Оценка угроз и уязвимостей

написано Александр Астахов | 10 июня, 2023

После *идентификации* угроз и уязвимостей необходимо оценить *вероятность* их объединения и возникновения риска. Это включает в себя оценку вероятности реализации угроз, а также того, насколько легко они могут использовать имеющиеся уязвимости.

*Оценка вероятности угроз*должна учитывать природу угроз и особенности, присущие различным группам угроз, например:

- *Преднамеренные угрозы*. Вероятность преднамеренных угроз зависит от мотивации, знаний, компетенции и ресурсов, доступных потенциальному злоумышленнику, а также от привлекательности активов для реализации атак.
- *Случайные угрозы*. Вероятность случайных угроз может оцениваться с использованием статистики и опыта. Вероятность таких угроз может зависеть от близости организации к источникам опасности, таким как автомагистрали и железнодорожные пути, а также заводы, имеющие дело с опасными материалами, химическими веществами или бензином. Также географическое положение организации оказывает влияние на возможность возникновения экстремальных погодных условий. Вероятность человеческих ошибок (одна из наиболее распространенных случайных угроз) и поломки оборудования также должны быть оценены.
- *Прошлые инциденты*. Инциденты, происходившие в прошлом, иллюстрирующие проблемы в существующих защитных мерах.
- *Новые разработки и тенденции*. Они включают в себя отчеты, новости и тенденции, полученные из Интернет, групп новостей, от других организаций и консультантов.

Лучше всего получать информацию, используемую для оценки вероятности угрозы и величины уязвимости, от тех, кто

непосредственно вовлечен в бизнес-процессы, находящиеся в условиях риска, а также от экспертов по безопасности, имеющих наибольший опыт в обращении с этими угрозами и уязвимостями. Также может быть полезным использование списков угроз и уязвимостей и взаимосвязей между угрозами и механизмами контроля из ISO 27002, приведенных в Приложении № 6.

Для оценки*вероятности* реализации угрозы может использоваться *трехуровневая качественная шкала:*

- ***H***— *низкая вероятность*. Маловероятно, что эта угроза осуществится, не существует инцидентов, статистики, мотивов и т.п., которые указывали бы на то, что это может произойти. Ожидаемая частота реализации угрозы не превышает 1 раза в 5—10 лет.
- ***C***— *средняя вероятность*. Возможно, эта угроза осуществится (в прошлом происходили инциденты), или существует статистика или другая информация, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий. Ожидаемая частота реализации угрозы — примерно один раз в год.
- ***B***— *высокая вероятность*. Эта угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия. Ожидаемая частота реализации угрозы — еженедельно или чаще.

Такой трехуровневой шкалы обычно достаточно для первоначальной высокоуровневой оценки угроз. В дальнейшем ее можно расширить, добавив еще пару промежуточных уровней.

Таблица. Оценка вероятности угроз (фрагмент)

№	Группа угроз	Уровень	Примечание
	Угрозы утечки конфиденциальной информации		
	Утечка конфиденциальной информации из сети по каналам связи (email, web, chat/IM и т.п.)Не целевое использование компьютерного оборудования и сети Интернет сотрудниками организации	С	Квалификация сотрудников досточно низкая и большинство каналов перекрыто, что снижает вероятность данной угрозы
	Утечка конфиденциальной информации на мобильных устройствах, носителях информации, ноутбуках и т.п.Не целевое использование компьютерного оборудования и сети Интернет сотрудниками организации	С	Угроза достаточно легко осуществима, однако ноутбуки и КПК не используются
	Прослушивание внешних каналов связи злоумышленниками	Н	Угроза не соответствует ценности информации

Общая вероятность инцидента также зависит от уязвимостей активов, т.е. насколько легко слабости активов могут быть использованы для успешного осуществления угроз.

Уязвимости, так же как и угрозы, могут быть оценены по *трехуровневой качественной шкале*. Значение уровня уязвимости показывает, насколько вероятно успешное осуществление угрозы с использованием данной уязвимости в случае, если эта угроза будет реализовываться. Соответствующие качественные уровни уязвимости могут быть определены, например, следующим образом:

- ***В*** *– вероятно*. Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует. Вероятность

успешной реализации угрозы ~ 0.9 – 1.

- ***С*** *– возможно*. Уязвимость может быть использована, но существует определенная защита. Вероятность успешной реализации угрозы ~ 0.5.
- ***Н*** *– маловероятно*. Уязвимость сложно использовать, и существует хорошая защита. Вероятность успешной реализации угрозы ~ 0 – 0.1.

Так же, как и с угрозами, для первоначальной высокоуровневой оценки уязвимостей вполне должно хватить данной трехуровневой шкалы. В дальнейшем для более детальной оценки, при необходимости, сможем добавить еще пару промежуточных уровней.

Оценка вероятности угроз и величины уязвимостей заносится в таблицу, изображенную на рисунке, и в реестр информационных рисков, минуя промежуточную таблицу.

Таблица. Результаты оценки угроз и уязвимостей (фрагмент)

№	Группы угроз	Уязвимости	Вероятность угроз	Уровень уязвимости	Механизмы контроля
	НСД к ресурсам ЛВС компании со стороны внутренних злоумышленниковМаскарад, использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации	Слабые пароли, отсутствие парольной политикиНаличие внутренних уязвимостей, обусловленных несвоевременным обновление ОСМониторинг действий пользователей не производится	С	В	Корректное управление доступомНизкая квалификация пользователей для осуществления НСД

№	Группы угроз	Уязвимости	Вероятность угроз	Уровень уязвимости	Механизмы контроля
	НСД к ресурсам ЛВС компании со стороны внешних злоумышленниковМаскарад, использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации	Отсутствуют последние обновления на корпоративном файрволлеЕдинственный защитный барьерНаличие внутренних уязвимостей, обусловленных несвоевременным обновлением ОСОтсутствие системы обнаружения вторжений (IDS)	В	С	Хорошая защита периметраОтсутствие известных уязвимостей

Следует обратить внимание на то, что в таблице оценки угроз и уязвимостей фигурируют группы угроз и группы уязвимостей, а оценка вероятности является суммарной оценкой вероятностей всех угроз и всех связанных с ними уязвимостей.

При оценке величины группы уязвимостей взвешиваются все найденные слабости защиты, способствующие успешному осуществлению угроз, и все существующие механизмы контроля, затрудняющие осуществление этих угроз. Суммарный уровень группы уязвимостей определяется путем сложения уровней всех идентифицированных уязвимостей и вычитания из них уровней всех идентифицированных механизмов контроля, при это действенность (уровень) механизма контроля определяется по такому же принципу, как и уровень уязвимости:

- ***В*** *– высокий уровень контроля*. Маловероятно, что такой механизм контроля удастся обойти. Вероятность обхода (преодоления) механизма контроля ~ 0 – 0.1.
- ***С*** *– средний уровень контроля*. Механизм контроля обеспечивает определенную защиту, однако есть возможность его обойти, затратив определенные усилия. Вероятность обхода (преодоления) механизма контроля ~ 0.5.
- ***Н*** *– низкий уровень контроля*. Такой механизм контроля незначительным образом уменьшает уязвимости активов, и

его довольно просто обойти. Вероятность обхода (преодоления) механизма контроля ~ 0.9 – 1.

Для определения итогового уровня уязвимости, рассматриваемой для конкретной группы угроз, обычно используются экспертные оценки. На правую чашу весов кладутся механизмы контроля, на левую – уязвимости. Если сильно перевешивают уязвимости, тогда итоговый уровень будет высоким. Если существенный перевес на стороне механизмов контроля, которые способны нивелировать все имеющиеся уязвимости, тогда итоговый уровень уязвимости будет низким. Если между механизмами контроля и уязвимостями наблюдается примерный паритет, тогда итоговый уровень уязвимости оценивается как средний.

Конечно, такая оценка навряд ли может считаться объективной, т.к. всецело зависит от мнения того или иного эксперта об уязвимостях и механизмах контроля. К сожалению, ничего более точного мы здесь предложить не можем. Многие умные люди пытались придумать более точные методы анализа угроз и уязвимостей, писали формулы, строили модели, но так ни до чего реально эффективного и не додумались. Любые математические выкладки, сопровождающие точные количественные методы измерений, оставались на бумаге, и если для чего то и годились, то только не для использования в практической работе.

Хорошая новость заключается в том, что для принятия решений по рискам, а больше излагаемая здесь методология ни для чего не нужна, вполне достаточно простого качественного подхода к оценке угроз и уязвимостей. Такой подход демонстрирует свою высокую эффективность и в полной мере соответствует потребностям современных организаций. На практике всего-навсего требуется правильно и своевременно идентифицировать возможные проблемы, расставив должны образом приоритеты по их предупреждению.

Для повышения объективности оценки следует применять

подтвердившие свою эффективность методы экспертной оценки, такие как, например, метод Дельфи. Надо устраивать коллективные обсуждения угроз, уязвимостей и механизмов контроля, на которые следует приглашать представителей различных бизнес-подразделений, владельцев активов и бизнес-процессов, экспертов по безопасности и внешних консультантов. Это повышает не только объективность оценок, но и, что не менее важно, осведомленность всех участников таких обсуждений.

Оценки ожидаемой частоты реализации угрозы от уровня к уровню по качественной шкале различаются в разы, поэтому маловероятно, чтобы компетентная экспертная группа так сильно ошибалась в своих оценках.

В Приложениях № 7 и № 8 приведены примеры опросных листов, используемых для оценки угроз и уязвимостей в методе CRAMM.