

Алгоритм: модель анализа угроз и уязвимостей

Для оценки рисков информационной системы организации защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

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.

Введение в модель

Даная модель основана на построении модели угроз и уязвимостей.

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

Исходя из введенных владельцем информационной системы данных, можно построить модель угроз и уязвимостей, актуальных для информационной системы компании. На основе полученной модели будет проведен анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитаны 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 (АС)– степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. 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 (**АСс, АСi, АСа**).

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 (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.

Принцип работы алгоритма

Входные 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.

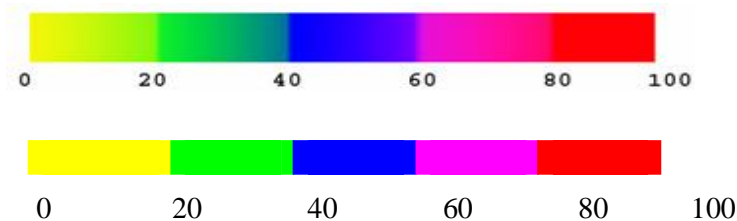
С точки зрения базовых угроз информационной безопасности существует два режима работы алгоритма:

- Одна базовая угроза (суммарная);
- Три базовые угрозы.

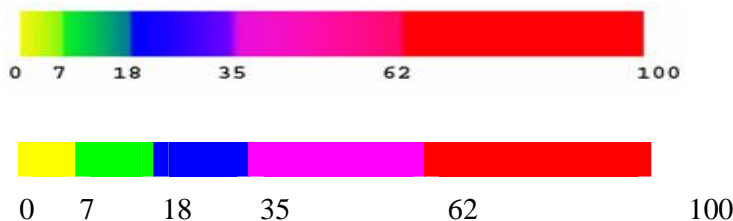
Принципы разбиения шкалы на уровни

При работе с алгоритмом используется шкала от 0 до 100%. Максимальное число уровней – 100, т.е. шкалу можно разбить на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта деления:

- равномерное;



- логарифмическое.



Расчет рисков по угрозе информационной безопасности

1. На первом этапе рассчитываем *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.

$$Th_{c,ia} = \frac{ER_{c,ia}}{100} \times \frac{P(V)_{c,ia}}{100},$$

где $ER_{c,ia}$ – критичность реализации угрозы (указывается в %);

$P(V)_{c,ia}$ – вероятность реализации угрозы через данную уязвимость (указывается в %).

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

2. Чтобы рассчитать *уровень угрозы по всем уязвимостям* STh , через которые возможна реализация данной угрозы на ресурсе, просуммируем полученные уровни угроз через конкретные уязвимости по следующей формуле:

2.1. Для режима с одной базовой угрозой:

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

2.2. Для режима с тремя базовыми угрозами:

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

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

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

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

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

3.1. Для режима с одной базовой угрозой:

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

3.2. Для режима с тремя базовыми угрозами:

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

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

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

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

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

4.1. Для режима с одной базовой угрозой:

$$R = CThR \times D,$$

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.

4.2. Для режима с тремя базовыми угрозами:

$$R_c = CThR_c \times D_c$$

$$R_i = CThR_i \times D_i$$

$$R_a = CThR_a \times D_a$$

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

$D_{a,c,i}$ – критичность ресурса по трем угрозам. Задается в деньгах или уровнях.

R - суммарный риск по трем угрозам.

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

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

5.1. Для режима с одной базовой угрозой:

5.1.1. Для режима работы в деньгах:

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

5.1.2. Для режима работы в уровнях:

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

5.2. Для режима работы с тремя угрозами:

5.2.1. Для режима работы в деньгах:

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

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

$CR_{a,c,i}$ – риск по системе по каждому виду угроз.

CR – риск по системе суммарно по трем видам угроз.

5.2.2. Для режима работы в уровнях:

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

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

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 (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 (или по одной суммарной угрозе) для ресурса;
- Риск реализации суммарно по всем угрозам для ресурса;
- Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) 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 угроз и уязвимостей

Рассмотрим расчет рисков для одной угрозы информационной безопасности, т.к. для остальных угроз риск рассчитывается аналогично.

1. Входные данные

Ресурс	Угрозы	Уязвимости
Сервер (критичность ресурса 100 у.е.)	Угроза 1 <i>Неавторизованное проникновение нарушителя внутрь охраняемого периметра (одного из периметров)</i>	Уязвимость 1 <i>Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию</i>
		Уязвимость 2 <i>Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты)</i>
	Угроза 2 <i>Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе</i>	Уязвимость 1 <i>Отсутствие авторизации для внесения изменений в систему электронной почты</i>
		Уязвимость 2 <i>Отсутствие регламента</i>

	Угроза 3	<i>корреспонденции</i>
	<i>Разглашение конфиденциальной информации сотрудниками компании</i>	Уязвимость 1 <i>Отсутствие соглашений о конфиденциальности</i> Уязвимость 2 <i>Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками</i>

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 $Th = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $CTh = 1 - \prod_{i=1}^n (1 - Th)$
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 $CTh = 1 - \prod_{i=1}^n (1 - Th)$	Общий уровень угроз по ресурсу (%), CThR $CThR = 1 - \prod_{i=1}^n (1 - CTh)$
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 $CThR = 1 - \prod_{i=1}^n (1 - CTh_i)$	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		

Таким образом, получим риск ресурса, рассчитанный по модели угроз и уязвимостей.