УДК 338.45

МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

© 2011 А.В. Балановская*

Ключевые слова: информационная безопасность, угрозы информационной безопасности, модель угроз, факторы категорий угроз, агент угроз, уязвимость, модель злоумышленника.

Рассматривается классификация возможных угроз информационной безопасности. Описывается структура модели информационной безопасности. Произведена оценка возможности реализации угрозы. Раскрывается сущность проблем информационной безопасности на основе выбора правильной стратегии по противодействию злоумышленникам.

Перечень и классификация возможных угроз информационной безопасности (ИБ) сами по себе тривиальны, давно разработаны и могут иметь тысячи названий в зависимости от степени детализации. Тем не менее, проблема формирования конкретной модели угроз является важнейшей основой для организации всей дальнейшей работы по обеспечению информационной безопасности конкретного бизнеса.

Модель угроз может быть описана только после построения модели злоумышленника (нарушителя), которая, в свою очередь, определяется сутью ценности защищаемого актива, приоритетами безопасности и собственно данными субъектов угроз. Практически любой информационный комплекс легко подвергается многоуровневой вертикальной структуризации, в результате чего в системе выделяются семь уровней: физический, сетевой, сетевых приложений, операционных систем, СУБД, приложений, бизнес-процессов. Важным при построении модели угроз является признание того, что на каждом из уровней угрозы, их источники, методы, средства защиты и подходы к оценке эффективности являются различными.

Главная цель злоумышленника - получение контроля над активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов (например, путем раскрытия конфиденциальной информации) эффективнее для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, требующее больших специфических опыта, знаний и ресурсов (в том числе временных), и поэтому менее эффективное по соотношению “затраты - получаемый результат”. Промышленное предприятие должно определить конкретные объекты защиты на каждом из уровней информационной инфраструктуры.

Наиболее актуальные источники угроз на физическом, сетевом уровнях и уровне сетевых приложений: внешние источники угроз - лица, распространяющие вирусы и другие вредоносные программы; внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами; комбинированные источники угроз - внешние и внутренние, действующие совместно и (или) согласованно. Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов: внутренние, реализующие угрозы в рамках своих полномочий и за их пределами; комбинированные источники угроз - внешние и внутренние, действующие в сговоре. Наиболее актуальные источники угроз на уровне бизнес-процессов: внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами; комбинированные источники угроз - внешние и внутренние, действующие в сговоре. Также необходимо учитывать угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью. Источники угроз для реализации угрозы используют уязвимости объектов и системы защиты. Модель угроз ИБ включает описание источников угрозы, уязвимостей, используемых угрозами, мето-

* Балановская Анна Вячеславовна, докторант Самарского государственного экономического университета. E-mail: balanovskay@mail.ru.

дов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба. Для источников угроз - людей может быть разработана модель нарушителя ИБ, включающая описание их опыта, знаний доступных ресурсов, необходимых для реализации угрозы, и возможной мотивации их действий.

Исключительно важным является вопрос приоритета при выборе конкретного набора актуальных угроз. Таким приоритетом в общем случае является вес, или весовой коэффициент угрозы, измеряемый вероятностью ее реализации. Именно вероятности реализации угроз являются наиболее подвижной и быстроизменяющейся составляющей проблемы, радикально влияющей на формирование политики безопасности промышленного предприятия. Сама по себе угроза не несет никакой опасности, она является только предположением о возможной опасности и не более того. Защищающаяся сторона должна решить, по крайней мере, две задачи. Первая задача заключается в оценке так называемой возможности реализации предполагаемой угрозы, а вторая - в оценке возможных затрат, всегда возникающих при применении средств защиты.

Оценка возможности реализации угрозы зависит от многих факторов. Во многих источниках возможность реализации угрозы определяется как некоторая вероятность. Если бы это было так, то многие проблемы были бы сняты, так как, проведя математические расчеты и используя понятие и меру риска, ошибиться, например, на величину 0,001, можно было бы достаточно уверенно себя чувствовать в плане прогнозирования реализации угрозы. Однако на деле не все так просто. Обратим внимание на ряд определений, введенных в ГОСТ Р 51897. В этом стандарте определено понятие риска как “сочетание вероятности события и его последствий”. Поэтому было бы целесообразно посмотреть, какой смысл вкладывается в понятие вероятности. В данном ГОСТе вероятность определяется как “мера того, что событие может произойти”. Также делается ссылка на ГОСТ Р 50779.10, в котором вероятность определяется как “действительное число от 0 до 1, относящееся к случайному событию. Число может отражать относительную частоту в серии наблюдений или степень уверенности в том, что некоторое событие произойдет”. Таким образом, возможность реализации угрозы, определяемая через понятие вероятность, содержит две составляющие, одна из которых определяет частотность событий, а вторая - степень уверенности, что событие произойдет.

Первая составляющая, определяющая частотность событий, достаточно хорошо проработана в классической теории вероятностей. Пример решения такой задачи - расчет вероятности попадания хотя бы одного артиллерийского снаряда в цель при проведенном залпе при известной статистике вероятности попадания одного снаряда в цель. Безусловно, статистику в данном случае можно приравнять к материализации опыта, и она должна быть использована. Однако есть вторая составляющая, определяемая как степень уверенности, которую следует отнести к субъективным факторам оценки. Эта составляющая введена из-за невозможности в общем виде ориентироваться на имеющуюся статистику ввиду существенных различий сферы действий в бизнесе и разных платформ оценки риска, в рассматриваемом случае выступающей в виде оценки возможности реализации угрозы.

Гораздо глубже позиции по оценке возможностей наступления событий раскрываются в стандарте Австралии/Новой Зеландии AS/NZS 4360:2004. В данном стандарте понятие оценки возможности через принятие риска интерпретируется в терминах “опасности или негативных воздействий”, а риск трактуется как “раскрытие последствий неопределенности или потенциальных отклонений от запланированного или ожидаемого”. В связи с этим в стандарте помимо использования классического понятия вероятности как относительной величины появления событий в серии испытаний вводится новое понятие “правдоподобие” как общее описание вероятности или частоты, определяемое как качественно, так и количественно.

Можно сделать вывод о том, что угроза, являющаяся источником потенциального ущерба, а потому представляющая некото-

рую опасность, каким-либо образом должна быть измерена. Фактически, речь идет уже о формировании модели угроз. Безусловно, измерение угрозы следует начать с оценки возможности ее возникновения. Такая оценка может быть сделана на основе данных по известным фактам появления угрозы, выраженным через статистическую частотность. Данную оценку можно рассматривать как оценку, основанную на имеющемся опыте эксплуатации. Кроме этого должна быть и на практике имеет место субъективная оценка, сущность которой определяется как особенностью бизнеса, так и субъективной оценкой собственником возможного проявления опасностей - угроз.

Вторым фактором оценки возможности реализации угрозы является оценка затрат, неизбежно возникающих при введении тех или иных средств защиты. Правильнее было бы сказать “ущерб” - урон, который понесет собственник, а не “затраты”. Урон может выражаться не только экономическим ущербом, нанесенным в текущий промежуток времени, но и в виде других ущербов, например репутации, которые могут привести к более существенным уронам в будущем. При внедрении средств защиты производятся затраты не только на приобретение средств, но и на их текущее обслуживание. Введение средств защиты снижает возможность реализации одной или группы угроз, уменьшая ущерб от реализации. Как правило, оптимальный вариант соотношения “затраты на покупку и эксплуатацию средств защиты - возможный ущерб от реализации угроз” определяется собственником. Например, возможен выбор таких защитных мер, реальные затраты на реализацию которых будут находиться на одном уровне с потерями, которые может понести собственник при реализации оставшихся угроз. Превышение затрат по сравнению с оптимальным уровнем, безусловно, уменьшает возможности реализации новых угроз, но в общем балансе “ущерб - затраты” последние могут стать излишне высокими.

Над путями практического поиска этого оптимума продолжают работать и в настоящее время, однако все решения по данному вопросу носят характер общеметодологических рекомендаций. Вряд ли в ближайшее время можно ожидать точных практических рекомендаций по этому вопросу, что связано с большим числом субъективных факторов. Современная философия выбора защитных мер основана на решении собственника, который обеспечивает выбор, в частности, на базе определения опасного для себя перечня угроз, которые по его представлению могут привести к существенным потерям. На такой философии построены наиболее применяемые в настоящее время стандарты, такие как ГОСТ Р ИСО/МЭК (гармонизированный с международным стандартом ISO/IEC 15408-1999), ориентируемый на продукты и информационные технологии, и международный стандарт ISO/IEC 17799, ориентируемый на организации.

Переход на применение строго регламентированных средств защиты, ориентируемых на определенный уровень защиты, как философия, которая продолжает функционировать в России на основе действующих руководящих документов, безусловно, существенно упрощает расчет затрат, однако такой подход в бизнес-организациях признан в мире как устаревший и непригодный. Поскольку собственники определяют опасные угрозы на основе и объективных, и субъективных факторов, деятельность по их оценке является неизбежной и крайне необходимой. Участие собственников в процессе признания и утверждения состава угроз крайне желательно, так как это позволит быстрее решить вопрос финансирования затрат на реализацию защитных мер.

Рассматривая процесс реализации угроз, приходим к пониманию сущности угроз и выбора правильной стратегии по противодействию им. Решающую роль в этом играет уязвимость, т.е. слабые места продукта, которые, как правило, используются в процессе реализации угрозы. Продукт, защищенный от большинства опасных с точки зрения возможности реализации угроз, нельзя получить случайно, он является следствием грамотного современного подхода к проектированию, когда на этапе разработки информационных продуктов заботятся об обеспечении информационной безопасности. Сегодня это большая редкость.

Уязвимость продукта в определенной мере является философским понятием. Для пере-

хода от общей философии нападения, базирующейся на понятиях "угроза" и "уязвимость", к более конкретной оценке следует рассмотреть категорию атак. Например, в ГОСТ Р ИСО/МЭК 15408-2002 этот вопрос предложено решать в такой последовательности. Необходимо "определить угрозу в терминах агента угроз, предполагаемого способа атаки, уязвимостей, которые являются основой для атаки, и в терминах информационных ресурсов, которые подвергаются атаке". В этом же документе предлагается классифицировать угрозы с помощью оценок правдоподобия развития угрозы в действительную атаку, оценивая правдоподобие этой атаки и последствия любого ущерба.

Рассмотренные факторы представляют собой фактически структуру модели действия противника. Собственник при разработке реальной модели противника должен провести наполнение и детализацию факторов, рассматриваемых ниже, и при необходимости ввести специфичные факторы, учитывающие особенности собственной системы. При переходе к категории атак необходимо провести оценку агента угроз и направлений атак. Оценка агента угроз включает оценку опыта, ресурсов и мотивации противника. Направление атак включает цель, метод, механизм воздействия и рассмотренные выше уязвимости.

Целями атак могут быть: неавторизованный доступ к ресурсам, получение доступа или раскрытие конфиденциальной информации, модификация информации, как с целью ее искажения, так и изменения адресов отправителя и получателя, затруднение или запрет доступа легальных пользователей к информации и ресурсам. Методы атак могут быть основаны на сосредоточенном или распределенном в пространстве или времени способах. Механизм воздействия атаки, как правило, содержит две фазы. Первая фаза определяется как проникновение в систему и характеризуется появлением инцидентов, связанных с ИБ. Вторая фаза атаки фактически является внедрением в систему, когда противник практически переходит во владение ресурсами и активами системы или предприятия.

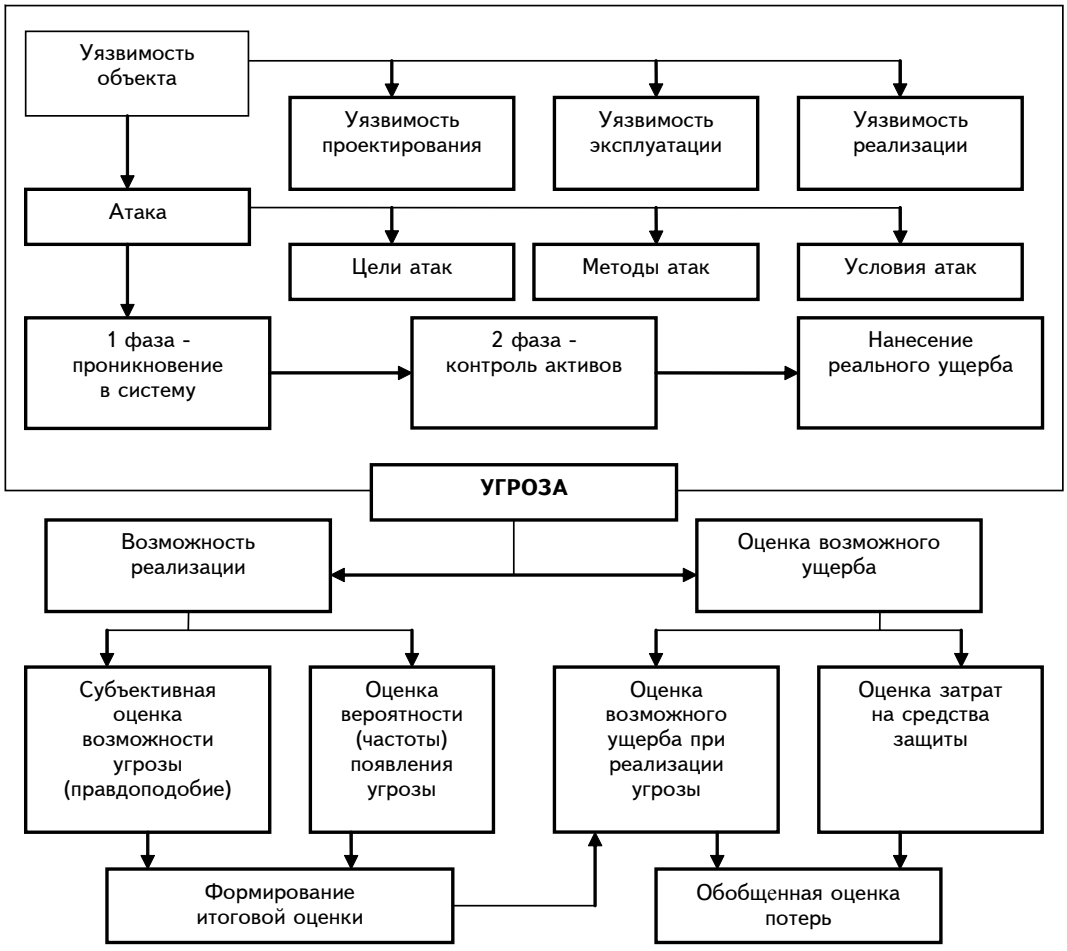

Рис. **Взаимосвязь факторов категории угроз**

На рисунке в графической форме показаны основные факторы и связи между ними, касающиеся такой важной категории, как угроза.

Теперь, когда определены модель угроз и модель злоумышленника при реализации угроз, приведем наиболее распространенное определение угрозы (ISO/IEC TR 13335). Угроза - потенциальная причина инцидента, который может нанести ущерб системе или предприятию.

Следует отметить, что развитие в 1990-х гг. корпоративных информационных систем обеспечивалось на основе исходной базы обеспечения ИБ, имеющей место в то время в России. Исходной и концептуальной основой защиты была ориентация на защиту от врага извне.

Считалось, что наличие внутреннего врага является более исключением, чем правилом, а наличие строгого контроля (допуска) персонала и ответственности за нарушения - достаточными для поддержания убедительного уровня ИБ внутри промышленного предприятия. Однако в дальнейшем как изменение общей среды, так и существенное увеличение числа корпоративных систем в корне изменили данную концептуальную схему.

Существенное увеличение числа корпоративных систем не позволяло обеспечить их комплектование персоналом из устойчиво доверительной среды. Существенно повысилась роль управляющего персоналом, появились значительно большие возможности по регулировке и настройке систем и сетей, а значит, возросли и возможности их недружелюбного использования. Исчез фактор боязни получить "белый билет", практически не дающий возможности работать в серьезных организациях при выявлении нарушений.

Свободный рынок труда, как правило, не особенно озабочен чистотой персонала и историей его прошлой деятельности, да и подделка личных досье уже не является редкостью. Увеличилось число недоброкачественного продукта, обладающего значительными уязвимостями, создающими простор для деятельности потенциальных злоумышленников. Возросла роль финансового фактора, увеличилась дистанция в оплате вышестоящего и нижестоящего персонала промышленного предприятия, как следствие, усилились фактор обиды и попытки нанесения вреда как предприятию, так и отдельному лицу.

Указанные и ряд других факторов создали основу по увеличению не только потенциальных, но и фактических возможностей роста внутренних угроз. В силу разных причин, одной из которых является нежелание "выносить сор из избы", до некоторого времени усиление факторов внутренних угроз замалчивалось. Однако за последнее время появилось достаточно информации по данному вопросу, в результате чего стало ясно, что наличие внутренних угроз является не только потенциальным, но и реальным орудием, успешно используемым злоумышленником. Из-за специфичности вопроса нет точной статистики влияния внутренних угроз, однако появляющаяся системно-обобщающая информация показывает, что данные угрозы стали играть далеко не второстепенную, а во многих случаях и первостепенную роль.

Обобщение международной и российской практики в области управления ИБ убеждает в том, что основными задачами системы обеспечения ИБ любого предприятия являются создание стабильной, эффективной торговой и производственной деятельности всех подразделений, защита от потерь, краж, искажения и уничтожения служебной информации, хищения финансовых средств, предотвращение угроз безопасности. Система ИБ необходима также для повышения качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Для достижения вышеперечисленных целей необходимо категорирование информации на служебную или коммерческую тайну, прогнозирование и своевременное выявление угроз безопасности, причин и условий, способствующих нанесению финансового, материального и морального ущерба, создание условий деятельности с наименьшим риском реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба, а также создание механизма и условий для эффективного реагирования на угрозы ИБ на основе правовых, организационных и технических средств.

Поступила в редакцию 04.07.2011 г.