Searchinform

Практика применения DLP-систем

Методика оценки рисков нарушения информационной безопасности

Вопросы для обсуждения

- Термины и определения
- Постановка задачи (общий подход к оценке рисков нарушения ИБ)
- Процедуры оценки рисков нарушения ИБ
- Оценка рисков нарушения ИБ в количественной (денежной) форме

Термины и определения

- **Априорные защитные меры** – защитные меры, эксплуатация которых сокращает качественно или количественно существующие уязвимости объектов защиты информационных активов, тем самым снижая вероятность реализации соответствующих угроз ИБ (например, средства защиты от несанкционированного доступа).
- **Апостериорные защитные меры** – защитные меры, эксплуатация которых сокращает степень тяжести последствий нарушения свойств ИБ информационных активов (например, средства резервного копирования и восстановления информации).
- **Допустимый риск нарушения ИБ** – риск нарушения ИБ, предполагаемый ущерб от которого организация в данное время и в данной ситуации готова принять.
- **Информационный актив** – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации; находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.
- **Источник угрозы ИБ** – объект или субъект, реализующий угрозы ИБ путем воздействия на объекты среды информационных активов организации.
- **Модель угроз ИБ** – описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.
- **Обработка риска нарушения ИБ** – процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

Термины и определения

- **Объект среды информационного актива** – материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).
- **Остаточный риск нарушения ИБ** – риск, остающийся после обработки риска нарушения ИБ.
- **Оценка риска нарушения ИБ** – систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации БС РФ на всех стадиях их жизненного цикла.
- **Риск** – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.
- **Риск нарушения ИБ** – риск, связанный с угрозой ИБ (риски нарушения ИБ заключаются в возможности утраты свойств ИБ информационных активов в результате реализации угроз ИБ, вследствие чего организации может быть нанесен ущерб).
- **Угроза ИБ** – угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации.
- **Ущерб** – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Постановка задачи

В Волшебной стране зарегистрировано ООО «Урфин Джюс и Со», специализирующееся на выпуске деревянных солдат модели «Дуболом-1». Для производства солдат требуются бревна, инструменты (топор, пила, рубанок), а также волшебный порошок. Себестоимость одного дуболома составляет 8000 рублей, отпускная цена – 18000 рублей. Соответственно, прибыль, которую получает Урфин Джюс от продажи одного дуболома равняется 10000 рублей. На изготовление каждого деревянного солдата мастер тратит одну неделю, так что его прибыль за месяц составляет 40000 рублей.

Однажды до Урфина Джюса доходят известия о том, что его бизнесу угрожает шастающая по Волшебной стране банда в составе девочки Элли, одноногого моряка, пса Тотошки, бесстрашного *(ех-трусливого)* льва и других негодяев. Бандиты собираются сжечь дуболомов. Кроме того, производство деревянных солдат весьма пожароопасно. Естественно, Урфин Джюс всерьез задумался о том, как обезопасить свое дело. Крупнейшим специалистом Волшебной страны в сфере безопасности считался Гудвин Великий и Ужасный, поэтому именно к нему Урфин Джюс и решил обратиться за помощью.

Постановка задачи

Гудвин предложил Урфину Джюсу на выбор с целью защиты дуболомов:

- приобрести несгораемый шкаф (сейф) за 100000 руб.;
- приобрести огнетушитель за 5000 руб.;
- в обмен на корм стоимостью 35000 руб. поручить вороне Кагги-Карр следить за тем, что собираются делать бандиты, и своевременно предупреждать Урфина Джюса об опасности.

Проблема! Что из предложенных средств должен предпочесть Урфин Джюс?

Сейф надежно защитит дуболома, но только одного, да и стоит сейф дорого.

Огнетушитель сравнительно дешев, но может быть использован только после того, как дуболома уже подожгут.

Работа Кагги-Карр обойдется дешевле, чем сейф, но сама по себе также не способна на 100% защитить дуболома.

Не в силах разобраться в свалившихся на его голову проблемах Урфин Джюс обращается к Страшиле Мудрому, известному эксперту в подобных вопросах, роль которого предстоит сыграть Вам.

Снова термины и определения

- **Активы** – топор, пила, рубанок, мастерская, навыки Урфина Джюса по обработке древесины, волшебный порошок, средства обеспечения связи с покупателями, процесс производства дуболомов, сами дуболомы и т.д.
- **Априорные защитные меры** – несгораемый шкаф (сейф).
- **Апостериорные защитные меры** – огнетушитель.
- **Допустимый риск нарушения ИБ** – 1 сгоревший дуболом в 6 месяцев.
- **Информационный актив** – информация о количестве и себестоимости дуболомов, прибыли Урфина Джюса, стоимости топора, пилы, рубанка, наличии волшебного порошка, средств обеспечения связи с покупателями, сведения о навыках Урфина Джюса по обработке древесины, контракты на производство дуболомов и т.п.
- **Источник угрозы ИБ** – Элли и ее друзья, факелы, свечи и др. огнеопасные предметы.
- **Модель угроз ИБ** – описание того, как, с помощью каких предметов и в каком количестве Элли и ее друзья могут уничтожать дуболомов.
- **Обработка риска нарушения ИБ** – обращение Урфина Джюса к Гудвину и Страшиле, а затем процесс выбора и осуществления защитных мер.
- **Объект среды информационного актива** – конторская книга, чеки, векселя, записки, пьяная болтовня и т.п.
- **Остаточный риск нарушения ИБ** – 1 сгоревший дуболом в год.
- **Оценка риска нарушения ИБ** – работа Страшилы.
- **Риск** – количество сгоревших дуболомов.
- **Риск нарушения ИБ** – количество сгоревших дуболомов.
- **Угроза ИБ** – угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации.
- **Ущерб** – утрата или порча дуболомов, мастерской, депрессия или пьянство Урфина Джюса и т.п. в результате действий бандитов.

Процедуры оценки рисков нарушения ИБ

В первую очередь Страшила проводит **идентификацию активов**, в ходе которой выясняется, что производство дуболомов и получаемая прибыль в немалой степени зависят от наличия надежных и достоверных сведений о стоимости топора, пилы, рубанка, наличии волшебного порошка, о количестве и себестоимости дуболомов, прибыли Урфина Джюса, средств обеспечения связи с покупателями, о навыках Урфина Джюса по обработке древесины, о наличии контрактов на производство дуболомов … т.е. всего того, что ранее было названо **информационными активами**. Для дальнейших рассуждений обозначим их как a_1, a_2, a_3, … a_n.

Второй этап — **оценка активов**. Если один из перечисленных активов теряется или утрачивает свои свойства (например, конфиденциальность), то процесс производства дуболомов может утратить свою эффективность либо даже вовсе приостановиться. Это означает, что Урфин Джюс будет терять деньги до тех пор, пока актив не будет восстановлен. Поэтому, чтобы оценить активы необходимо определить ряд показателей:

Процедуры оценки рисков нарушения ИБ

- **Стоимость простоя процесса** *(C)* – параметр показывает сколько рублей в единицу времени теряет Урфин Джюс в связи с тем, что процесс простаивает. Исходя из того, что месячная прибыль составляет 40000 рублей, будем считать, что *C = 40000 рублей / 20 рабочих дней = 2000 рублей*.
- **Время восстановления актива** *(ta_i)* – показывает как долго процесс изготовления дуболомов будет простаивать до своего возобновления (т.е. до того момента пока не будет восстановлен актив, который его (процесс) обеспечивает). Если выйдет из строя или потеряется, например, топор или пила, то Урфину Джюсу придется съездить в город и приобрести новые. При этом пока он будет находится в пути, естественно, никакого производства не будет. Поездка займет весь день, да и информация о ценах на топоры и пилы лишней не станет – цены стоит узнать заранее, а на это также потребуется время. Волшебный порошок – вообще уникальная вещь, в городе его не купишь, а ждать пока вырастут новые растения, из которых его можно приготовить, придется целых 2 недели. Кроме того, сами сведения об обладания Урфином Джюсом волшебным порошком представляют собой очевидный информационный актив: утрата конфиденциальности в этом случае может превратить дуболомов из эксклюзивного товара в заурядный со всеми вытекающими последствиями для бизнеса. В нашей истории будем считать, что *ta_1 - время восстановления информационного актива* a_1 *(стоимость топора) составит 1 день; ta_2 - время восстановления актива* a_2 *(стоимость пилы) – 1 день; ta_3 - время восстановления актива* a_3 *(наличие волшебного порошка) – 14 дней.*

Процедуры оценки рисков нарушения ИБ

- **Стоимость восстановления** *Ca_i* – показывает, сколько потребуется денег, чтобы восстановить актив. Это может быть стоимость ремонта или стоимость приобретения нового актива взамен старого, стоимость обновления необходимой информации (например, для того, чтобы узнать актуальную стоимость топора, нужно, как минимум, купить газету, позвонить и т.д.). Таким образом, *Ca_1 - стоимость восстановления информационного актива* a_1 *(стоимость топора) составит 500 рублей; Ca_2 - стоимость восстановления актива* a_2 *(стоимость пилы) – 1000 рублей (хорошие пилы продаются только в стране жевунов); Ca_3 – стоимость восстановления актива* a_3 *(наличие волшебного порошка) – 50000 рублей.*

Третий этап — **идентификация и оценка угроз**. Допустим, в нашем случае были выделены две угрозы - «террористический акт с поджогом» и «пожар». Для каждой из них были определены вероятности реализации *(PT_i)*: *PT_1 - вероятность реализации угрозы T_1* (теракт с поджогом) - *0,001; PT_2 - вероятность реализации угрозы T_2* (пожар) - *0,0005.* Поскольку *у нас з*а единицу времени взяты сутки, данные вероятности означают, что, по мнению эксперта, теракты происходят раз в 1000 суток, а пожары — раз в 2000 суток.

Процедуры оценки рисков нарушения ИБ

Четвертый этап — **оценка вероятности воздействия угрозы на актив** (PI_i). Предположим, эксперт оценил данные показатели следующим образом:

Информационный актив	T_1	T_2
Стоимость топора	0,1	0,9
Стоимость пилы	0,1	0,9
Волшебный порошок	0,9	0,9

Значения *PI* при угрозе T_1 означают, что если теракт с поджогом произойдет, то в лишь в одном случае из 10 террористы будут «сбивать» или «накручивать» стоимость топора или пилы. В то же время несложно предположить, что в 9 случаях из 10 террористы направят свои усилия на уничтожение волшебного порошка: ведь это похоронит бизнес Урфина Джюса. В случае угрозы T_2: пожар уничтожит все вещи с одинаковой вероятностью.

Оценка рисков нарушения ИБ

Пятый этап — **расчет рисков**. В отличие от других подобных методик мы не будем механически суммировать стоимость утраченных активов, а будем отталкиваться от угроз. Допустим, для каждого из активов и для каждой из угроз мы рассчитали риски по формуле: $R=PT_i * PI_i * W$, где PT_i – вероятность реализации угроз, PI_i – вероятность воздействия угрозы на актив, а W – стоимость последствий, в свою очередь, рассчитываемая как $W=ta_i * C+Ca_i$, где ta_i – время восстановления актива, C – стоимость простоя процесса, Ca_i – стоимость восстановления актива. В нашем случае: *W(стоимости топора)=1*(40000/20)+500=2500 руб., W(стоимости пилы)=1*(40000/20)+1000=3000 руб., W(волшебного порошка)=14*(40000/20)+ +50000=78000 руб.* Тогда получим следующие значения рисков:

Информационный актив	T_1	T_2
Стоимость топора	0,25	1,125
Стоимость пилы	0,3	1,35
Волшебный порошок	70,2	35,1

Если угроза затронула один из активов, существует вероятность, что она затронет и другой, подверженный данной угрозе. В этом случае процесс простаивает по двум причинам, и получается, что мы это учитываем дважды. Ведь чтобы приостановить процесс достаточно выхода из строя хотя бы одного из активов. Для того, чтобы это учесть, стоит воспользоваться формулой для расчета вероятности суммы совместных событий (которая как раз и показывает вероятность того, что произошло хотя бы одно из событий).

Оценка рисков нарушения ИБ

Для угрозы T_1 вероятность того, что террористы сожгут топор либо пилу либо волшебный порошок, будет составлять 0,919 (обозначим $PI(a_1,a_2,a_3)$ — с такой вероятностью процесс будет простаивать хотя-бы один день (обозначим t_1). С другой стороны, есть вероятность, что процесс будет простаивать еще 13 дней (обозначим t_2), и она равна той, с которой сожгут волшебный порошок (0,9). Кроме того, с этой же вероятностью его придется заменить. А топор и пилу придется заменить с вероятностью 0,1. Тогда формула для расчета суммарного риска по данной угрозе будет выглядеть следующим образом:

$$\mathbf{RT_1=PT_1*(PI(a_1,a_2,a_3)*C*t_1+PI(a_3)*C*t_2+PI(a_1)*C(a_1)+PI(a_2)*C(a_2)+PI(a_3)*C(a_3))=0,001*(1225+15600+50+100+45000)=70,39\ рублей/сутки}$$

Точно так же рассчитаем риск при угрозе T_2 (пожар):

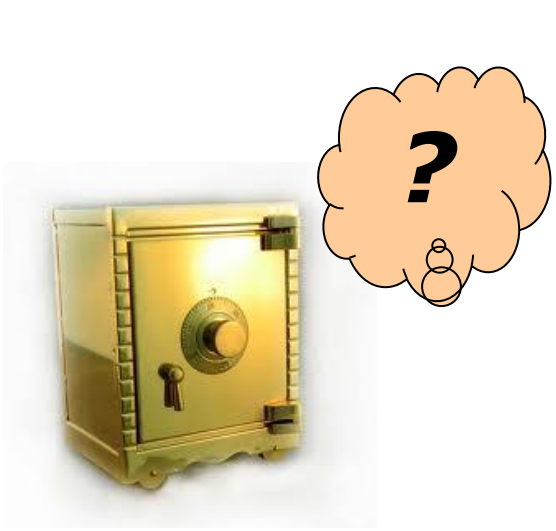
$$\mathbf{RT_2=PT_2*(PI(a_1,a_2,a_3)*C*t_1+PI(a_3)*C*t_2+PI(a_1)*C(a_1)+PI(a_2)*C(a_2)+PI(a_3)*C(a_3))=35,87\ рублей/сутки}$$

Полученные цифры можно интерпретировать следующим образом: если Урфин Джюс будет ежедневно откладывать столько рублей, то его накопления смогут покрыть последствия реализованной угрозы в тот момент, когда она случится. Руководству организации как и Урфину Джюсу следует решить, устраивают ли их эти цифры, или необходимо снизить риски (хотя есть еще вариант с делегированием рисков). Один из методов снижения рисков - внедрение средств защиты информации. Стоит отметить, что есть и другие методы - воздействие на источник угрозы или перенос организации в другую среду функционирования (может снизить значение вероятности реализации угрозы (PT)). Другой метод — создание дубликатов или резервных копий — позволяет снизить время восстановления актива.

Проблема выбора средств защиты

Вспомним, что Гудвин предложил Урфину Джюсу на выбор с целью защиты дуболомов:

- приобрести несгораемый шкаф (сейф) за 100000 руб.;
- приобрести огнетушитель за 5000 руб.;
- в обмен на корм стоимостью 35000 руб. поручить вороне Кагги-Карр следить за тем, что собираются делать бандиты, и своевременно предупреждать Урфина Джюса об опасности.



Проблема выбора средств защиты

Выбор того или иного средства защиты изменяет (уменьшает) параметр PI_i.

Оценка вероятности воздействия угрозы на актив без СЗИ

Информационный актив	T_1	T_2
Стоимость топора	0,1	0,9
Стоимость пилы	0,1	0,9
Волшебный порошок	0,9	0,9

RT_1= 70,39 руб./сутки
RT_2= 35,87 руб./сутки
R= RT_1+RT_2=106,26 руб./сутки

Оценка вероятности воздействия угрозы на актив при наличии сейфа

Информационный актив	T_1	T_2
Стоимость топора	0,1	0,9
Стоимость пилы	0,1	0,9
Волшебный порошок	0,05	0,01

RT_1= 5,79 руб./сутки
RT_2= 2,05 руб./сутки
R= RT_1+RT_2=7,84 руб./сутки

Оценка вероятности воздействия угрозы на актив при наличии огнетушителя

Информационный актив	T_1	T_2
Стоимость топора	0,1	0,1
Стоимость пилы	0,1	0,1
Волшебный порошок	0,9	0,9

RT_1= 70,39 руб./сутки
RT_2= 35,27 руб./сутки
R= RT_1+RT_2=105,66 руб./сутки

Оценка вероятности воздействия угрозы на актив при использовании информации, предоставляемой вороной

Информационный актив	T_1	T_2
Стоимость топора	0,1	0,9
Стоимость пилы	0,1	0,9
Волшебный порошок	0,01	0,9

RT_1= 2,75 руб./сутки
RT_2= 35,87 руб./сутки
R= RT_1+RT_2=38,62 руб./сутки

Оценка эффективности применения средств защиты

Для оценки эффективности средств защиты следует ввести несколько производных величин:

R'=R–RR – величина, на которую снизился риск (разность между риском до внедрения средства защиты и остаточным риском). Кроме того, приобретенное средство защиты, станет вторичным активом, обеспечивающим процесс защиты активов (в т.ч. и информации). Стоимость простоя данного процесса равна R'. Теперь при необходимости можно будет использовать эту цифру для оценки рисков при угрозах направленных на средства защиты.

Величина снижения риска (R')		
Средство защиты	**Стоимость, руб.**	**R', руб./сутки**
Несгораемый шкаф (сейф)	100000	98,42
Огнетушитель	30000	0,6
Ворона	35000	67,64

N=R'/R – эффективность средств защиты. Показатель позволяет определить, какое из средств защиты будет наиболее эффективным для защиты активов.

Эффективность средств защиты (N)		
Средство защиты	**Стоимость, руб.**	**N, %**
Несгораемый шкаф (сейф)	100000	92,62
Огнетушитель	30000	0,56
Ворона	35000	63,65

Оценка эффективности применения средств защиты

t_r – время возврата инвестиций. Обозначим стоимость средств защиты как C_d, тогда: $t_r = C_d / R$'. Приведенные цифры показывают через какое время (в данном случае в сутках) средство защиты окупится и начнет приносить прибыль.

Время возврата инвестиций (t_r)		
Средство защиты	**Стоимость (C_d), руб.**	**t_r, суток**
Несгораемый шкаф (сейф)	100000	1016,1
Огнетушитель	30000	8333,3
Ворона	35000	517,4

На основании этих трех величин, а также стоимости приобретения средств защиты Урфину Джюсу (и руководству организации) будет гораздо проще выбрать то, что им покажется наиболее подходящим.

Спасибо за внимание!