МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУГРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ им. проф. М.А. БОНЧ-БРУЕВИЧА»

Факультет Информационных систем и технологий
Кафедра Информационных управляющих систем

РАБОТА
ЗАЩИЩЕНА С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

проф., д.т.н.		Н.Н. Мошак
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ПРАКТИЧЕСКАЯ РАБОТА № 1

«Оценка риска информационной безопасности корпоративной информационной системы на основе модели угроз и уязвимостей»

по курсу: Защищенные информационные системы

РАБОТУ ВЫПОЛНИЛ(А)
СТУДЕНТ(КА) ГР. _____ _____ _____
подпись, дата инициалы, фамилия

Санкт-Петербург 2017

Цель работы: рассчитать риск информационной безопасности корпоративной информационной системы на основе модели угроз и уязвимостей

Исходные данные:

- ресурсы (сервер закрытого контура, сервер открытого контура, МЭ открытого контура, СКЗИ закрытого контура, однонаправленный шлюз, оборудование ЛВС закрытого контура, оборудование ЛВС открытого контура);
- критичность ресурса (задать самостоятельно);
- отделы, к которым относятся ресурсы (закрытого и открытого контура);
- угрозы, действующие на ресурсы (сформулировать самостоятельно с учетом лекционного материала);
- уязвимости, через которые реализуются угрозы (сформулировать самостоятельно с учетом лекционного материала);
- задать вероятность реализации угрозы через данную уязвимость (на основе полученной модели проводится анализ вероятности реализации угроз информационной безопасности на каждый ресурс);
- критичность реализации угрозы через данную уязвимость (задать самостоятельно).

ЗАДАНИЕ

-описать угрозы/уязвимости (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);
- рассчитать уровень угрозы;
- рассчитать общий уровень угроз, действующий на ресурс;
- рассчитать риск ресурса
- сформулировать выводы.

1. Постановка задачи

Анализ информационных рисков позволяет эффективно управлять информационной безопасностью автоматизированной системой обработки информации (АСОИ) или корпоративной информационной системой (КИС) предприятия (организации). Для этого в начале работ по анализу рисков необходимо определить, что именно подлежит защите на предприятии и воздействию каких угроз оно подвержено, а затем выработать рекомендации по практике защиты. Такой анализ производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Анализ риска можно проводить согласно методике по сценарию, представленному на рис. 1. Каждый из шести этапов анализа риска должен быть конкретизирован.

На первом и втором этапах выявляются сведения, составляющие для предприятия коммерческую тайну, которые предстоит защищать.

Понятно, что такие сведения хранятся в установленных местах и на конкретных носителях, передаются по каналам связи и обрабатываются в соответствии с принятым регламентом. При этом основным фактором в технологии обращения с информацией является архитектура КИС, от которой во многом зависит защищенность информационных ресурсов предприятия.

В связи с этим необходимо еще раз подчеркнуть, что степень информационной безопасности определяется не только (а может быть и не столько) средствами и способами защиты, но и особенностями построения КИС. И когда говорят о **КИС в**

защищенном исполнении, речь идет прежде всего о выборе такой архитектуры (топологии) системы обработки информации, расположения средств обработки конфиденциальной информации и способов ее хранения и передачи, которые существенно уменьшат число возможных точек доступа к информации.

Третий этап анализа риска - построение схем каналов доступа, утечки или воздействия на информационные ресурсы основных узлов КИС.

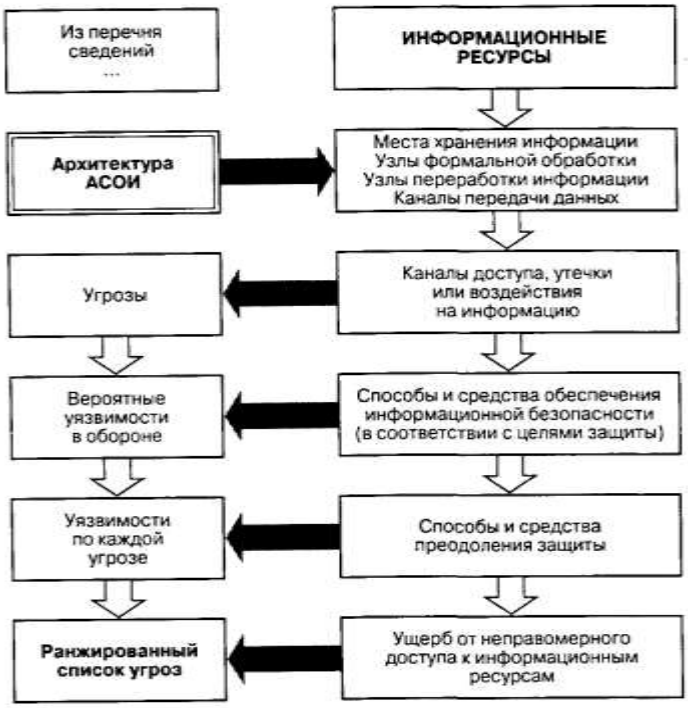

Рис.1 - Сценарий анализа информационных рисков компании

Каждый канал доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они представляют собой уязвимости и требуют применения средств недопущения нежелательных воздействий на информацию.

Анализ способов защиты всех возможных точек атак соответствует целям защиты, и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств (четвертый этап).

На пятом этапе исходя из известных на данный момент способов и средств преодоления оборонительных рубежей находятся вероятности реализации угроз по каждой из возможных точек атак.

На заключительном этапе производится оценка ущерба организации в случае реализации каждой из атак. Эти данные вместе с оценками уязвимости позволяют получить ранжированный список угроз информационным ресурсам.

Результаты работы представляются в виде, удобном для их восприятия и выработки решений о коррекции существующей системы защиты информации. При этом важно, что каждый информационный ресурс может быть подвержен воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

Величина информационного риска по каждому ресурсу - это произведение вероятности нападения на ресурс, вероятности реализации угрозы и ущерба от информационного вторжения. В данном произведении могут быть использованы различные способы взвешивания составляющих.

Объединение рисков по всем ресурсам дает общую величину риска при принятой

архитектуре КИС и внедренной в нее системы защиты информации.

Таким образом, варьируя варианты построения системы защиты информации и архитектуры КИС, можно (за счет изменения вероятности реализации угроз) представить и рассмотреть различные значения риска. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с заданным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение информационной безопасности к остаточному риску.

При построении систем обеспечения информационной безопасности так-же нужно определить **стратегию управления рисками** на предприятии.

На сегодня известно несколько подходов к управлению рисками. Один из наиболее распространенных - *уменьшение риска путем принятия комплексной системы контрмер*, включающей программно-технические и организационные меры защиты. Близким является подход, связанный *с уклонением от риска*. От некоторых классов рисков можно уклониться, например: вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Наконец, в ряде случаев допустимо принятие риска. В этой ситуации важно определиться со следующей дилеммой: что для предприятия выгоднее - бороться с рисками или же с их последствиями. Здесь приходится решать оптимизационную задачу.

После того как стратегия управления рисками выбрана, проводится окончательная оценка мероприятий по обеспечению информационной безопасности с подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение входят все материалы анализа рисков и рекомендации по их снижению.

Отметим, что выполнение анализа рисков и оценки потерь требует глубоких системных знаний и аналитического мышления во многих областях, смежных с проблемой защиты информации.

2. Методы оценивания информационных рисков

В настоящее время используются различные методы оценки информационных рисков отечественных компаний и управления ими. Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

1) идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса;
2) оценивание возможных угроз;
3) оценивание существующих уязвимостей;
4) оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы. При этом информационные риски компании зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности

компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть установлены как количественными методами (например, при нахождении стоимостных характеристик), так и качественными, скажем, с учетом штатных или чрезвычайно опасных нештатных воздействий внешней среды.

Возможность реализации угрозы для некоторого ресурса компании оценивается вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

- привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);
- возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);
- техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;
- степенью легкости, с которой уязвимость может быть использована.

3. 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 или в деньгах. В зависимости от выбранного режима работы, может состоять из критичности ресурса по конфиденциальности, целостности и доступности (Dc, 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.

4. Расчет рисков по угрозе информационной безопасности

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

$$\mathrm{Th}_{c,I,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где $\mathrm{ER}_{c,I,a}$ – *критичность реализации угрозы* (указывается в %);

$\mathrm{P(V)}_{c,I,a}$ – *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.

4.2. 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:

$$\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$$

Для режима с тремя базовыми угрозами:

$$\mathrm{CTh_c} = 1 - \prod_{i=1}^{n} (1 - Th_c)$$

$$\mathrm{CTh_i} = 1 - \prod_{i=1}^{n} (1 - Th_i)$$

$$\mathrm{CTh_a} = 1 - \prod_{i=1}^{n} (1 - Th_a)$$

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

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

Для режима с одной базовой угрозой:

$$\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh)$$

Для режима с тремя базовыми угрозами:

$$\mathrm{CThR_c} = 1 - \prod_{i=1}^{n} (1 - CTh_c)$$

$$\mathrm{CThR_i} = 1 - \prod_{i=1}^{n} (1 - CTh_i)$$

$$\mathrm{CThR_a} = 1 - \prod_{i=1}^{n} (1 - CTh_a)$$

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

4.4. Риск по ресурсу R рассчитывается следующим образом:

Для режима с одной базовой угрозой:

$$\mathrm{R} = CThR \times D,$$

где D – критичность ресурса. Задается в деньгах или уровнях.

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

$$D_{a/год} = D_{a/час} \times T$$

Для остальных угроз критичность ресурса задается в год. Для режима с тремя базовыми угрозами:

$$\mathrm{R_c} = CThR_c \times D_c$$

$$\mathrm{R_i} = CThR_i \times D_i$$

$$\mathrm{R_a} = CThR_a \times D_a$$

$$\mathrm{R} = \left(1 - \prod_{i=1}^{3} \left(1 - \frac{R_i}{100}\right)\right) \times 100$$

$\mathrm{D_{a,c,i}}$ – 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.

4.5. Риск по информационной системе CR рассчитывается по формуле:

Для режима с одной базовой угрозой:

- для режима работы в деньгах:

$$CR = \sum_{i=1}^{n} R_i$$

- для режима работы в уровнях:

$$\mathrm{CR} = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100$$

Для режима работы с тремя угрозами:

- для режима работы в деньгах:

$$CR_{a,c,i} = \sum_{i=1}^{n} R_i$$

$$CR = \sum_{i=1}^{n} CR_{a,c,i}$$

$\mathrm{CR_{a,c,I}}$ - риск по системе по каждому виду угроз

CR - риск по системе суммарно по трем видам угроз

- для режима работы в уровнях:

$$\mathrm{CR_{a,c,i}} = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100$$

$$\mathrm{CR} = (1 - \prod_{i=1}^{3}(1 - \frac{R_{a,c,i}}{100})) \times 100$$

4.6. 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**):

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

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 (видео- наблюдение, 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 электрон- ной Почты
		Уязвимость 2 Отсутствие регламента работы с системой криптографической за- щиты электронной корреспонденции
	Угроза 3 Разглашение конфиденциальной информации сотрудниками компании	Уязвимость 1 Отсутствие соглашений о конфиденциальности
		Уязвимость 2 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками

1.1 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 $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$
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 $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$	Общий уровень угроз по ресурсу (%), CThR $\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh)$
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 $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	Риск ресурса (у.е.), R $R = CThR \times D$
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		

Д.т.н., профессор Н.Н.Мошак