ИНФОРМАЦИОННАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ДОМИНИРУЮЩИЙ ИСТОЧНИК УГРОЗЫ

В.Н. Ершов,
кандидат технических наук, доцент кафедры бизнес-информатики Костромского государственного университета им. Н.А. Некрасова
E-mail: yvn@mail.ru

П.Л. Смирнова,
студент магистратуры Костромского государственного университета им. Н.А. Некрасова
E-mail: perovapol@gmail.com
Адрес: г. Кострома, ул. 1 Мая, д. 14

Закон «О персональных данных» вызывает много споров и обсуждений. Во многом это объясняется неоднозначной, а иногда и недостаточной методологической базой, описывающей процедуру построения системы защиты. В конечном итоге, доказывать адекватность и достаточность принятых мер предстоит оператору персональных данных. В статье предлагается методика определения актуальных угроз информационной безопасности с явным учетом модели нарушителя, что позволяет повысить эффективность системы защиты и более аргументировано обосновать принятые меры.

Ключевые слова: информационная безопасность, персональные данные, модель угроз, модель нарушителя.

Практически каждая организация ведет обработку персональных данных физических лиц, и поэтому, в соответствии с федеральным законом №152 «О персональных данных», является операторами персональных данных. По требованиям ФЗ-152 обеспечение безопасности обработки персональных (ПД) является задачей оператора, а учитывая возможные меры наказания и необходимым условием существования организации.

Для разработки системы защиты можно использовать несколько вариантов: воспользоваться услугами сторонней специализированной фирмы, создать систему защиты собственными силами и комбинированный, когда часть работ делается собственными силами, часть отдается на аутсорсинг. Каждый вариант имеет свои плюсы и минусы. Первый вариант может быть использован практически всеми компаниями. В этом случае, как правило, вместе с разработкой системы делегируется ответственность за правильность ее разработки. Второй вариант, удобен организациям, у которых уже имеются собственные службы

безопасности или специалисты по ИБ, либо их планируется создать. Третий вариант бюджетнее первого, за счет того, что часть работ выполняется собственными силами, но высока вероятность появления «лоскутности» в проектируемой системе. При выборе, для большинства фирм, решающим фактором является сумма затрат на разработку системы.

Для компаний среднего, и тем более малого бизнеса привлечение сторонней организации, способной провести аудит системы безопасности, спроектировать систему защиты, разработать пакет нормативной документации в соответствии с законодательством, является крайне затратным. Реализация защиты своими силами (при отсутствие штатного специалиста) требует базовых знаний по информационной безопасности, много времени на изучение законодательства, его требований, проработку механизмов, гарантирующих соблюдения этих требований, реализации этапов построения системы защиты. И это не смотря на то, что большинство этапов разработки системы защиты носят алгоритмический характер, достаточно однозначны и написаны в виде методических рекомендаций [1].

Таким образом, руководителям приходится выбирать между найм ом дорогостоящих специалистов, выделением ресурсов на самостоятельную разработку системы защиты или нарушением закона со всеми вытекающими последствиями.

Основу построения системы защиты составляет построение дерева актуальных угроз.

Методика ФСТЭК, опубликованная в документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 года [15], достаточно полно описывает алгоритм выявления актуальных угроз информационной безопасности и построения модели угроз информационной безопасности.

«Методика определения актуальных угроз» предоставляет дерево всех возможных угроз, универсальных для любой информационной системы, а так же механизм определения веса каждой угрозы применительно к конкретной организации. В результате применения методики ФСТЭК, угрозы сортируются по весам, и делятся на актуальные, защита которых является первостепенной и обязательной, и на неактуальные, защитой которой можно пренебречь.

ФСТЭК России определяет основные методы защиты от угроз в документах со статусом «Для служебного пользования», которые рассылаются по индивидуальному запросу организации. Дополнив этот список мероприятиями, необходимыми для отдельно взятой ИСПДн, можно получить руководство к действию по созданию системы защиты.

Однако что бы определить меры защиты необходимо оценить, от кого защищаться в первую очередь, то есть построить модель нарушителя. Только опираясь на модель нарушителя, можно построить адекватную систему информационной защиты.

К сожалению, в настоящее время среди доступных источников [3, 6, 8, 9, 10, 11] четко прописанных правил для определения модели нарушителя для ИСПДн нет. Поэтому, предложим собственную методику определения модели нарушителя для ИСПДн на основании анализа существующих нормативно-методических документов и доработки предложенных методик.

Известно две формализованные классификации нарушителей, отличающихся набором признаков (*табл. 1*).

Таблица 1.

Таблица учета признаков нарушителей

Признак	ФСТЭК	ФСБ[1]
По отношению к информационной системе	Внешний, внутренний	Внешний, внутренний
По ресурсным возможностям	Внутренний	Внешний, внутренний (ограниченно)
По квалификации	Внутренний, внешний (ограниченно)	-

ФСТЭК и ФСБ России поддерживают суждение о том, что все возможные нарушители первоначально делятся на два класса — внешние, осуществляющие атаки из-за пределов контролируемой зоны, и внутренние, осуществляющие атаки, находясь в пределах контролируемой зоны.

Из документа ФСБ «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 года №149/54-144 следует, что

[1] На основании сведений, полученных из открытых источников информации

различают шесть основных типов нарушителей — Н1, Н2, ..., Н6. Причем, возможности нарушителя Hi+1 включают в себя возможности Hi. Таким образом, нарушители типа Н6 — являются самыми опасными для организации. Так же, мера опасности нарушителей, следуя данной методике, напрямую зависит от его принадлежности к классу внешних или внутренних угроз. Таким образом, в рассматриваемой модели нарушители классов Н1 — Н3 относятся к внутренним, а Н4 — Н6 — к внешним. Внешние угрозы действительно считаются более опасными с точки зрения причинения возможного ущерба [12, 13], однако, исходя из данных статистики, информационные ресурсы на порядок чаще подвергаются нападениям со стороны внутренних нарушителей [12, 14], а поэтому умалять их опасность по сравнению с внешними не стоит.

ФСТЭК выделяет восемь категорий внутренних нарушителей, ранжируя их по возрастанию возможностей, а, соответственно, и по возрастанию степени опасности. Однако, метода для выявления прямых зависимостей типа «угроза — нарушитель», с вытекающей из них вероятной опасностью не существует, поэтому модель актуальных угроз строится на основе интуитивного перебора всех возможных нарушителей относительно отдельно взятой угрозы. Для внешних нарушителей подробной классификации не выделяется, и, следовательно, не производится изучение возможностей этих нарушителей, что в конечном итоге может стать узким местом в системе защиты.

Совместив описанные методики, предлагается ввести следующие характеристики, позволяющие построить модель внешнего и внутреннего нарушителя организации (*табл. 2*).

Из приведенного выше перечня нарушителей каждой организации целесообразно выбрать для себя актуальную модель нарушителя, определив возможность реализации угроз группами потенциальных нарушителей, приведенными в *табл. 2.* Итоговым значением выбранной модели нарушителя будет являться совокупность идентификаторов самых опасных внешних и внутренних нарушителей, характерных для рассматриваемой системы. Например, OutH3, InH5. Однако, формального определения этой модели недостаточно. На наш взгляд, правильным будет корректировать актуальность каждой угрозы с явным учетом характерной для нее модели нарушителя. Для этого, предлагается определять актуальность угроз, совершенных конкретным нарушителем по методике, аналогичной методике определения актуальных угроз по ФСТЭК России, внеся некоторые изменения.

По методике, описанной в документе «Методика определения актуальных угроз» [15] для определения актуальных угроз необходимо сначала посчитать коэффициент реализуемости каждой угрозы по формуле:

$$Y = (Y_1 + Y_2)/20, \qquad (1)$$

Таблица 2.

Характеристики возможных нарушителей организации

Внешние нарушители		Внутренние нарушители	
OutH1	Лица, имеющие санкционированный доступ в периметр защиты: зарегистрированный пользователь, физическое лицо и т.д.	**InH1**	Лица, имеющие санкционированный доступ в периметр защиты, но не имеющие доступа к ИСПДн: уборщица, охрана, персонал и т.д.
OutH2	Лица, не имеющие санкционированный доступ в периметр защиты: гость (незарегистрированный пользователь), хакеры-самоучки и т.д.	**InH2**	Зарегистрированные пользователи, ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места: пользователь, оператор и т.д.
OutH3	Недобросовестные партнеры	**InH3**	Зарегистрированные пользователи, ИСПДн, осуществляющие удаленный доступ к ресурсам ИСПДн по локальным или распределенным ИС: продвинутый пользователь и т.д.
OutH4	Конкуренты, сторонние организации	**InH4**	Зарегистрированные пользователи с полномочиями администратора безопасности фрагмента ИСПДн
OutH5	Криминальные структуры, разведывательные службы	**InH5**	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн
OutH6	Иностранные государства, государственные структуры.	**InH6**	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн, программисты-разработчики ИСПДн, лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн

где Y – показатель реализуемости угрозы, Y_1 – показатель исходной защищенности информационной системы, Y_2 – числовой коэффициент, соответствующий вероятности возникновения угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Под числовым коэффициентом, соответствующим вероятности реализации угрозы понимается определяемый экспертным путем показатель в десятибалльной шкале, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях.

Полученному количественному коэффициенту возможности реализации угрозы ставится в соответствие качественный показатель, по правилам определенным методикой ФСТЭК.

Далее, необходимо определить опасность каждой угрозы, разбив их на три группы – с низкой, средней и высокой опасностью в зависимости от возможных последствий реализации угрозы.

Непосредственный выбор актуальных угроз происходит, согласно правилам, описанным в *табл. 3*, опирающихся на принцип Парето. Защита только от актуальных угроз позволяет экономить временные и материальные ресурсы реагируя только на те, что представляют реальную опасность.

Таблица 3.

Правила отнесения угрозы безопасности к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Очевидно, что представленная методика ФСТЭК не позволяет явно учитывать модель нарушителя. Косвенно модель нарушителя учитывается при определении показателя реализуемости, когда сопоставляются конкретная угроза с некой воображаемой совокупностью нарушителей, характерной для организации. Таким образом, нарушитель никак не влияет на показатели опасности угрозы и степени исходной защищенности. В первом случае, показатель не зависит от вида нарушителя, его реализующего, так как он учитывает непосредственно ущерб от успешной реализации угрозы, при этом неважно кто эту угрозу совершил. Во втором случае, для показателя необходима только общая картина возможных нарушителей, которая в полной мере определяется методикой. Однако, на наш взгляд, вид нарушителя напрямую определяет вероятность реализации угрозы, поэтому необходимо учитывать доминирующий источник угрозы.

Рассмотрим на конкретном примере, каким образом учет модели нарушителя влияет на отбор актуальных угроз.

Например, в качестве угрозы возьмем поломку оборудования ИСПДн в средней школе, где хранится информация о посещении занятий школьниками. Ввод данных осуществляется один раз в неделю, в удобное для персонала время. В ходе аудита было определено, что исходная защищенность рассматриваемой информационной системы средняя, то есть $Y_1 = 5$. Оценим данную угрозу по методике ФСТЭК. Взвесив вероятность реализации угрозы всеми возможными лицами, присвоим ей значение «средняя», то есть $Y_2 = 5$. По формуле (1), определяющей реализуемость угрозы, получается $Y = 0{,}5$, то есть степень реализуемости – средняя. Для выяснения опасности данной угрозы, оценим вероятный урон в случае успешной реализации данной угрозы. Получили значение «низкий», так как поломка оборудования приведет всего лишь к временному ограничению доступности сведений ИСПДн, что не является критичным в рассматриваемом примере. По *табл. 3* получаем, что угроза поломки оборудования неактуальна, то есть нет необходимости принимать дополнительные меры защиты.

Теперь посмотрим, каким образом внедрение модели нарушителя может повлиять на конечный результат. Так как в примере рассматривается одна и та же информационная система, степень исходной защищенности не изменится, т.е. Y_1=5 и показатель опасности угрозы останется по прежнему низким. Определяя вероятность реализации угрозы, каждый раз будем принимать во внимание конкретную группу нарушителей, характерную для нашей ИСПДн. Допустим, нашей моделью нарушителя является следующая комбинация (*см. табл. 2*): InH1, InH2, InH5, InH6, Out H1, Out H2, Out H3. Поэтому, будем рассматривать вероятность реализации угрозы поломки оборудования относительно каждой из этих групп (*табл. 4*).

Таблица 4.

Градация вероятностей реализации угрозы «Поломка оборудования» нарушителем

ID	Группа нарушителей	Коэффициент вероятности реализации
InH1	Уборщица, охранник, сотрудник не имеющий прав доступа к ИСПД	10
InH2	Пользователи ИСПДн, операторы ИСПДн	5
InH5	Системный администратор ИСПДн	0
InH6	Администратор безопасности ИСПДн, программисты-разработчики ИСПДн, лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн	0
Out H1	Лица, имеющие санкционированный доступ в периметр защиты: зарегистрированный пользователь, физическое лицо	0
Out H2	Лица, не имеющие санкционированный доступ в периметр защиты: гость (незарегистрированный пользователь), хакеры-самоучки	2
Out H3	Недобросовестные партнеры	0

Оценка вероятности реализации для группы InH1 объясняется тем, что в ходе опроса выяснилось, что в данной организации уборку в помещении, где стоит сервер, осуществляет уборщица под присмотром охранника. Как следствие, велика вероятность разрыва или отсоединения коммутирующих проводов.

Как видно из таблицы, одна и та же угроза относительно разных групп нарушителей имеет разную степень вероятности реализации. Соответственно и возможность реализации угрозы для представленных групп нарушителей будет разной (*табл.5*).

Сопоставляя полученные результаты, получим актуальную угрозу «Поломка оборудования» при реализации ее группой нарушителей InH1. Для всех остальных групп нарушителей угроза неактуальна. Следовательно, необходимо принимать меры защиты от реализации рассматриваемой угрозы обслуживающим персоналом. При необходимости, можно привести пример, когда актуальная угроза при разложении по моделям нарушителей для наиболее высокой группы становится неактуальной. В этом случае, мы имеем возможность сократить издержки на реализацию мер защиты.

Приведенный пример показывает необходимость использования модели нарушителя при оценке актуальности угроз, как она позволяет подробно изучить угрозу, рассмотреть вероятность ее реализации всеми объективно значимыми группами нарушителей, и, выявив , как доминирующие источники угрозы, более точно определить возможность её реализации.

Таблица 5.

Возможность реализации угрозы «Поломка оборудования» нарушителем

ID	Группа нарушителей	Возможность реализации	
InH1	Уборщица, охранник, сотрудник не имеющий прав доступа к ИСПД	0,75	Высокая
InH2	Пользователи ИСПДн, операторы ИСПДн	0,5	Средняя
InH5	Системный администратор ИСПДн	0,25	Низкая
InH6	Администратор безопасности ИСПДн, программисты-разработчики ИСПДн, лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн	0,25	Низкая
Out H1	Лица, имеющие санкционированный доступ в периметр защиты: зарегистрированный пользователь, физическое лицо	0,25	Низкая
Out H2	Лица, не имеющие санкционированный доступ в периметр защиты: гость (незарегистрированный пользователь), хакеры-самоучки	0,35	Средняя
Out H3	Недобросовестные партнеры	0,25	Низкая

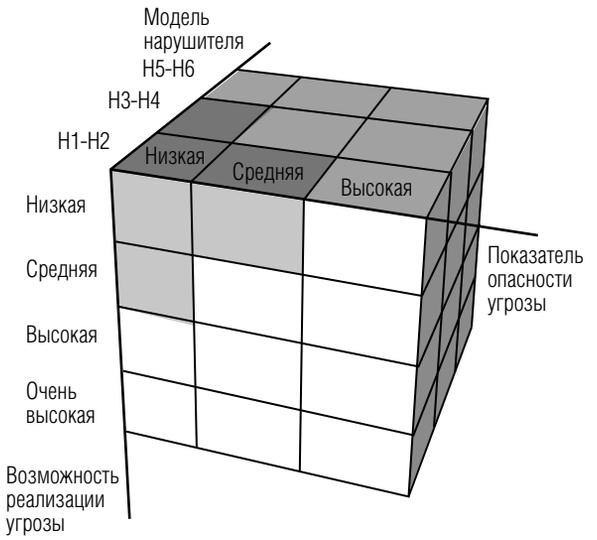

Рис. 1. Трехмерная структура системы информационной безопасности персональных данных

Для введения в методику ФСТЭК модели нарушителя предлагаем параметр вероятности возникновения угрозы заменить на соответствующий ему показатель вероятности реализации угрозы нарушителем. Исходя из этого, выбор актуальных угроз возможно осуществлять на основе гиперкуба (*рис. 1*).

Итак, по нашему мнению, выбор актуальных угроз безопасности необходимо осуществлять на основе оценки вероятности реализации одной и той же угрозы всеми возможными группами нарушителей, то есть с учетом доминирующих источников угроз. Следовательно, строить систему защиты, способную адекватно нейтрализовать выявленные уязвимости можно только на этом основании. Конечно, учет доминирующих источников требует больших временных затрат при проектировании системы, однако позволяет сократить издержки при её реализации. ■

Литература

1. Смирнова П.Л. Анализ процесса подготовки организационно-распорядительных документов согласно федеральному закону №152 // Всероссийский конкурс научно-исследовательских работ студентов и аспирантов в области информатики и информационных технологий в рамках всероссийского фестиваля науки 7 - 9 сентября 2011 г. Том 2 / Отв. ред. В.В. Серебровский. Белгород, 2011. С. 368-375.
2. Федеральный Закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.).
4. Порядок проведения классификации информационных систем персональных данных (утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20).
5. Смирнова П.Л. Влияние организационной культуры на актуальность угроз информационной безопасности // Экономическая наука – хозяйственной практике: материалы научной сессии XIII Международной научно-практической конференции, Кострома 14-15 октября / Отв. ред. Н.В. Исаев. Кострома: КГУ имени Н.А. Некрасова, 2011. С. 496-503.
6. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/54-144).
7. Герчиков В.И. Управление персоналом: работник – самый эффективный ресурс компании: Учебное пособие для вузов. М.: ИНФРА-М, 2008.
8. Домарев В.В. Безопасность ИТ. Системный подход. Киев: ДиаСофт, 2004.
9. Астахов А. Искусство управления информационными рисками. М.: ДМК Пресс, GlobalTrust, 2009.
10. Белов Е.Б., Лось В.П., Мещеряков Р.В, Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов. М: Горячая линия – Телеком, 2006.
11. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. 2-е изд. М.: Академический Проект; Гаудеамус. 2004.
12. Марчук В. Основы информационной безопасности для руководителя небольшой компании // Microsoft MVP Enterprise Security. – 8.07.2011. URL: http://www.securitylab.ru/analytics/406256.php
13. Сычев А., Кузнецов Д. Анализ проблем защиты от внешнего нарушителя // ИнформКурьер-Связь. 2010. №№ 7-8. URL: http://www.securitylab.ru/analytics/397848.php
14. Инсайдерские угрозы в России 2009. URL: http://www.securitylab.ru/analytics/368176.php
15. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Зам. директора ФСТЭК России 14 февраля 2008 г.)