**Тема 6: "МЕТОДИКА ОЦЕНКИ РИСКОВ   
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ"**

***6.1 Управление рисками. Основные понятия.***

При внедрении системы управления информационной безопасностью (СУИБ) в организации одной из основных точек преткновения обычно становится система управления рисками.

Система управления рисками (СУР) является главным, базовым элементом СУИБ.

СУР позволяет получить ответ на главный вопрос:

*На каком направлении информационной безопасности требуется сосредоточить внимание?*

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, которые работают с большими объемами ценной информации или если компания обрабатывает или хранит ценную информацию своих клиентов (банк).

Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков.

Использование информационных систем связано с риском. (Если ИС не использовать вообще, то риск будет связан с другими факторами).

Говоря о рисках для бизнеса, мы имеем в виду возможность с определенной вероятностью понести определенный ущерб. Это может быть как прямой материальный ущерб, так и косвенный ущерб, выражающийся, например, в упущенной выгоде, вплоть до выхода из бизнеса, ведь, если риском не управлять, то бизнес можно потерять.

**Если возможный ущерб неприемлемо велик**, необходимо принять экономически оправданные меры защиты. Периодическая переоценка рисков необходима для контроля эффективности защитных мер и для учета изменений обстановки.

С количественной точки зрения уровень риска является произведением вероятности реализации определенной угрозы (использующей некоторые уязвимые места), на величину возможного ущерба: **R=Р(V) D**.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми).

*Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически*:

- оценка и переоценка (измерение) рисков;

- выбор эффективных и экономически оправданных защитных мер и средств для уменьшения или нейтрализации рисков.

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.

2. Выбор методики оценки рисков.

З. Инвентаризация активов.

4. Анализ угроз и их последствий, выявление уязвимых мест в защите.

5. Оценка рисков.

6. Обработка рисков.

7. Выбор защитных мер.

8. Реализация и проверка выбранных мер.

9. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую работу.

На сегодняшний день существует **две** основные методики оценки рисков информационной безопасности: метод оценки рисков, основанный на построении **модели угроз** и **уязвимостей** и метод оценки рисков, основанный на построении **модели информационных потоков**.

Разработка методики оценки риска – достаточно трудоемкая задача. Во-первых, такая методика должна **всесторонне описывать информационную систему, ее ресурсы, ее угрозы и уязвимости.** Задача заключается в том, чтобы построить максимально гибкую модель информационной системы, которую можно было бы настраивать в соответствии с реальной системой. Во-вторых, методика оценки рисков должна быть предельно прозрачна, чтобы владелец информации, использующий ее, мог адекватно оценить ее эффективность и применимость к своей конкретной системе.

Остановимся подробнее на методах оценки информационного риска.

***6.2 Метод оценки рисков на основе модели угроз и уязвимостей.***

Для того, чтобы оценить риск информации, анализируются все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз.

Исходя из введенных владельцем информационной системы данных, строится модель угроз и уязвимостей, актуальных для информационной системы компании.

На основе полученной модели проводится анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитываются риски.

**Основные понятия и допущения модели**

*Базовые угрозы информационной безопасности* – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании.

*Ресурс* – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

*Угроза –* действие, которое потенциально может привести к нарушению безопасности.

Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

*Уязвимость* – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

*Критичность ресурса* (**D**) – ущерб, который понесет компания от потери ресурса. Задается в уровнях (количество уровней может быть в диапазоне от 2 до 100) или в деньгах. В зависимости от выбранного режима работы, может состоять из критичности ресурса по конфиденциальности, целостности и доступности (Dс, Di, Da).

*Критичность реализации угрозы* (**ER**) – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности (ERc, ERi, ERa).

*Вероятность реализации угрозы через данную уязвимость в течение года* (**P(V)**) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

*Максимальное критичное время простоя* (**Tmax**) – 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.

**Принцип работы алгоритма**

Исходные данные:

- Ресурсы;

- Критичность ресурса;

- Отделы, к которым относятся ресурсы;

- Угрозы, действующие на ресурсы;

- Уязвимости, через которые реализуются угрозы;

- Вероятность реализации угрозы через данную уязвимость;

- Критичность реализации угрозы через данную уязвимость.

С точки зрения базовых угроз информационной безопасности существует два режима работы алгоритма:

- Одна базовая угроза (суммарная);

- Три базовые угрозы.

**Расчет рисков по угрозе информационной безопасности**

1. На первом этапе рассчитывается *уровень угрозы по уязвимости* **Th** на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации



где ERc,I,a – критичность реализации угрозы (указывается в %);

P(V)c,I,a – вероятность реализации угрозы через данную уязвимость (указывается в %).

Вычисляется одно или три значения в зависимости от количества базовых угроз. Получается значение уровня угрозы по уязвимости в интервале от 0 до 1.

2. Для расчета уровня угрозы по всем уязвимостям **CTh**, через которые возможна реализация данной угрозы на ресурсе, суммируются полученные уровни угроз через конкретные уязвимости по следующей формуле:

Для режима с одной базовой угрозой:



Для режима с тремя базовыми угрозами:







Значения *уровня угрозы по всем уязвимостям* получаются в интервале от 0 до 1.

3. Аналогично рассчитывается *общий уровень* угроз по ресурсу **CThR** (учитывая все угрозы, действующие на ресурс):

Для режима с одной базовой угрозой:



Для режима с тремя базовыми угрозами:







Значение *общего уровня угрозы* получается в интервале от 0 до 1.

4. *Риск по ресурсу* R рассчитывается следующим образом:

Для режима с одной базовой угрозой:



где D критичность ресурса. Задается в деньгах или уровнях.

В случае угрозы доступность (отказ в обслуживании) критичность ресурса в год вычисляется по следующей формуле:



*Для* *остальных угроз критичность ресурса задается в год.*

Для режима с тремя базовыми угрозами:









Da,c,i – критичность ресурса по трем угрозам. Задается в деньгах или уровнях.

R – суммарный риск по трем угрозам.

Таким образом, получается значение *риска по ресурсу* в уровнях (заданных пользователем) или деньгах.

5. Риск по информационной системе **CR** рассчитывается по формуле:

Для режима с одной базовой угрозой:

- для режима работы в деньгах:



- для режима работы в уровнях:



Для режима работы с тремя угрозами:

- для режима работы в деньгах:





CRa,c,i – риск по системе по каждому виду угроз

CR - риск по системе суммарно по трем видам угроз

- для режима работы в уровнях:





**Задание контрмер**

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 (**Rold**) и риск с учетом заданной контрмеры (**Rnew**) (или с учетом того, что уязвимость закрыта).

Эффективность введения контрмеры рассчитывается по следующей формуле (**E**):



В результате работы алгоритма пользователь системы получает следующие данные:

- Риск по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;

- Риск суммарно по всем угрозам для ресурса;

- Риск по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;

- Риск по всем угрозам для информационной системы;

- Риск по всем угрозам для информационной системы после задания контрмер;

- Эффективность контрмеры;

-Эффективность комплекса контрмер.

***Пример расчета риска информационной безопасности на основе модели угроз и уязвимостей***

(Расчет рисков приведен только для одной угрозы информационной безопасности, т.к. для остальных угроз риск рассчитывается аналогично).

1. Угрозы и уязвимости

| **Ресурс** | **Угрозы** | **Уязвимости** |
| --- | --- | --- |
| Сервер (критичность ресурса 100 у.е.) | Угроза 1 Неавторизованное проникновение нарушителя внутрь охраняемого периметра (одного из периметров) | Уязвимость 1 Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию |
| Уязвимость 2 Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты) |
| Угроза 2 Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе | Уязвимость 1 Отсутствие авторизации для внесения изменений в систему электронной Почты доверенными сотрудниками |
| Уязвимость 2 Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции |
| Угроза 3 Разглашение конфиденциальной информации сотрудниками компании 1.1 Вероятность реализации | Уязвимость 1 Отсутствие соглашений о конфиденциальности |
| Уязвимость 2 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими |

1. Вероятность реализации

|  |  |  |
| --- | --- | --- |
| Угроза/Уязвимость | Вероятность реализации угрозы через данную уязвимость в течение года (%), P()V) | Критичность реализации угрозы через уязвимость (%), ER |
| Угроза 1/Уязвимость 1 | 50 | 60 |
| Угроза 1/Уязвимость 2 | 20 | 60 |
| Угроза 2/Уязвимость 1 | 60 | 40 |
| Угроза 2/Уязвимость 2 | 10 | 40 |
| Угроза 3/Уязвимость 1 | 10 | 80 |
| Угроза 3/Уязвимость 2 | 80 | 80 |

2. Уровень угрозы

|  |  |  |
| --- | --- | --- |
| Угроза/Уязвимость | Уровень угрозы (%), Th | Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh |
| Угроза 1/Уязвимость 1 | 0,3 | 0,384 |
| Угроза 1/Уязвимость 2 | 0,12 |
| Угроза 2/Уязвимость 1 | 0,24 | 0,270 |
| Угроза 2/Уязвимость 2 | 0,04 |
| Угроза 3/Уязвимость 1 | 0,08 | 0,669 |
| Угроза 3/Уязвимость 2 | 0,64 |

3. Общий уровень угроз, действующих на ресурс

|  |  |  |
| --- | --- | --- |
| Угроза/Уязвимость | Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh | Общий уровень угроз по ресурсу(%), CThR |
| Угроза 1/Уязвимость 1 | 0,384 | 0,8511 |
| Угроза 1/Уязвимость 2 |
| Угроза 2/Уязвимость 1 | 0,270 |
| Угроза 2/Уязвимость 2 |
| Угроза 3/Уязвимость 1 | 0,669 |
| Угроза 3/Уязвимость 2 |

4. Риск ресурса

Критичность ресурса (ущерб, который понесет Компания от потери ресурса) – 100 у.е.

Для угрозы доступность, критичность ресурса задается в час (а не в год, как для остальных угроз).Поэтому, чтобы получить критичность ресурса в год, необходимо умножить критичность ресурса в час на максимально критичное время простоя ресурса за год.

|  |  |  |
| --- | --- | --- |
| Угроза/Уязвимость | Общий уровень угроз по ресурсу(%), CThR | Риск ресурса (у.е.), R |
| Угроза 1/Уязвимость 1 | 0,8511 | 85,11 |
| Угроза 1/Уязвимость 2 |
| Угроза 2/Уязвимость 1 |
| Угроза 2/Уязвимость 2 |
| Угроза 3/Уязвимость 1 |
| Угроза 3/Уязвимость 2 |