Цель работы: рассчитать риск информационной системы (ИС) на основе модели информационных потоков.

Теоретические положения

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 проводится оценки 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.

Составление структурно-функциональной схемы ИС

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» контур из «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» контурами корпоративной 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.

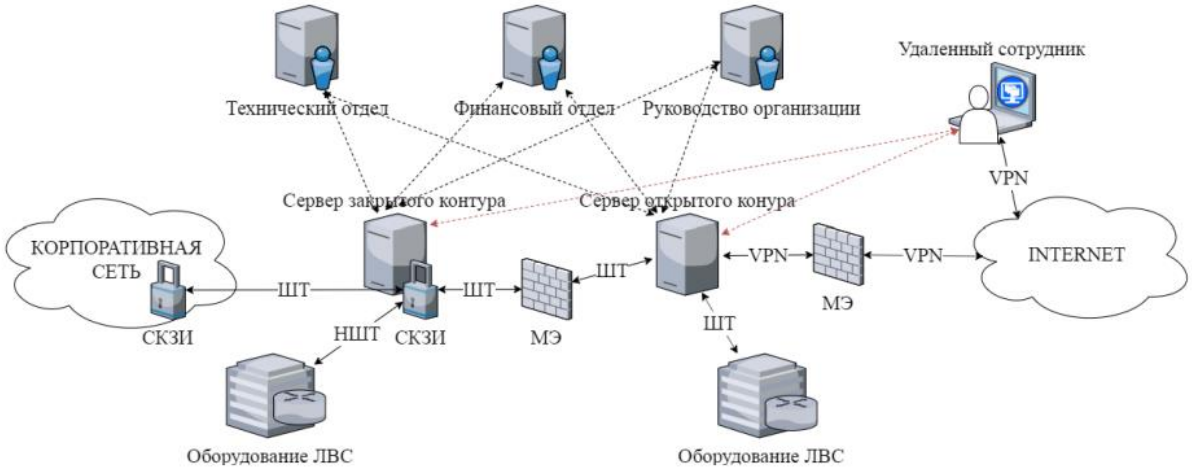

Рис.5.1. Структурно-функциональная схема ИС организации

Рисунок 1 - Структурно-функциональная схема ИС

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 доступа к ним удалённого сотрудника и группы пользователей.

Определения веса ресурса

Определим вес средств защиты каждого аппаратного ресурса, средств защиты каждого вида информации, хранящемся на нем, а также ПО с указанием веса каждого средства.

Таблица 1 - Вес ресурса

Тип средства защиты	Средство защиты	Вес средства защиты
Средства защиты закрытого контура		
Средства физической защиты	[Д,К] Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение)	35
	[К] Система наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом	30
Средства локальной защиты	[Ц] Настроенная политика аудита (учет всех действий на сервере, в т. ч. авторизация, выход из учетной записи, модификации данных)	25
	[К, Ц] Отсутствие дисководов и USB-портов (исключение возможности использования внешних носителей с предположительно вредоносным кодом и/или выгрузки информации)	25
Средства корпоративной сетевой защиты	[Д] Межсетевой экран	20
	[К, Ц] Система антивирусной защиты	20
	[Ц] Система обнаружения и предотвращения утечек (DLP-система)	15
Средства резервирования и контроля целостности	[Д, Ц] Средства создания резервной копии (каждые три дня)	15

	[Ц] Аппаратная система контроля целостности	20
Средства защиты открытого контура		
Средства физической защиты	[К,Д] Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение)	30
	[К] Система наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом	25
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 защиты	[Д] Межсетевой экран	20
	[К, Ц] Система антивирусной защиты	25
	[Ц] Система обнаружения и предотвращения утечек (DLP-система)	15
Средства резервирования и контроля целостности	[Д, Ц] Средства создания резервной копии (резервная копия создается каждые три дня в соответствии с политикой безопасности организации)	10

	[Ц] Аппаратная система контроля целостности	20
Средства защиты информации		
Средство локальной защиты	[Ц] Использование средств криптографической защиты информации	35
	[Д] Распределение прав доступа к информации в соответствии с матрицей доступа	30
	[К, Ц] Наличие соглашений о конфиденциальности (исключение разглашения конфиденциальной информации сотрудниками организации)	30
Средства резервирования и контроля целостности	[Д, Ц] Средства создания резервной копии (резервная копия создается каждые три дня в соответствии с политикой безопасности организации)	15
	[Ц] Аппаратная система контроля целостности	20
Средства защиты рабочих мест		
Средства физической защиты	[К, Д] Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком)	30
	[К] Система наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом	25
Средства локальной защиты	[К, Ц] Наличие соглашений о конфиденциальности (исключение разглашения конфиденциальной	25

	информации сотрудниками организации)	
	[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	15
	[Ц] Средства антивирусной защиты (антивирусный монитор)	25
Средства персональной сетевой защиты	[К, Ц] Система криптозащиты электронной почты	30
	[Д, К] Система криптозащиты электронной почты	25

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

Описание типов и прав доступа сотрудников

Приведем сводную таблицу 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 периодически контролирует деятельность других отделов – необходимо наличие двух информационных потоков от руководства к открытому и закрытому контурам. Удаленному сотруднику предоставлен только доступ к открытому серверу. 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 2 – Тип и права доступа

Информационный поток	**Вид доступа**	**Права доступа**	**VPN-соединение**	**Количество человек**
Руководство организации – Сервер закрытого контура	Локальный	Чтение, запись, удаление	Не требуется	10
Руководство организации – Сервер открытого контура	Локальный	Чтение, запись, удаление	Не требуется	
Технический отдел – Сервер закрытого контура	Локальный	Чтение, запись, удаление	Не требуется	15
Технический отдел – Сервер открытого контура	Локальный	Чтение, запись, удаление	Не требуется	
Финансовый отдел – Сервер закрытого контура	Локальный	Чтение	Не требуется	20
Финансовый отдел – Сервер открытого контура	Локальный	Чтение, запись	Не требуется	
Удаленный сотрудник – Сервер открытого контура	Удаленный	Чтение, запись	Да	5

Доступ в сети Интернет

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.

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 3 - Доступ сети Интернет

Отдел	**Доступ к сети Интернет**
Руководство организации	Есть
Технический отдел	Есть
Финансовый отдел	Нет

Определение ущерба организации при реализации угроз ИБ для каждого информационного потока

Приведем сводную таблицу, в которой перечислим ущерб организации, который возникнет в случае реализации угроз ИБ для каждого информационного потока.

Таблица 4 – Ущерб при реализации угроз ИБ

Информационный поток	**Конфиденциальность (у.е. в год)**	**Доступность (у.е. в час)**	**Целостность (у.е. в год)**
Руководство организации – Сервер закрытого контура	100	75	90
Руководство организации – Сервер открытого контура	80	70	65
Технический отдел – Сервер закрытого контура	90	70	60
Технический отдел – Сервер открытого контура	65	65	55

Финансовый отдел – Сервер закрытого контура	85	55	45
Финансовый отдел – Сервер открытого контура	75	45	40
Удаленный сотрудник – Сервер открытого контура	65	30	30

Расчет рисков по угрозе нарушения «конфиденциальности»

6.1 Расчет коэффициентов защищенности

Для каждого информационного потока рассчитывается коэффициент локальной либо удаленной защищенности информации, хранящейся на ресурсе, в зависимости от типа доступа. Если доступ локальный, то рассчитывается только коэффициент локальной защищенности информации. Если доступ удаленный, то рассчитывается коэффициент удаленной защищенности информации, хранящейся на ресурсе и коэффициент локальной защищенности рабочего места пользователя.

Коэффициент локальной защищенности информации рассчитывается, если доступ к информации в данном информационном потоке *локальный*. Он равен сумме весов средств физической и локальной защиты информации. Учитываются все средства физической защиты и средства локальной защиты информации, обеспечивающие защиту информации по угрозе «конфиденциальность».

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

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.

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

Таблица 5 - Расчет наименьших коэффициентов для информационных потоков

Информационный поток	**Коэффициент локальной защищенности информации**	**Коэффициент удаленной защищенности информации**	**Коэффициент локальной защищенности рабочего места**	**НК**
Руководство организации – Сервер закрытого контура	120	-	175	120
Руководство организации – Сервер открытого контура	95	-	150	95
Технический отдел – Сервер закрытого контура	95	-	150	95
Технический отдел – Сервер открытого контура	85	-	140	85
Финансовый отдел – Сервер закрытого контура	60	-	90	60
Финансовый отдел – Сервер открытого контура	55	-	85	55
Удаленный сотрудник – Сервер открытого контура	30	20	45	20

6.2 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.

Таблица 6 - Расчет результирующих коэффициентов для информационных потоков

Информационный поток	**НК**	**Вес VPN соединения**	**Результирующий коэффициент**
Руководство организации – Сервер закрытого контура	120	0	120
Руководство организации – Сервер открытого контура	95	0	95
Технический отдел – Сервер закрытого контура	95	0	95
Технический отдел – Сервер открытого контура	85	0	85
Финансовый отдел – Сервер закрытого контура	60	0	60
Финансовый отдел – Сервер открытого контура	55	0	55
Удаленный сотрудник – Сервер открытого контура	20	20	40

6.3 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 ИК увеличивается 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.

Таблица 7 - Расчет итогового коэффициента защищенности

Информационный поток	**РК**	**Количество человек в группе**	**Наличие Интернет-соединения**	**Итоговый коэффициент защищенности (ИК)**
Руководство организации – Сервер закрытого контура	120	10	Да (ИК=2N/РК)	0,16
Руководство организации – Сервер открытого контура	95			0,21
Технический отдел – Сервер закрытого контура	95	15	да (ИК=2N/РК)	0,31
Технический отдел – Сервер открытого контура	85			0,35
Финансовый отдел – Сервер закрытого контура	60	20	Нет (ИК=N/РК)	0,33
Финансовый отдел – Сервер открытого контура	55			0,36
Удаленный сотрудник –	40	5	Да (ИК=2N/РК)	0,25

Сервер открытого контура				

6.4 Расчет итоговой вероятности

Чтобы получить итоговую вероятность (ИВ), необходимо сначала определить базовую вероятность (БВ) реализации угрозы нарушения конфиденциальности и умножить её на ИК: ИВ=БВ×ИК. Базовая вероятность 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×ИК. Итоговая вероятность $ИВ = 1 - ((1 - ИВ_1)(1 - ИВ_2) \dots (1 - ИВ_N))$, как суммарная по нескольким группам пользователей.

Таблица 8 - Расчет итоговой вероятности

Информационный поток	**БВ**	**ИБВ**	**ИК**	**ПВ**	**ИВ**
Закрытый контур					
Руководство организации – Сервер закрытого контура	0,01	0,2	0,16	0,032	0,151
Технический отдел – Сервер закрытого контура	0,03		0,31	0,062	
Финансовый отдел – Сервер закрытого контура	0,01		0,33	0,066	
Открытый контур					
Руководство организации – Сервер открытого контура	0,02	0,25	0,21	0,052	0,261
Технический отдел – Сервер открытого контура	0,04		0,35	0,087	

Финансовый отдел – Сервер открытого контура	0,02		0,36	0,09	
Удаленный сотрудник – Сервер открытого контура	0,04		0,25	0,062	

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.

6.5 Расчёт риска по угрозе нарушение «конфиденциальности» для каждой информации

Риск по угрозе «конфиденциальность» для каждой информации рассчитывается как произведение итоговой вероятности на ущерб.

Таблица 9 - Расчет риска

Информационный поток	**ИВ**	**Ущерб**	**Значение риска**
Закрытый контур			
Руководство организации – Сервер закрытого контура	0,151	100	15

Технический отдел – Сервер закрытого контура		90	13
Финансовый отдел – Сервер закрытого контура		85	13
Открытый контур			
Руководство организации – Сервер открытого контура	0,261	80	20
Технический отдел – Сервер открытого контура		65	16
Финансовый отдел – Сервер открытого контура		75	19
Удаленный сотрудник – Сервер открытого контура		65	17

7.1 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.

Таблица 10 - Расчет риска для ресурса

Информационный поток	**Значение риска для информации**	**Значение риска для ресурса**
Закрытый контур		
Руководство организации – Сервер закрытого контура	15	41

Технический отдел – Сервер закрытого контура	13	
Финансовый отдел – Сервер закрытого контура	13	
Открытый контур		
Руководство организации – Сервер открытого контура	20	72
Технический отдел – Сервер открытого контура	16	
Финансовый отдел – Сервер открытого контура	19	
Удаленный сотрудник – Сервер открытого контура	17	

Расчет рисков по угрозе нарушения «доступности»

8.1 Расчет коэффициентов защищенности

Расчеты производятся аналогичным образом, однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности.

Таблица 11 - Расчет коэффициентов защищенности

Информационный поток	**Коэффициент локальной защищенности информации**	**Коэффициент удаленной защищенности информации**	**Коэффициент локальной защищенности рабочего места**	**НК**
Руководство организации – Сервер закрытого контура	65	-	90	65
Руководство организации – Сервер открытого контура	60	-	85	60
Технический отдел – Сервер закрытого контура	65	-	90	65

Технический отдел – Сервер открытого контура	60	-	85	60
Финансовый отдел – Сервер закрытого контура	50	-	75	50
Финансовый отдел – Сервер открытого контура	45	-	70	45
Удаленный сотрудник – Сервер открытого контура	45	20	70	20

8.2 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.

Таблица 12 - Учет наличия доступа через VPN

Информационный поток	**НК**	**Вес VPN соединения**	**Результирующий коэффициент**
Руководство организации – Сервер закрытого контура	65	0	65
Руководство организации – Сервер открытого контура	60	0	60
Технический отдел – Сервер закрытого контура	65	0	65
Технический отдел – Сервер открытого контура	60	0	60

Финансовый отдел – Сервер закрытого контура	50	0	50
Финансовый отдел – Сервер открытого контура	45	0	45
Удаленный сотрудник – Сервер открытого контура	20	20	40

8.3 Расчёт итогового коэффициента защищённости

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности.

Таблица 13 - Расчет итогового коэффициента защищенности

Информационный поток	**РК**	**Количество человек в группе**	**Наличие Интернет-соединения**	**Итоговый коэффициент защищенности (ИК)**
Руководство организации – Сервер закрытого контура	65	10	Да (ИК=2N/РК)	0,307
Руководство организации – Сервер открытого контура	60			0,333
Технический отдел – Сервер закрытого контура	65	15	да (ИК=2N/РК)	0,461
Технический отдел – Сервер открытого контура	60			0,5

Финансовый отдел – Сервер закрытого контура	50	20	Нет (ИК=N/РК)	0,4
Финансовый отдел – Сервер открытого контура	45			0,444
Удаленный сотрудник – Сервер открытого контура	40	5	Да (ИК=2N/РК)	0,25

8.4 Расчет итоговой вероятности

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угрозы доступности.

Таблица 14 - Расчет итоговой вероятности

Информационный поток	**БВ**	**ИБВ**	**ИК**	**ПВ**	**ИВ**
Закрытый контур					
Руководство организации – Сервер закрытого контура	0,02	0,15	0,307	0,046	0,165
Технический отдел – Сервер закрытого контура	0,03		0,461	0,069	
Финансовый отдел – Сервер закрытого контура	0,05		0,4	0,06	
Открытый контур					
Руководство организации – Сервер открытого контура	0,02	0,17	0,333	0,056	0,234

Технический отдел – Сервер открытого контура	0,04		0,5	0,085	
Финансовый отдел – Сервер открытого контура	0,05		0,444	0,075	
Удаленный сотрудник – Сервер открытого контура	0,05		0,25	0,042	

8.5 Расчёт риска по угрозе нарушение «доступности» для каждой информации

Риск по угрозе «доступность» для каждой информации рассчитывается как произведение итоговой вероятности на ущерб.

Таблица 15 - Расчет риска

Информационный поток	**ИВ**	**Ущерб**	**Значение риска**
Закрытый контур			
Руководство организации – Сервер закрытого контура	0,165	75	12
Технический отдел – Сервер закрытого контура		70	11
Финансовый отдел – Сервер закрытого контура		55	9
Открытый контур			
Руководство организации – Сервер открытого контура	0,234	70	16

Технический отдел – Сервер открытого контура		65	15
Финансовый отдел – Сервер открытого контура		45	10
Удаленный сотрудник – Сервер открытого контура		30	7

8.6 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.

Таблица 16 - Расчет риска для ресурса

Информационный поток	**Значение риска для информации**	**Значение риска для ресурса**
Закрытый контур		
Руководство организации – Сервер закрытого контура	12	32
Технический отдел – Сервер закрытого контура	11	
Финансовый отдел – Сервер закрытого контура	9	
Открытый контур		
Руководство организации – Сервер открытого контура	16	48
Технический отдел – Сервер открытого контура	15	
Финансовый отдел – Сервер открытого контура	10	

Удаленный сотрудник – Сервер открытого контура	7	

Расчет рисков по угрозе нарушения «целостности»

9.1 Расчет коэффициентов защищенности

Расчеты производятся аналогичным образом, однако теперь рассматриваются средства, закрывающие данный тип угрозы – угроза целостности.

Таблица 17 - Расчет коэффициентов защищенности

Информационный поток	**Коэффициент локальной защищенности информации**	**Коэффициент удаленной защищенности информации**	**Коэффициент локальной защищенности рабочего места**	**НК**
Руководство организации – Сервер закрытого контура	85	-	115	85
Руководство организации – Сервер открытого контура	65	-	95	65
Технический отдел – Сервер закрытого контура	50	-	80	50
Технический отдел – Сервер открытого контура	45	-	70	45
Финансовый отдел – Сервер закрытого контура	55	-	85	55
Финансовый отдел – Сервер открытого контура	45	-	75	45
Удаленный сотрудник –	45	40	65	40

Сервер открытого контура				

9.2 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.

Таблица 18 - Учет наличия доступа через VPN и средств резервирования и контроля "целостности"

Информационный поток	**НК**	**Вес VPN соединения**	**Веса средств резервирования и копирования**	**Результирующий коэффициент (РК)**
Руководство организации – Сервер закрытого контура	85	0	35	120
Руководство организации – Сервер открытого контура	65	0	30	95
Технический отдел – Сервер закрытого контура	50	0	35	85
Технический отдел – Сервер открытого контура	45	0	25	70
Финансовый отдел – Сервер закрытого контура	55	0	35	90
Финансовый отдел – Сервер открытого контура	45	0	25	70
Удаленный сотрудник –	40	20	10	70

Сервер открытого контура				

9.3 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.

Таблица 19 - Расчет итогового коэффициента защищенности

Информационный поток	**РК**	**Наличие резервного копирования**	**Количество человек в группе**	**Наличие Интернет-соединения**	**Итоговый коэффициент защищенности (ИК)**
Руководство организации – Сервер закрытого контура	120	1	10	Да (ИК=2N/РК)	0,166
Руководство организации – Сервер открытого контура	95	1			0,210
Технический отдел – Сервер закрытого контура	85	1	15	да (ИК=2N/РК)	0,352
Технический отдел – Сервер открытого контура	70	1			0,428
Финансовый отдел – Сервер закрытого контура	90	1	20	Нет (ИК=N/РК)	0,222

Финансовый отдел – Сервер открытого контура	70	1			0,285
Удаленный сотрудник – Сервер открытого контура	70	1	5	Да (ИК=2N/РК)	0,142

9.4 Расчет итоговой вероятности

Расчеты производятся аналогичным образом, как и для типа угрозы «конфиденциальность», однако теперь рассматриваются средства, закрывающие данный тип угрозы – угроза целостности.

Таблица 20 - Расчет итоговой вероятности

Информационный поток	**БВ**	**ИБВ**	**ИК**	**ПВ**	**ИВ**
Закрытый контур					
Руководство организации – Сервер закрытого контура	0,01	0,12	0,166	0,019	0,084
Технический отдел – Сервер закрытого контура	0,02		0,352	0,042	
Финансовый отдел – Сервер закрытого контура	0,03		0,222	0,026	
Открытый контур					
Руководство организации – Сервер открытого контура	0,01	0,15	0,210	0,031	0,149
Технический отдел – Сервер открытого контура	0,02		0,428	0,064	

Финансовый отдел – Сервер открытого контура	0,03		0,285	0,042	
Удаленный сотрудник – Сервер открытого контура	0,04		0,142	0,021	

9.5 Расчёт риска по угрозе нарушение «целостности» для каждой информации

Риск по угрозе нарушения «целостности» для каждой информации рассчитывается как произведение итоговой вероятности на ущерб.

Таблица 21 - Расчет риска для каждой информации

Информационный поток	**ИВ**	**Ущерб**	**Значение риска**
Закрытый контур			
Руководство организации – Сервер закрытого контура	0,084	90	7
Технический отдел – Сервер закрытого контура		60	5
Финансовый отдел – Сервер закрытого контура		45	3
Открытый контур			
Руководство организации – Сервер открытого контура	0,149	65	9
Технический отдел – Сервер открытого контура		55	8

Финансовый отдел – Сервер открытого контура		40	5
Удаленный сотрудник – Сервер открытого контура		30	4

9.6 Расчёт риска по угрозе нарушение «целостности» 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.

Таблица 22 - Расчет риска для ресурса

Информационный поток	**Значение риска для информации**	**Значение риска для ресурса**
Закрытый контур		
Руководство организации – Сервер закрытого контура	7	15
Технический отдел – Сервер закрытого контура	5	
Финансовый отдел – Сервер закрытого контура	3	
Открытый контур		
Руководство организации – Сервер открытого контура	9	26
Технический отдел – Сервер открытого контура	8	
Финансовый отдел – Сервер открытого контура	5	
Удаленный сотрудник – Сервер открытого контура	4	

Выводы: в ходе выполнения практической работы был рассчитаны риски информационной системы на основе модели информационных потоков. 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».

Итоговая вероятность реализации угрозы «конфиденциальность» около 15% и 26% для серверов «закрытого» и «открытого» контуров. Значение риска для ресурсов при этом равняется 41 у.е. и 72 у.е. для серверов «закрытого» и «открытого» контуров соответственно. Поскольку предполагаемый риск для открытого сервера больше, а для закрытого – меньше, чем допустимый ущерб конфиденциальности в год (в среднем это 91 у.е. и 71 у.е. соответственно), можно сделать вывод, что информационная система организации слабо защищена от угрозы типа «конфиденциальность». В целях повышения безопасности системы следует принять дополнительные меры и усилить уже имеющиеся средства защиты на сервере открытого контура.

Итоговая вероятность реализации угрозы нарушения «доступности» составила около 16% и 23% для серверов «закрытого» и «открытого» контуров. Значение риска для ресурсов при этом равняется 32 у.е. и 48 у.е. для серверов «закрытого» и «открытого» контуров соответственно. Поскольку предполагаемый риск меньше, чем допустимый ущерб доступности в год (в среднем это 66 у.е. и 52 у.е. соответственно), можно сделать вывод, что информационная система организации хорошо защищена от угрозы этого типа.

Итоговая вероятность реализации угрозы нарушения «целостности» составила около 8% и 15% для серверов «закрытого» и «открытого» контуров. Значение риска для ресурсов при этом равняется 15 у.е. и 26 у.е. для серверов «закрытого» и «открытого» контуров соответственно. Поскольку предполагаемый риск меньше допустимого ущерба «целостности» в год (в среднем это 65 у.е. и 48 у.е. соответственно), можно сделать вывод, что информационная система организации хорошо защищена от угрозы этого типа.