Пример расчета риска информационной безопасности на основе модели информационных потоков

Входные данные

Например, информационная система Компании состоит из двух ресурсов: сервера и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связанны между собой. На сервере хранятся виды информации: бухгалтерский отчет и база клиентов Компании. На рабочей станции расположена база данных наименований товаров Компании с описанием.

К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет):

- **главный бухгалтер.**

К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов Компании):

- **бухгалтер (с рабочей станции);**
- **финансовый директор (через глобальную сеть Интернет).**

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров Компании с описанием):

- **бухгалтер.**

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. Причем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Средства защиты

1. **Средства защиты сервера:**

Средство защиты	**Эффективность средства защиты**
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение)	**25**
Средства локальной защиты	
Отсутствие возможности подключения внешних носителей	**10**

Средства корпоративной сетевой защиты	
Межсетевой экран	**10**
Обманная система	**2**
Система антивирусной защиты на сервере	**10**
Средства резервирования и контроля целостности	
Аппаратная система контроля целостности	**20**

2. **1.1. Средства защиты первой информации (бухгалтерский отчет):**

Средство защиты	**Эффективность средства защиты**
Средства локальной защиты	
Средства криптографической защиты (криптозащита данных на ПК)	**20**
Средства резервирования и контроля целостности	
Резервное копирование	**10**
Программная система контроля целостности	**10**

3. **1.2. Средства защиты второй информации (база клиентов Компании):**
4. **Средств защиты информации нет.**
5. **Средства защиты рабочей станции:**

Средство защиты	**Эффективность средства защиты**
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	**10**
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	**10**
Отсутствие возможности подключения внешних носителей	**10**
Средства персональной сетевой защиты	
Персональный межсетевой экран	**3**
Система криптозащиты электронной почты	**10**

6. **2.1. Средства защиты информации (база данных наименований товаров Компании с их описанием):**

Средство защиты	**Эффективность средства защиты**
Средства резервирования и контроля целостности	
Резервное копирование	**10**
Программная система контроля целостности	**10**

7. **Средства защиты клиентского места группы пользователей:**

3.1. Средства защиты клиентского места бухгалтера (группа обычных пользователей):

Средство защиты	Эффективность средства защиты
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	**10**
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	**10**
Отсутствие возможности подключения внешних носителей	**10**
Средства персональной сетевой защиты	
Персональный межсетевой экран	**3**
Система криптозащиты электронной почты	**10**

3.2. Средства защиты клиентского места главного бухгалтера (группа обычных пользователей):

Средство защиты	Эффективность средства защиты
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	**10**
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	**10**
Отсутствие возможности подключения внешних носителей	**10**
Средства персональной сетевой защиты	
Персональный межсетевой экран	**3**
Система криптозащиты электронной почты	**10**

3.3. Средства защиты клиентского места финансового директора (группа авторизованных Интернет-пользователей):

Средства защиты клиентского места групп авторизованных Интернет-пользователей невозможно оценить, т.к. неизвестно, откуда будут осуществлять доступ пользователи этой группы.

Вид и права доступа групп пользователей к информации, наличие соединения через VPN, количество человек в группе:

	Вид доступа	Права доступа	Наличие VPN-соединения	Количество человек в группе
Главный бухгалтер / бухгалтерский отчет	**локальный**	**чтение, запись,**	**нет**	**1**

		удаление		
Бухгалтер / база клиентов Компании	**удаленный**	**чтение**	**есть**	**1**
Финансовый директор / база клиентов Компании	**удаленный**	**чтение, запись**	**есть**	**1**
Бухгалтер / база данных наименований товаров Компании	**локальный**	**чтение, запись, удаление**	**нет**	**1**

Наличие у группы пользователей выхода в Интернет:

	Доступ в Интернет
Главный бухгалтер	**Есть**
Бухгалтер	**Нет**
Финансовый директор	**Не анализируется**

Ущерб Компании от реализации угроз информационной безопасности:

	Конфиденциальность (у.е. в год)	Целостность (у.е. в год)	Доступность (у.е. в час)
Главный бухгалтер / бухгалтерский отчет	**100**	**100**	**1**
Бухгалтер / база клиентов Компании	**100**	**100**	**1**
Финансовый директор / база клиентов Компании	**100**	**100**	**1**
Бухгалтер / база данных наименований товаров Компании	**100**	**100**	**1**

Наследование:

Т.к. сервер и рабочая станция Компании находятся в одной сетевой группе, т.е. физически соединены между собой, необходимо распространить наименьший коэффициент защиты и наибольшую базовую вероятность группы Интернет-пользователей на все информации на всех ресурсах, входящих в сетевую группу.

Пример расчета рисков по угрозе конфиденциальность

Коэффициенты защищенности:

При локальном доступе к информации на ресурсе необходимо найти коэффициент локальной защищенности информации на ресурсе, который состоит из суммы эффективностей средств физической и локальной защиты.

При удаленном доступе рассчитываем коэффициенты локальной защищенности рабочего места группы пользователей, имеющей доступ к информации, (сумма эффективностей средств физической, локальной и персональной сетевой защиты) и удаленной защищенности информации на ресурсе (сумма эффективностей средств корпоративной сетевой защиты). В дальнейших расчетах участвует наименьший коэффициент.

При локальном и удаленном доступе находим все три коэффициента, из которых также выбираем наименьший.

Расчет рисков по угрозе конфиденциальность:

1. **Коэффициенты защищенности:**

	Коэффициент локальной защищенности информации	**Коэффициент удаленной защищенности информации**	**Коэффициент локальной защищенности рабочего места группы пользователей**	**Наименьший коэффициент**
Главный бухгалтер / бухгалтерский отчет	**55**	**-**	**-**	**55**
Бухгалтер / база клиентов Компании	**-**	**22**	**43**	**22**
Финансовый директор / база клиентов Компании	**-**	**22**	**-**	**22**
Бухгалтер / база данных наименований товаров Компании	**30**	**-**	**-**	**30**

2. **Учет наличия доступа при помощи VPN:**

При локальном доступе наличие VPN не анализируется. При удаленном доступе при использовании VPN к наименьшему коэффициенту защищенности прибавляется эффективность VPN шлюза (20). Если при удаленном доступе VPN-соединение не используется для групп Интернет-пользователей, итоговый коэффициент защищенности умножается на 4, для групп обычных пользователей (не Интернет-пользователей) – остается неизменным.

	Наименьший коэффициент	**Эффективность VPN-соединения**	**Результирующий коэффициент**
Главный бухгалтер /	**55**	**-**	**55**

бухгалтерский отчет			
Бухгалтер / база клиентов Компании	**22**	**20**	**42**
Финансовый директор / база клиентов Компании	**22**	**20**	**42**
Бухгалтер / база данных наименований товаров Компании	**30**	**-**	**30**

3. **Учет количества человек в группе и наличия у группы пользователей доступа в Интернет:**

	Результирующий коэффициент	**Количество человек в группе пользователей**	**Наличие у группы пользователей доступа в Интернет**	**Итоговый коэффициент**
Главный бухгалтер / бухгалтерский отчет	**55**	**1**	**2**	**0,036**
Бухгалтер / база клиентов Компании	**42**	**1**	**1**	**0,024**
Финансовый директор / база клиентов Компании	**42**	**1**	**-**	**0,024**
Бухгалтер / база данных наименований товаров Компании	**30**	**1**	**1**	**0,033**

4. **Если к информации имеет доступ группа пользователей, превышающая 50 человек, то это соответственно увеличивает итоговый коэффициент.**
5. **Если группа пользователей имеет доступ в Интернет, то это увеличивает итоговый коэффициент в 2 раза.**
6. **Пример расчета итогового коэффициента:**

7. **Итоговая вероятность:**

Чтобы получить итоговую вероятность, необходимо определить итоговую базовую вероятность и умножить ее на итоговый коэффициент.

Базовая вероятность	**Итоговая базовая**	**Итоговый коэффициент**	**Промежуточная вероятность**	**Итоговая вероятность**

					вероятность
Главный бухгалтер / бухгалтерский отчет	0,35	0,7	0,036	0,0252	0,0252
Бухгалтер / база клиентов Компании	0,35	0,7	0,024	0,0168	
Финансовый директор / база клиентов Компании	0,7	0,7	0,024	0,0168	0,0331
Бухгалтер / база данных наименований товаров Компании	0,35	0,7	0,033	0,0231	0,0231

Т.к. к информации на ресурсе, находящейся в сетевой группе, имеют доступ группа Интернет-пользователей, их базовая вероятность распространяется на все информации.

Итоговая вероятность для второй информации, к которой имеют доступ несколько групп пользователей, рассчитываем по формуле:

где Pinf - вероятность реализации угрозы для вида информации;
Pug,i - вероятность реализации угрозы для связи "информация - группа пользователей";
n - количество групп пользователей.

8. Риск по угрозе конфиденциальность.

	Итоговая вероятность	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	0,0252	100	2,52
База клиентов Компании	0,0331	100	3,31
База данных наименований товаров Компании	0,0231	100	2,31

Пример расчета рисков по угрозе целостность

1. Первые три пункта вычисляются аналогично расчету по угрозе конфиденциальность.
2. Учет средств резервирования и контроля целостности:

	Наименьший коэффициент	Эффективность VPN-соединения	Эффективность средств резервирования	Результирующий коэффициент

			и контроля целостности	
Главный бухгалтер / бухгалтерский отчет	**55**	**-**	**40**	**95**
Бухгалтер / база клиентов Компании	**22**	**20**	**20**	**62**
Финансовый директор / база клиентов Компании	**22**	**20**	**20**	**62**
Бухгалтер / база данных наименований товаров Компании	**30**	**-**	**20**	**50**

3. **Учет наличия резервного копирования, количества человек в группе пользователей и наличия у группы пользователей доступа в Интернет:**

	Результирующий коэффициент	**Наличие резервного копирования**	**Количество человек в группе пользователей**	**Наличие у группы пользователей доступа в Интернет**	**Итоговый коэффициент**
Главный бухгалтер / бухгалтерский отчет	**95**	**1**	**1**	**2**	**0,021**
Бухгалтер / база клиентов Компании	**62**	**1**	**1**	**1**	**0,016**
Финансовый директор / база клиентов Компании	**62**	**4**	**1**	**-**	**0,065**
Бухгалтер / база данных наименований товаров Компании	**50**	**1**	**1**	**1**	**0,02**

4. **Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то эффективность резервного копирования (10) прибавляется к коэффициенту защищенности. Если у информации на ресурсе резервное копирование не осуществляется, и группе**

пользователей, имеющей доступ к информации, разрешены запись или удаление, то итоговый коэффициент увеличивается в 4 раза.

5. **Аналогично расчету по угрозе конфиденциальность получим итоговую вероятность:**

	Базовая вероятность	Итоговая базовая вероятность	Итоговый коэффициент	Промежуточная вероятность	Итоговая вероятность
Главный бухгалтер / бухгалтерский отчет	0,25	0,7	0,021	0,0147	0,0147
Бухгалтер / база клиентов Компании	0,1	0,7	0,016	0,0112	
Финансовый директор / база клиентов Компании	0,7	0,7	0,065	0,0455	0,05619
Бухгалтер / база данных наименований товаров Компании	0,25	0,7	0,02	0,014	0,014

6. **Риск по угрозе целостность**

	Итоговая вероятность:	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	0,0147	100	1,47
База клиентов Компании	0,05619	100	5,61
База данных наименований товаров Компании	0,014	100	1,4

Пример расчета рисков по угрозе отказ в обслуживании

Расчет рисков по угрозе доступность

1. **Расчет коэффициента защищенности по угрозе доступность.**

   При расчете рисков по угрозе доступность анализируются средства резервирования: кластер, резервное копирование и резервный канал. Влияние резервного канала учитывается в том случае, если группа обычных пользователей (не Интернет-пользователей) имеет только удаленный доступ к информации на ресурсе.

	Кластер		Резервное копирование		Резервный канал	
	есть	нет	есть	нет	есть	нет
Запись и Удаление	20	Const	4	Увеличивается в 5 раз	5	Const

Удаление	**20**	**Const**	**4**	**Увеличивается в 4 раз**	**5**	**Const**
Запись	**20**	**Const**	**4**	**Увеличивается в 4 раз**	**5**	**Const**
Чтение	**40**	**Const**	**4**	**Увеличивается в 2 раз**	**5**	**Const**

	Коэффициент защищенности	**Наличие у группы пользователей доступа в Интернет**	**Итоговый коэффициент**
Главный бухгалтер / бухгалтерский отчет	**0,25**	**2**	**0,5**
Бухгалтер / база клиентов Компании	**2**	**1**	**2**
Финансовый директор / база клиентов Компании	**4**	**-**	**4**
Бухгалтер / база данных наименований товаров Компании	**0,25**	**1**	**0,25**

2. **Расчет итогового времени простоя**

	Базовое время простоя	**Итоговое базовое время простоя**	**Время простоя сетевого оборудования**	**Итоговый коэффициент**	**Промежуточное время простоя**	**Итоговое время простоя**
Главный бухгалтер / бухгалтерский отчет	**40**	**70**	**-**	**0,5**	**35**	**35**
Бухгалтер / база клиентов Компании	**40**	**70**	**10**	**2**	**140**	**280**
Финансовый директор / база клиентов Компании	**70**	**70**	**-**	**4**	**280**	
Бухгалтер / база данных наименований товаров Компании	**40**	**40**	**-**	**0,25**	**10**	**10**

3. **При расчете рисков по угрозе доступность базовые времена простоя наследуются только в пределах ресурса.**
4. **Время простоя сетевого оборудования добавляется к итоговому времени простоя.**
5. **Если итоговое время простоя превышает максимально критичное (280 часов в год по базовым настройкам), оно приравнивается к максимально критичному времени простоя.**

6. **Для второй информации на сервере, к которой имеют доступ несколько групп пользователей, итоговое время простоя рассчитывается по следующей формуле:**

где Tinf - время простоя для информации;
Tmax - максимальное критичное время простоя;
Tug,i - время простоя для связи "информация - группа пользователей";
n - количество групп пользователей.

7. **Расчет рисков**

	Итоговое время простоя	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	**35**	**1**	**35**
База клиентов Компании	**280**	**1**	**280**
База данных наименований товаров Компании	**10**	**1**	**10**

Влияние ответов политики безопасности на коэффициенты

Модель информационных потоков не может учесть организационные меры, вопросы, связанные с поведением сотрудников организации и некоторые другие аспекты. Для того, чтобы наиболее полно охватить все угрозы, действующие на информационные ресурсы организации, вводится раздел "Политика безопасности", который содержит вопросы. Ответы на вопросы "Политики безопасности" влияют на эффективность средств защиты и изменяют риск реализации угроз информационной безопасности.

Разделы Политики безопасности:

1. **Политика безопасности**
2. **Организационные меры**
3. **Безопасность персонала**
4. **Физическая безопасность**
5. **Управление коммуникациями и процессами**
6. **Контроль доступа**
7. **Разработка и сопровождение систем**
8. **Непрерывность ведения бизнеса**
9. **Соответствие системы требованиям**

Примеры вопросов:

Вопрос 1:

Существует ли в компании разработанная политика информационной безопасности, все положения которой на практике внедрены в информационную систему?

Варианты ответов:

- ***Да***
- ***Нет***

- *Положения политики внедрены частично*

Влияние ответов:

Да – эффективность средств защиты увеличивается на 10%;

Нет – эффективность средств защиты уменьшается на 10%;

Положения политики внедрены частично – эффективность средств защиты уменьшается на 3%.

Вопрос 2:

Может ли раскрытие какой-либо информации принести существенную выгоду посторонним лицам, заинтересованным организациям и т. п.?

Варианты ответов:

- ***Да***
- ***Нет***

Влияние ответов:

***Да* – эффективность средств защиты по угрозе Конфиденциальность по ресурсам, к которым имеют доступ группы Интернет-пользователей, уменьшается на 5%.**

***Нет* – эффективность средств защиты по угрозе Конфиденциальность по ресурсам, к которым имеют доступ группы Интернет-пользователей, увеличивается на 2%.**

Вопрос 3:

Администраторы или офицеры безопасности администрируют систему удаленно через Интернет, не применяя средств криптозащиты трафика?

Варианты ответов:

- **Да**
- **Нет**

Влияние ответов:

Да – эффективность средств защиты уменьшается на 50%. Эффективность средств защиты ресурсов, к которым имеют доступ группы администраторов или офицеров безопасности, уменьшается на 100%.

Нет – ничего не меняется.

Ущерб Компании от реализации угроз информационной безопасности:

	Конфиденциальность	**Целостность**	**Доступность**

	(у.е. в год)	(у.е. в год)	(у.е. в час)
Главный бухгалтер / бухгалтерский отчет	**100**	**100**	**1**
Бухгалтер / база клиентов Компании	**100**	**100**	**1**
Финансовый директор / база клиентов Компании	**100**	**100**	**1**
Бухгалтер / база данных наименований товаров Компании	**100**	**100**	**1**

Наследование:

Т.к. сервер и рабочая станция Компании находятся в одной сетевой группе, т.е. физически соединены между собой, необходимо распространить наименьший коэффициент защиты и наибольшую базовую вероятность группы Интернет-пользователей на все информации на всех ресурсах, входящих в сетевую группу.