

Алгоритм: модель информационных потоков

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Рассматривая средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации.

В результате работы алгоритма программа представляет следующие данные:

1. Инвентаризацию ресурсов;
2. Значения риска для каждого ценного ресурса организации;
3. Значения риска для ресурсов после задания контрмер (остаточный риск);
4. Эффективность контрмер;
5. Рекомендации экспертов.

Введение в модель

Для того, чтобы оценить риск информации, необходимо проанализировать защищенность и архитектуру построения информационной системы.

Владельцу информационной системы требуется сначала описать архитектуру своей сети:

- все ресурсы, на которых хранится ценная информация;
- все 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;
- 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 введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Основные понятия и допущения модели

- Ресурс – физический ресурс, на котором располагается ценная информация (сервер, рабочая станция, мобильный компьютер и т.д.)
- Сетевая группа – группа, в которую входят физически взаимосвязанные ресурсы.
- Отдел - структурное подразделение организации.
- Бизнес-процессы - производственные процессы, в которых обрабатывается ценная информация.
- Группа пользователей – группа пользователей, имеющая одинаковый класс и средства защиты. Субъект, осуществляющий доступ к информации.
- Класс группы пользователей – особая характеристика группы, показывающая, как осуществляется доступ к информации.
- Основные классы групп пользователей:
 - Анонимные Интернет-пользователи;
 - Авторизованные Интернет-пользователи;
 - Обычные пользователи, осуществляющие локальный и удаленный доступ к информации;
 - Системные администраторы и офицеры безопасности (так называемые, суперпользователи), т.е. пользователи, имеющие исключительные права;
 - Пользователи, осуществляющие доступ к информации из офиса компании через Интернет;
 - Пользователи, осуществляющие доступ к информации из офиса компании по модему;
 - Мобильные Интернет-пользователи.
- Средства защиты рабочего места группы пользователей – средства защиты клиентского места пользователя, т.е. ресурса, с которого пользователь осуществляет доступ к информации.
- Характеристики группы пользователей – под характеристиками группы пользователей понимаются виды доступа группы пользователей (локальный либо удаленный доступ) и права, разрешенные группе пользователей при доступе к информации (чтение, запись или удаление).
- Информация – ценная информация, хранящаяся и обрабатываемая в ИС. Т.е. объект, к которому осуществляется доступ. Исходя из допущений данной модели, вся информация является ценной, т.к. оценить риск неценной информации не представляется возможным.
- Средства защиты – средства защиты ресурса, на котором расположена (или обрабатывается) информация и средства защиты самой информации, т.е. применяемые к конкретному виду информации, а не ко всему ресурсу.
- Эффективность средства защиты – количественная характеристика средства защиты, определяющая степень его влияния на информационную систему, т.е. насколько

сильно средство влияет на защищенность информации и рабочего места группы пользователей. Определяется на основе экспертных оценок.

- Коэффициент локальной защищенности информации на ресурсе. Рассчитывается, если к информации осуществляется только локальный доступ. В этом случае клиентское место группы пользователей и ресурс, на котором хранится информация, совпадают; поэтому защищенность группы пользователей отдельно оценивать не нужно.
- Коэффициент удаленной защищенности информации на ресурсе. Рассчитывается, когда к информации осуществляется удаленный доступ; т.е. по сути это суммарный коэффициент средств защиты объекта.
- Коэффициент локальной защищенности рабочего места группы пользователей. Рассчитывается, когда группа пользователей осуществляет удаленный доступ к информации, т.е. это суммарный коэффициент защиты субъекта или клиентского места группы пользователей. Данный коэффициент невозможно определить для групп анонимных и авторизованных Интернет-пользователей.
- Наследование коэффициентов защищенности. 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. Механизм наследования будет подробно описан далее.
- Базовое время простоя ресурса (без применения средств защиты) – время, в течение которого доступ к информации ресурса невозможен (отказ в обслуживании). Определяется в часах в год на основе экспертных оценок без учета влияния на информацию средств защиты. Базовое время простоя зависит от групп пользователей, имеющих доступ к ресурсу: время простоя увеличивается, если к ресурсу имеют доступ Интернет-пользователи.
- Дополнительное время простоя ресурса – время простоя, в течение которого доступ к информации ресурса невозможен, обусловленное неадекватной работой программного или аппаратного обеспечения ресурса. Задается пользователем. Указывается в часах в год. (Исключение: время простоя не может задаваться для твердой копии).
- Сетевое устройство - устройство, с помощью которого осуществляется связь между ресурсами сети. Например, коммутатор, маршрутизатор, концентратор, модем, точка доступа.
- Время простоя сетевого устройства – время, в течение которого доступ, осуществляемый с помощью сетевого устройства, к информации ресурса невозможен из-за отказа в обслуживании сетевого устройства.
- Максимальное критичное время простоя (T_{max}) – значение времени простоя, которое является критичным для организации. Т.е. ущерб, нанесенный организации при простаивании ресурса в течение критичного времени простоя, максимальный. При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный организации, не увеличивается.

- Контрмера – действие, которое необходимо выполнить для закрытия уязвимости.
- Риск – вероятный ущерб, который понесет организация при реализации угроз информационной безопасности, зависящий от защищенности системы.
- Риск после задания контрмер – значение риска, пересчитанного с учетом задания контрмер (закрытия уязвимостей).
- Эффективность комплекса контрмер – оценка, насколько снизился уровень риска после задания комплекса контрмер по отношению к первоначальному уровню риска.

Принцип работы алгоритма

Итак, пройдя первый этап (описание необходимых для модели данных), перейдем непосредственно к работе алгоритма модели.

Риск оценивается отдельно по каждой связке «группа пользователей – информация», т.е. модель рассматривает взаимосвязь «субъект – объект», учитывая все их характеристики.

Риск реализации угрозы информационной безопасности для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Владелец информации задает ущерб отдельно по трем угрозам; это проще и понятнее, т.к. оценить ущерб в целом не всегда возможно.

Рассмотрим принцип работы модели последовательно для одной связи «информация – группа пользователей» (для остальных считаем аналогично).

Расчет рисков по угрозам конфиденциальность и целостность

Расчет рисков для угроз конфиденциальность и целостность¹:

1. Определяем вид доступа группы пользователей к информации. От этого будет зависеть количество средств защиты, т.к. для локального и удаленного доступа применяются разные средства защиты.
2. Определяем права доступа группы пользователей к информации. Это важно для целостности, т.к. при доступе «только чтение» целостность информации нарушить нельзя, и для доступности. Определенные права доступа влияют на средства защиты информации.
3. Вероятность реализации угрозы зависит от класса группы пользователей. Например, анонимные Интернет-пользователи представляют наибольшую угрозу для ценной информации компании, значит, если данная группа имеет доступ к информации, риск реализации угрозы увеличивается. Также, в зависимости от класса группы пользователей меняются их средства защиты. Например, для авторизованных и анонимных Интернет-пользователей мы не можем определить средства защиты их рабочего места.
4. Особым видом средства защиты является антивирусное программное обеспечение. В условиях современного функционирования компьютерных систем хранения и обработки информации вредоносное программное обеспечение представляет собой наиболее опасную и разрушительную угрозу. Зная силу влияния вирусных программ,

¹ Алгоритмы расчета для угроз целостности и конфиденциальности похожи, поэтому здесь мы их объединили.

отсутствие антивирусного программного обеспечения на ресурсе (или клиентском месте пользователя) необходимо принимать во внимание отдельно. Если на ресурсе не установлен антивирус, то вероятность реализации угроз конфиденциальности, целостности и доступности резко возрастает. Данная модель это учитывает.

5. Теперь у нас есть все необходимые знания, чтобы определить средства защиты информации и рабочего места группы пользователей. Просуммировав веса средств защиты, получим суммарный коэффициент. Для угрозы целостность учитываются специфические средства защиты – средства резервирования и контроля целостности информации. Если к ресурсу осуществляется локальный и удаленный доступ, то на данном этапе будут определены три коэффициента: коэффициент локальной защищенности информации на ресурсе, коэффициент удаленной защищенности информации на ресурсе и коэффициент локальной защищенности рабочего места группы пользователей. Из полученных коэффициентов выбираем минимальный. Чем меньше коэффициент защищенности, тем слабее защита, т.е. важно учесть наименее защищенное (наиболее уязвимое) место в информационной системе.
6. На этом этапе вступает в силу понятие наследования коэффициентов защищенности и базовых вероятностей. Например, на ресурсе, входящем в сетевую группу, содержится информация, к которой осуществляется доступ групп пользователей (анонимных, авторизованных или мобильных) из Интернет. Для этой связи «информация – группа Интернет-пользователей» рассчитывается только коэффициент удаленной защищенности информации на ресурсе, т.к. оценить защищенность групп пользователей мы не можем². Теперь этот коэффициент защищенности необходимо сравнить с коэффициентами защищенности, полученными для нашей связи «информация – группа пользователей». Это очень важный момент. Таким образом, мы учитываем влияние других ресурсов системы на наш ресурс и информацию. 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. Явным преимуществом данной модели является то, что она учитывает взаимосвязи между ресурсами информационной системы.
7. Отдельно учитывается наличие криптографической защиты данных при удаленном доступе. Если пользователи могут получить удаленный доступ к ценным данным, не используя систему шифрования, это может сильно повлиять на целостность и конфиденциальность данных.
8. На последнем этапе перед получением итогового коэффициента защищенности связи «информация – группа пользователей» анализируем количество человек в группе пользователей и наличие у группы пользователей выхода в Интернет. Все эти параметры сказываются на защищенности информации.
9. Итак, пройдя по всему алгоритму, мы получили конечный, итоговый коэффициент защищенности для нашей связки «информация – группа пользователей».
10. Далее полученный итоговый коэффициент нужно умножить на базовую вероятность реализации угрозы информационной безопасности. Базовая вероятность определяется на основе метода экспертных оценок. Группа экспертов, исходя из классов групп

² Для группы мобильных Интернет-пользователей коэффициент удаленной защиты группы пользователей рассчитывается.

пользователей, получающих доступ к ресурсу, видов и прав их доступа к информации, рассчитывает базовую вероятность для каждой информации. Владелец информационной системы, при желании, может задать этот параметр самостоятельно. Перемножив базовую вероятность и итоговый коэффициент защищенности, получим итоговую вероятность реализации угрозы. Напомним, что для каждой из трех угроз информационной безопасности мы отдельно рассчитываем вероятность реализации.

11. На завершающем этапе значение полученной итоговой вероятности накладываем на ущерб от реализации угрозы и получаем риск угрозы информационной безопасности для связи «вид информации – группа пользователей».
12. Чтобы получить риск для вида информации (с учетом всех групп пользователей, имеющих к ней доступ), необходимо сначала просуммировать итоговые вероятности реализации угрозы по следующей формуле:

$$P_{inf} = 1 - \prod_{i=1}^n (1 - P_{ug,n}).$$

А затем полученную итоговую вероятность для информации умножаем на ущерб от реализации угрозы, получая, таким образом, риск от реализации угрозы для данной информации.

13. Чтобы получить риск для ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

Расчет рисков по угрозе отказ в обслуживании

Если для целостности и конфиденциальности вероятность реализации угрозы рассчитывается в процентах, то для доступности аналогом вероятности является время простоя ресурса, содержащего информацию. Однако, риск по угрозе отказ в обслуживании все равно считается для связки «информация - группа пользователей», т.к. существует ряд параметров, которые влияют не на ресурс в целом, а на отдельный вид информации.

Итак:

1. На первом этапе определяем базовое время простоя для информации.
2. Далее необходимо рассчитать коэффициент защищенности связки «информация - группы пользователя». Для угрозы отказ в обслуживании коэффициент защищенности определяется, учитывая права доступа группы пользователей к информации и средства резервирования.
3. Так же, как для угроз нарушения конфиденциальности и доступности, наличие антивирусного программного обеспечения является особым средством защиты и учитывается отдельно.
4. Накладывая коэффициент защищенности на время простоя информации, получим время простоя информации, учитывая средства защиты информации. Оно рассчитывается в часах простоя в год.
5. Специфичный параметр для связки «информация – группа пользователей» - время простоя сетевого оборудования. Доступ к ресурсу может осуществляться разными группами пользователей, используя разное сетевое оборудование. Для сетевого

оборудования время простоя задает владелец информационной системы. Время простоя сетевого оборудования суммируется со временем простоя информации, полученным в результате работы алгоритма, таким образом, мы получаем итоговое время простоя для связи «информация – группа пользователей».

6. Значение времени простоя для информации (T_{inf}), учитывая все группы пользователей, имеющих к ней доступ, вычисляется по следующей формуле:

$$T_{inf} = (1 - \prod_{i=1}^n (1 - \frac{T_{ug,n}}{T_{max}})) \times T_{max}$$

где T_{max} – максимальное критичное время простоя;

$T_{ug,n}$ – время простоя для связи «информация – группа пользователя».

7. Ущерб для угрозы отказ в обслуживании задается в час. Перемножив итоговое время простоя и ущерб от реализации угрозы, получим риск реализации угрозы отказ в обслуживании для связи «информация - группа пользователей».

Задание контрмер

В новой версии алгоритма пользователь имеет возможность задавать контрмеры. Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. Т.е. на выходе пользователь получает значение двух рисков – риска без учета контрмеры (R_{old}) и риск с учетом заданной контрмеры (R_{new}) (или с учетом того, что уязвимость закрыта).

Эффективность введения контрмеры рассчитывается по следующей формуле (E):

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

В результате работы алгоритма пользователь системы получает следующие данные:

- Риск реализации по трем базовым угрозам для вида информации;
- Риск реализации по трем базовым угрозам для ресурса;
- Риск реализации суммарно по всем угрозам для ресурса;
- Риск реализации по трем базовым угрозам для информационной системы;
- Риск реализации по всем угрозам для информационной системы;
- Риск реализации по всем угрозам для информационной системы после задания контрмер;
- Эффективность контрмеры;
- Эффективность комплекса контрмер.

Пример расчета риска информационной безопасности на основе модели информационных потоков

1. Входные данные:

Например, информационная система Компании состоит из двух ресурсов: сервера³ и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связаны 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. При чем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Средства защиты:

1. Средства защиты сервера:

Средство защиты	Вес 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 дисководов и USB портов	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

1.1. Средства защиты первой информации (бухгалтерский отчет):

Средство защиты	Вес средства защиты
Средства локальной защиты	

³ При этом, сервером в данном примере будем считать компьютер, на котором несколько папок открыты для удаленного доступа.

Средства криптографической защиты (криптозащита данных на ПК)	20
Средства резервирования и контроля целостности	
Резервное копирование	10
Программная система контроля целостности	10

1.2. Средства защиты второй информации (база клиентов Компании):

Средств защиты информации нет.

2. Средства защиты рабочей станции:

Средство защиты	Вес 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 дисководов и USB портов	10
Средства персональной сетевой защиты	
Персональный межсетевой экран	3
Система криптозащиты электронной почты	10

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

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

3. Средства защиты клиентского места группы пользователей:

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

Средство защиты	Вес 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 дисководов и USB портов	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	Вес средства защиты
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	10

замком, видео наблюдение)	
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	10
Отсутствие дисководов и USB портов	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, удаление	нет	1
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 ⁴

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 у.е.	100 у.е.	1 у.е.

⁴ Доступ в Интернет групп пользователей, осуществляющих доступ к информации через Интернет, по понятным причинам не анализируется.

Бухгалтер / база клиентов Компании	100 у.е.	100 у.е.	1 у.е.
Финансовый директор / база клиентов Компании	100 у.е.	100 у.е.	1 у.е.
Бухгалтер / база данных наименований товаров Компании	100 у.е.	100 у.е.	1 у.е.

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

1. Коэффициенты защищенности:

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

При удаленном доступе рассчитываем *коэффициенты локальной защищенности рабочего места группы пользователей, имеющей доступ к информации*, (сумма весов средств физической, локальной и персональной сетевой защиты) и *удаленной защищенности информации на ресурсе* (сумма весов 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 вес VPN шлюза (20). Если при удаленном доступе VPN-соединение не используется для групп Интернет-пользователи итоговый коэффициент защищенности умножается на 4, для групп обычных пользователей (не Интернет-пользователей) – остается неизменным.

	Наименьший коэффициент	Вес VPN-соединения	Результирующий коэффициент
Главный бухгалтер / бухгалтерский отчет	55	-	55
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

Если к информации имеет доступ группа пользователей, превышающая 50 человек, то это соответственно увеличивает итоговый коэффициент.

Если группа пользователей имеет доступ в Интернет, то это увеличивает итоговый коэффициент в 2 раза.

Пример расчета итогового коэффициента: $K = \frac{1 \cdot 2}{55} = 0,036$

4. Итоговая вероятность:

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

	Базовая вероятность	Итоговая базовая вероятность	Итоговый коэффициент	Промежуточная вероятность	Итоговая вероятность
Главный бухгалтер / бухгалтерский отчет	0,35	0,7	0,036	0,0252	0,0252
Бухгалтер / база клиентов Компании	0,7	0,7	0,024	0,0168	0,0331
Финансовый директор / база клиентов Компании	0,35	0,7	0,024	0,0168	
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: $P_{inf} = 1 - \prod_{i=1}^n (1 - P_{ug,n})$

5. 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. Первый пункт вычисляется аналогично расчету по угрозе конфиденциальность.

2. Учет средств резервирования и контроля целостности

	Наименьший коэффициент	Вес VPN-соединения	Вес средств резервирования и контроля целостности	Результирующий коэффициент
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

Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то вес 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.

4. 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	0,05619
Финансовый директор / база клиентов Компании	0,7	0,7	0,065	0,0455	
Бухгалтер / база данных наименований товаров Компании	0,25	0,7	0,02	0,014	0,014

5. 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	5	Const

				в 4 раз		
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	70	70	-	2	140	280
Финансовый директор / база клиентов Компании	40	70	10	4	280	
Бухгалтер / база данных наименований товаров	40	40	-	0,25	10	10

Компании						
----------	--	--	--	--	--	--

При расчете рисков по угрозе доступность базовые времена простоя наследуются только в пределах ресурса.

Время простоя сетевого оборудования добавляется к итоговому времени простоя.

Если итоговое время простоя превышает максимально критичное (280 часов в год по базовым настройкам), оно приравнивается к максимально критичному времени простоя.

Для второй информации на сервере, к которой имеют доступ несколько групп пользователей,

итоговое время простоя рассчитывается по следующей формуле: $T_{\text{inf}} = (1 - \prod_{i=1}^n (1 - \frac{T_{\text{ug},n}}{T_{\text{max}}})) \times T_{\text{max}}$.

3. 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. Определенные ответы на вопросы Политики безопасности влияют на веса средств защиты и изменяют риск реализации угроз информационной безопасности.

Разделы Политики безопасности:

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

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 – все веса средств защиты увеличиваются на 10%;

Нет – все веса средств защиты уменьшаются на 10%;

Положения политики внедрены частично – все веса средств защиты уменьшаются 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 – все веса средств защиты по угрозе Конфиденциальность по ресурсам, к которым имеют доступ группы Интернет-пользователей, уменьшаются на 5%

Нет – все веса средств защиты по угрозе Конфиденциальность по ресурсам, к которым имеют доступ группы Интернет-пользователей, увеличиваются 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 – все веса средств защиты уменьшаются на 50%. Все веса средств защиты ресурсов, к которым имеют доступ группы администраторов или офицеров безопасности, уменьшаются на 100%.

Нет – ничего не меняется.