Сервер закрытого контура	48	0	48
Руководство организации –	42	0	42

Сервер открытого контура			
Технический отдел – Сервер закрытого контура	46	0	46
Технический отдел – Сервер открытого контура	43	0	43
Финансовый отдел – Сервер закрытого контура	38	0	38
Финансовый отдел – Сервер открытого контура	36	0	36
Удалённый сотрудник – Сервер закрытого контура	20	20	40
Удалённый сотрудник – Сервер открытого контура	15	20	35

5.4.3. Расчёт итогового коэффициента защищённости

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.13.

Таблица 5.13

Информационный поток	Результирующий коэффициент защищенный	Количество человек в группе	Наличие Интернет-соединения	Итоговый коэффициент защищенности
Руководство организации – Сервер закрытого контура	48	10	Есть (*2N/PK*)	0,417
Руководство организации – Сервер открытого контура	42			0,476
Технический отдел – Сервер закрытого контура	46	13	Есть (*2N/PK*)	0,565
Технический отдел – Сервер открытого контура	43			0,605
Финансовый отдел – Сервер закрытого контура	38	17	Нет (*N/PK*)	0,447
Финансовый отдел – Сервер открытого контура	36			0,472
Удалённый сотрудник – Сервер закрытого контура	40	6	Есть (*2N/PK*)	0,3
Удалённый сотрудник – Сервер открытого контура	35			0,343

5.4.4. Расчёт итоговой вероятности

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.14. Для удобства разобьем расчет итоговой вероятности для серверов закрытого и открытого контуров.

Таблица 5.14

Информационный поток	БВ	ИБВ	ИК	ПВ	ИВ
Руководство организации – Сервер закрытого контура	0,02	0,12	0,417	0,05	0,226
Технический отдел – Сервер закрытого контура	0,03	0,12	0,476	0,057	
Финансовый отдел – Сервер закрытого контура	0,05	0,12	0,565	0,068	
Удалённый сотрудник – Сервер закрытого контура	0,02	0,12	0,605	0,073	
Руководство организации – Сервер открытого контура	0,01	0,14	0,447	0,063	0,202
Технический отдел – Сервер открытого контура	0,03	0,14	0,472	0,066	
Финансовый отдел – Сервер открытого контура	0,04	0,14	0,3	0,042	
Удалённый сотрудник – Сервер открытого контура	0,05	0,14	0,343	0,048	

5.4.5. Расчёт риска по угрозе нарушение «доступности» для каждой информации

Риск по угрозе «доступность» для каждой информации рассчитывается как произведение итоговой вероятности на ущерб. Расчёт риска по угрозе «доступность» показан в табл.5.15.

Таблица 5.15

Информационный поток	ИВ	Ущерб	Значение риска
Руководство организации – Сервер закрытого контура	0,226	55	15
Технический отдел – Сервер закрытого контура		50	13
Финансовый отдел – Сервер закрытого контура		30	8
Удалённый сотрудник – Сервер закрытого контура		25	7
Руководство организации – Сервер открытого контура	0,202	30	6
Технический отдел – Сервер открытого контура		25	5
Финансовый отдел – Сервер открытого контура		30	6
Удалённый сотрудник – Сервер открытого контура		25	5

5.4.6. Расчёт риска по угрозе нарушение «доступности» для ресурса

Риск для ресурса, на котором хранится несколько видов информаций равен сумме рисков по всем видам информации. Так как основными ресурсами в организации являются сервер закрытого контура и сервер открытого контура, то риски для данных ресурсов рассчитываются как сумма рисков по всем информационным потокам к этому ресурсу. Расчёт риска по угрозе «доступность» для ресурса показана в табл.5.16.

Таблица 5.16

Информационный поток	Значение риска для информации	Значение риска для ресурса
Руководство организации – Сервер закрытого контура	15	49
Технический отдел – Сервер закрытого контура	13	
Финансовый отдел – Сервер закрытого контура	8	
Удалённый сотрудник – Сервер закрытого контура	7	

Руководство организации – Сервер открытого контура	6	22
Технический отдел – Сервер открытого контура	5	
Финансовый отдел – Сервер открытого контура	6	
Удалённый сотрудник – Сервер открытого контура	5	

На этом расчет рисков по угрозе нарушение «доступности» закончен.

5.5. Расчет рисков по угрозе нарушение «целостности»

5.5.1. Расчет коэффициентов защищенности

Расчеты производятся аналогичным образом, однако теперь рассматриваются средства, закрывающие данный тип угрозы – угроза целостности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.17.

Таблица 5.17

Информационный поток	Коэффициент локальной защищенности информации	Коэффициент удаленной защищенности информации	Коэффициент локальной защищенности рабочего места	НК
Руководство организации – Сервер закрытого контура	113	–	45	45
Руководство организации – Сервер открытого контура	105	–	45	45
Технический отдел – Сервер закрытого контура	93	–	32	32
Технический отдел – Сервер открытого контура	85	–	26	26
Финансовый отдел – Сервер закрытого контура	96	–	38	38
Финансовый отдел – Сервер открытого контура	82	–	20	20
Удалённый сотрудник – Сервер закрытого контура	75	53	30	30
Удалённый сотрудник – Сервер открытого контура	63	39	28	28

5.5.2. Учет наличия доступа через VPN и средств резервирования и контроля целостности

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угроза целостности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.18

Таблица 5.18

Информационный поток	НК	Вес VPN-соединения	Веса средств резервирования и контроля целостности	РК
Руководство организации – Сервер закрытого контура	45	0	28+25	98
Руководство организации –	45	0	22+18	85

Сервер открытого контура				
Технический отдел – Сервер закрытого контура	32	0	24+20	76
Технический отдел – Сервер открытого контура	26	0	20+15	61
Финансовый отдел – Сервер закрытого контура	38	0	28+20	86
Финансовый отдел – Сервер открытого контура	20	0	22+16	58
Удалённый сотрудник – Сервер закрытого контура	30	20	20+15	85
Удалённый сотрудник – Сервер открытого контура	28	20	20+10	78

5.5.3. Расчёт итогового коэффициента защищённости

Расчеты производятся аналогичным образом, как и для типа угрозы нарушение «конфиденциальности», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угроза целостности. Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то вес резервного копирования прибавляется к коэффициенту защищенности. Если резервное копирование не осуществляется, и в группе пользователей, имеющей доступ к информации, разрешены запись или удаление, то итоговый коэффициент увеличивается в 4 раза.

Расчёт результирующих коэффициентов для информационных потоков представлен в табл. 5.19.

Таблица 5.19

Информационный поток	РК	Наличие резервного копирования	Количество человек в группе	Наличие Интернет-соединения	ИК
Руководство организации – Сервер закрытого контура	98	1	10	Есть (*2N/PK*)	0,204
Руководство организации – Сервер открытого контура	85	1			0,235
Технический отдел – Сервер закрытого контура	76	1	13	Есть (*2N/PK*)	0,34
Технический отдел – Сервер открытого контура	61	1			0,426
Финансовый отдел – Сервер закрытого контура	86	1	17	Нет (*N/PK*)	0,198
Финансовый отдел – Сервер открытого контура	58	1			0,293
Удалённый сотрудник – Сервер закрытого контура	85	1	6	Есть (*2N/PK*)	0,141
Удалённый сотрудник – Сервер открытого контура	78	1			0,154

5.5.4. Расчёт итоговой вероятности

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угроза целостности. Расчёт результирующих коэффициентов для информационных потоков представлен в табл.5.20. Для удобства разобьем расчет итоговой вероятности для серверов закрытого и открытого контуров.

Таблица 5.20

Информационный поток	БВ	ИБВ	ИК	ПВ	ИВ
Руководство организации – Сервер закрытого контура	0,01	0,12	0,204	0,024	0,137
Технический отдел – Сервер закрытого контура	0,02	0,12	0,235	0,028	
Финансовый отдел – Сервер закрытого контура	0,03	0,12	0,34	0,041	
Удалённый сотрудник – Сервер закрытого контура	0,04	0,12	0,426	0,051	
Руководство организации – Сервер открытого контура	0,01	0,15	0,198	0,03	0,113
Технический отдел – Сервер открытого контура	0,02	0,15	0,293	0,044	
Финансовый отдел – Сервер открытого контура	0,03	0,15	0,141	0,021	
Удалённый сотрудник – Сервер открытого контура	0,04	0,15	0,154	0,023	

5.5.5. Расчёт риска по угрозе нарушения «целостности» каждого вида информации

Риск по угрозе нарушения «целостности» для каждой информации рассчитывается как произведение итоговой вероятности на ущерб. Расчёт риска по угрозе показан в табл.5.21.

Таблица 5.21

Информационный поток	ИВ	Ущерб	Значение риска
Руководство организации – Сервер закрытого контура	0,137	50	7
Технический отдел – Сервер закрытого контура		40	5
Финансовый отдел – Сервер закрытого контура		40	5
Удалённый сотрудник – Сервер закрытого контура		30	4
Руководство организации – Сервер открытого контура	0,113	40	5
Технический отдел – Сервер открытого контура		25	3
Финансовый отдел – Сервер открытого контура		40	5
Удалённый сотрудник – Сервер открытого контура		25	3

5.5.6. Расчёт риска по угрозам нарушения «целостности» ресурса

Риск для ресурса, на котором хранится несколько видов информаций равен сумме рисков по всем видам информации. Так как основными ресурсами в организации являются сервер закрытого контура и сервер открытого контура, то риски для данных ресурсов рассчитываются как сумма рисков по всем информационным потокам к этому ресурсу. Расчёт риска по угрозе нарушения «целостности» ресурса показана в табл. 5.22.

Таблица 5.22

Информационный поток	Значение риска для информации	Значение риска для ресурса
Руководство организации – Сервер закрытого контура	7	21
Технический отдел – Сервер закрытого контура	5	
Финансовый отдел – Сервер закрытого контура	5	

Удалённый сотрудник – Сервер закрытого контура	4	
Руководство организации – Сервер открытого контура	5	16
Технический отдел – Сервер открытого контура	3	
Финансовый отдел – Сервер открытого контура	5	
Удалённый сотрудник – Сервер открытого контура	3	

На этом расчет рисков по угрозе нарушение «целостности» закончен.

Выводы по практической работе

В ходе выполнения практической работы был рассчитаны риски информационной системы на основе модели информационных потоков. Для достижения поставленной цели:

- разработана структурно-функциональная схема информационной системы с отображением физических и логических ресурсов, а также типы информационных потоков;
- определены веса средств защиты каждого аппаратного ресурса, каждого вида информационного ресурса, хранящегося и/или обрабатывающегося на нём;
- указан вид доступа и права доступа для каждого пользователя (групп пользователей), а также наличие соединения через VPN, количество человек в группе для каждого информационного потока;
- указано наличие у пользователей выхода в Интернет;
- определен ущерб организации от реализации угроз ИБ для каждого информационного потока;
- произведен расчёт рисков информационной системы на основе модели информационных потоков по угрозам нарушение «конфиденциальности», «целостности» и «доступности».

В ходе выполнения расчетов была получена итоговая вероятность реализации угрозы «конфиденциальность»около 20% для серверов «закрытого» и «открытого» контуров. Значение риска для ресурсов при этом равняется 73 и 65 для серверов «закрытого» и «открытого» контуров соответственно. Поскольку предполагаемый риск меньше чем допустимый ущерб конфиденциальности в год (в среднем это 91 у.е. и 70 у.е. соответственно), можно сделать вывод, что информационная система организации защищена достаточно хорошо от угрозы типа «конфиденциальность». Однако в целях дальнейшего повышения безопасности системы рекомендуется принять дополнительные меры и/или усилить уже имеющиеся.

Итоговая вероятность реализации угрозы нарушение «доступности» составила около 20% для серверов «закрытого» и «открытого» контуров. Значение риска для ресурсов при этом равняется 49 у.е. и 22 у.е. для серверов «закрытого» и «открытого» контуров соответственно. Поскольку предполагаемый риск для закрытого сервера больше, а для открытого – меньше чем допустимый ущерб конфиденциальности в год (в среднем это 40 у.е. и 28 у.е. соответственно), можно сделать вывод, что информационная

система организации слабо защищена от угрозы типа «доступность». В целях повышения безопасности системы следует принять дополнительные меры и усилить уже имеющиеся средства защиты на сервере закрытого контура. Возможно, следует усилить уже имеющиеся средства защиты на сервере открытого контура.

Итоговая вероятность реализации угрозы нарушение «целостности» составила около 10% для серверов «закрытого» и «открытого» контуров. Значение риска для ресурсов при этом равняется 21 у.е. и 16 у.е. для серверов «закрытого» и «открытого» контуров соответственно. Поскольку предполагаемый риск меньше чем даже половина допустимого ущерба «целостности» в год (в среднем это 42 у.е. и 33 у.е. соответственно), можно сделать вывод, что информационная система организации хорошо защищена от угрозы этого типа.

6. Содержание отчета

1. Цель работы.
2. Теоретические положения.
3. Структурно-функциональная схема ИС«закрытого» и «открытого» контура ИС, с указанием защищаемых ресурсов.
4. Архитектура ИС.
5. Полученные результаты расчетов (для каждого вида информации)
   - 5.1. Итоговая вероятность реализации угрозы нарушения «конфиденциальности».
   - 5.2. Итоговая вероятность реализации угрозы нарушения «целостности».
   - 5.3. Итоговая вероятность реализации угрозы нарушения «доступности».
   - 5.4. Сравнительная оценка рисков по угрозе нарушение «конфиденциальности», «целостности» и «доступности».
6. Выводы

7. Контрольные вопросы

1. Что лежит в основе построения логической структуры ИС и определения информационных потоков?
2. Как выбрать веса средства защиты каждого аппаратного ресурса и средства защиты каждого вида информации, хранящемся и обрабатываем на нем?
3. Как определяется ущерб организации от реализации угроз ИБ для каждого информационного потока?
4. Приведите последовательность расчета рисков для каждого вида ценной информации по угрозе нарушение «конфиденциальности».
5. Рассчитать риски для каждого вида ценной информации по угрозе нарушение «целостности».

6. Рассчитать риски для каждого вида ценной информации по угрозе нарушение «доступности».
7. Как проводится расчет коэффициентов защищенности?
8. Как проводится расчет итоговой вероятности (ИВ)?
9. Как проводится расчет риска по угрозе нарушение «конфиденциальности» для каждого вида информации?
10. Чем отличается расчет риска по угрозе нарушение «конфиденциальности» для каждого вида информации от аналогичных расчетов риска по угрозам нарушение «целостности» и «доступности»?
11. Как проводится расчет риска по угрозе нарушение «конфиденциальности» для ресурса?
12. Чем отличается расчет риска по угрозе нарушение «конфиденциальности» для ресурса от аналогичных расчетов риска по угрозам нарушение «целостности» и «доступности»?

Библиографический список

1. ГОСТ Р ИСО 7498-2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.2. Архитектура защиты. М.: ИПК «Издательство стандартов», 1999.
2. Мошак Н.Н., Тимофеев Е.А. Особенности построения политики информационной безопасности в инфокоммуникационной сети // Электросвязь. 2005, №9.
3. Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез: монография. СПб.: ГУАП, 2014. 193 с.
4. Мошак Н.Н., Татарникова Т.М. Защита сетей от несанкционированного доступа. Учеб. пособие / СПб.: ГУАП, 2014. с. 121.
5. ЗимаВ., Молдовян А., Молдовян.Н. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000. 320 с.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника. 2004.
7. Мошак Н.Н. Безопасность информационных систем: Учеб. пособие/ Н.Н.Мошак – СПб.: ГУАП, 2019. – 169 с.
   ISBN 978-5-8088-1414-1

Оглавление