**Тема 7: "МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ КОМПАНИИ DIGITAL SECURITY"**

***7.1 Метод оценки рисков на основе модели информационных потоков.***

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации.

Данная модель позволяет оценить защищенность каждого вида информации.

Алгоритм 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.

***7.2.Описание архитектуры ИС.***

Для того, чтобы построить модель ИС, необходимо проанализировать защищенность и архитектуру построения информационной системы.

Специалист по ИБ, привлекая владельца (менеджера) информационной системы (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 введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Целесообразно составить карту ИС на которой отобразить все указанные характеристики. Иными словами, необходимо:

1. Изобразить ИС в виде структурной схемы, на которой отобразить:

1) все ресурсы (сервер, РС и т.д.);

2) отделы, к которым относятся ресурсы;

3) сетевые группы (локальные сети), физические связи ресурсов между собой и их подключения к Интернет;

4) виды ценной информации, хранящейся на ресурсах;

5) пользователей (группы пользователей), имеющих доступ к ценной (конфиденциальной) информации.

***Рис. 5 ИС в виде структурной схемы***

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

|  |  |
| --- | --- |
| Средства защиты сервера | Вес |
| 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 |

|  |  |
| --- | --- |
| Средства защиты информации (информация №1) | Вес |
| Средства локальной защиты  |
| Средства криптографической защиты (криптозащита данных на ПК)  | 20 |
| Средства резервирования и контроля целостности  |
| Резервное копирование  | 10 |
| Программная система контроля целостности  | 10 |

|  |  |
| --- | --- |
| Средства защиты рабочей станции | Вес |
| Средство физической защиты |
| Контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение)  | 10 |
| Средства локальной защиты  |
| Средства антивирусной защиты (антивирусный монитор) | 10 |
| Отсутствие дисководов и USB портов | 10 |
| Средства персональной сетевой защиты |
| Наличие персонального межсетевого экрана | 3 |
| Система криптозащиты электронной почты | 10 |

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:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Информационный поток | Вид доступа | Права доступа | Наличие VPN-соединения | Количество человек в группе |
| (Наименование) | (Локальный, удаленный) | (Чтение, запись, удаление) | (Да, нет) | (1,2,.n) |

4. Указать наличие у пользователей выхода в Интернет

|  |  |
| --- | --- |
| Пользователь (группа пользователей.) | Доступ в Интернет |
| Доступ в Интернет (Наименование)  | (Есть, нет, не анализируется) |

5. Указать ущерб компании от реализации угроз ИБ для каждого информационного потока:

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

Ущерб определяется с участием владельца ИС, либо им самим непосредственно.

*На этом описание архитектуры ИС завершается.*

Далее производится расчет рисков **для каждого вида ценной информации хранящейся в ИС по** угрозе «нарушение конфиденциальности».

***7.3 Расчет рисков по угрозе конфиденциальность***

**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*:

средства физической защиты: (охрана, замок, пропускной режим в помещение) (25);

средства локальной защиты:

отсутствие дисководов и USB портов (10);

криптозащита данных на ПК (20).

*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.

Эти средства (межсетевой экран, серверная антивирусная защита) находятся **на сервере**.

*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.

Средства физической защиты – те же.

Средства локальной защиты: антивирус, отсутствие дисководов и USB-портов.

Средства персональной сетевой защиты: межсетевой экран (брандмауэр), средства криптозащиты электронной почты.

Эти средства (персональный межсетевой экран брандмауэр, средства криптозащиты электронной почты) находятся на рабочей станции (на компьютере, подключенном к локальной сети).

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Информационный поток | *Коэффициент локальной защищенности информации* | *Коэффициент удаленной защищенности информации* | *Коэффициент локальной защищенности рабочего места* | *Наименьший коэффициент* |
| (Наименование)  | (Ф+Л)  | (СКСЗ)  | (Ф+Л+ПСЗ)  | (НК) min |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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

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

При удаленном доступе через VPN к наименьшему коэффициенту защищенности потока прибавляется вес VPN шлюза (20). Это сетевое устройство повышает защищенность информации.

При этом от наименьшего коэффициента переходят к результирующему: **РК=НК+20 (или +0)**

|  |  |  |  |
| --- | --- | --- | --- |
| Информационный поток | Наименьший коэффициент | Вес VPN соединения | Результирующий коэффициент |
| (Наименование)  | (НК) | (20 либо 0)  | (РК) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**3.** Далее от результирующего коэффициента (РК) переходят к **итоговому коэффициенту (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 ИК увеличивается в 2 раза: **ИК=2 N/РК.**

Если при удаленном доступе 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=(4 N)/РК**

Результаты расчетов сводятся в таблицу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Информационный поток | Результирующий коэффициент | Количество человек в гр. | Наличие Интернет | Итоговый коэффициент |
| Главный бухгалтер - бухгалтерский отчет | (РК)  | (N) | I=2,1 | ИК=(N I )/РК |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**4. Расчет итоговой вероятности (ИВ).**

Чтобы получить **ИВ**, необходимо сначала определить **базовую вероятность (БВ)** реализации угрозы нарушения конфиденциальности и умножить ее на **ИК**: **ИВ=БВ 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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Информационный поток | Базовая вероятность (БВ) | Итоговая базовая вероятность (ИБВ) | Итоговый коэффициент (ИК) | Промежуточная вероятность (ПВ) | Итоговая вероятность (ИВ) |
| Главный бухгалтер – бухгалтерский отчет | 0,2 | 0,5 | 0,036 | 0,018 | 0,018 |
| Бухгалтер – база клиентов Компании | 0,2 | 0,5 | 0,024 | 0,012 | 0,024 |
| Финансовый директор – база клиентов Компании | 0,5 | 0,5 | 0,024 | 0,012 |
| Бухгалтер – база данных наименований товаров Компании | 0,2 | 0,5 | 0,033 | 0,0165 | 0,0165 |

Итоговая базовая вероятность (**ИБВ**) одинакова для всех потоков, поскольку к информации «база клиентов Компании» имеется доступ через Интернет (Финансовый директор имеет права «запись, чтение»). Базовая вероятность реализации угрозы конфиденциальности для потока «Финансовый директор – база клиентов Компании» самая большая (0,7) и она распространяется на все информации, хранящиеся на всех ресурсах, входящих в локальную сеть (сетевую группу).

Это так называемое **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. 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.

Промежуточная вероятность (**ПВ**) вычисляется, как: **ПВ=ИБВ ИК**.

 Итоговая вероятность **ИВ1=ПВ1; ИВ3=ПВ3.**

Итоговая вероятность **ИВ2=1-(1-ПВ21) (1-ПВ22**), как суммарная по двум группам пользователей.

**5 .Расчет риска по угрозе конфиденциальность для каждой информации (1,2,3)**

Риск по угрозе конфиденциальность для каждой информации (1-бух. отчет, 2-база клиентов, 3-база наименований товаров) рассчитывается, как произведение итоговой вероятности на ущерб:

**R1=ИВ1\*D1=0,018\*100=1,8;**

**R2=ИВ2\*D2=0,024\*100=2,4;**

**R3=ИВ3\*D3=0,0165\*100=1,65.**

где У – ущерб от реализации угрозы.

**6.Расчет риска по угрозе конфиденциальность для ресурса**.

Риск для ресурса, на котором хранится несколько видов информаций (несколько БД) равен сумме рисков по всем видам информации.

**Расчет рисков по угрозе целостность**

**1. Расчет коэффициентов защищенности**.

Выполняется аналогично расчету по угрозе конфиденциальность. Фактически берутся наименьшие коэффициенты НК из предыдущего расчета.

**2. Учет средств резервирования и контроля целостности.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Информационный поток** | **Наименьший коэффициент (НК) т (РК)** | **Вес VPN-соединения**  | **Веса средств резервирования и контроля целостности**  | **Результирующий коэффициент** |
| Главный бухгалтер – бухгалтерский отчет | 55- |  | 40АСКЦ-20 РК-10 ЦП-10 | 9555+40 |
| Бухгалтер – база клиентов Компании | 22 | 20 | 20РК-10 ЦП-10 | 6222+20+20 |
| Финансовый директор – база клиентов Компании | 22 | 20 | 20АСКЦ-20 | 6222+20+20 |
| Бухгалтер – база данных наименований товаров Компании | 30 | - | 20РК-10ЦП-10 | 5030+20 |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Информационный поток** | **Результирующий коэффициент (РК)** | **Наличие резервного копирования** | **Кол-во человек в группе** | **Наличие у группы доступа в Интернет** | **Итоговый коэффициент** |
| Главный бухгалтер – бухгалтерский отчет | 95 | 1 | 1 | 2 | 0,021(1/95)\*2 |
| Бухгалтер – база клиентов Компании | 62 | 1 | 1 | 1 | 0,0161/62 |
| Финансовый директор – база клиентов Компании | 62 | 4 | 1 | - | 0,063(1/62)\*4 |
| Бухгалтер – база данных наименований товаров Компании | 50 | 1 | 1 | 1 | 0,021/50 |

Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то вес резервного копирования (10) прибавляется к коэффициенту защищенности (п.2). Если резервное копирование не осуществляется, и в группе пользователей, имеющей доступ к информации, разрешены запись или удаление, то итоговый коэффициент увеличивается в 4 раза.

**4. Расчет итоговой вероятности.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Информационный поток | Базовая вероятность (БВ) | Итоговая базовая вероятность (ИБВ) | Итоговый коэффициент (ИК) | Промежуточная вероятность | **Итоговая вероятность** |
| Главный бухгалтер – бухгалтерский отчет | 0,25 | 0,7 | 0,021 | 0,01470,7\*0,021 | **0,0147** |
| Бухгалтер – база клиентов Компании | 0,1 | 0,7 | 0,016 | 0,01120,7\*0,016 | **0,05619** |
| Финансовый директор – база клиентов Компании | 0,7 | 0,7 | 0,065 | 0,04550,7\*0,065 |
| Бухгалтер – база данных наименований товаров Компании | 0,25 | 0,7 | 0,02 | 0,0140,7\*0,02 | **0,014** |

Базовая вероятность определяется на основе метода экспертных оценок. Ее значения по данной угрозе **целостность** отличаются от значений в расчете по угрозе **конфиденциальность**. Группа экспертов, исходя из классов групп 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.

Итоговая базовая вероятность. Базовая вероятность реализации угрозы конфиденциальности для потока «Финансовый директор - база клиентов Компании» самая большая (0,7) и она распространяется на все информации, хранящиеся на всех ресурсах, входящих в локальную сеть (сетевую группу).

Перемножив итоговую 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.

Итоговая вероятность по второй информации:

**ИВ2=1-(1-ПВ21)\*(1-ПВ22)**, как суммарная по двум группам пользователей.

**6. Расчет риска по угрозе целостность**.

На завершающем этапе значение полученной итоговой вероятности умножаем на ущерб от реализации угрозы и получаем риск угрозы информационной безопасности для связи <вид информации - группа пользователей>.

**R1=ИВ1\*D1=0,0147\*100=1,47;**

**R2=ИВ2\*D2=0,05619\*100=5,61;**

**R3=ИВ3\*D3=0,014\*100=1,4.**

* 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:



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

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