УДК 004.056.53

М.М. Бусько

АНАЛИЗ МЕТОДИЧЕСКОЙ БАЗЫ ОПРЕДЕЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разработка и построение модели угроз безопасности информации является важным, а в некоторых случаях обязательным элементом в системе информационной безопасности. На основе модели угроз определяются требования к применяемым мерам по защите информации. В статье сделан анализ методик, стандартов, алгоритмов по оценке угроз, с целью определения наиболее приемлемого подхода для практического применения. В результате анализа выявлено, что наиболее качественным документом для практического применения при моделировании угроз безопасности информации является проект «Методики определения угроз безопасности информации в информационных системах» ФСТЭК. Однако процесс, представленный в методике является весьма трудоемким и требует создания экспертной группы достаточно высокой квалификации. Применение математических методов с последующей программной реализацией решит проблемы трудоемкости и экспертной субъективности.

Ключевые слова: угроза информационной безопасности; модель угроз; риск информационной безопасности; методика оценки риска; оценка актуальности угрозы.

M.M. Busko

ANALYSIS OF THE METHODICAL BASE FOR DETERMINING INFORMATION SECURITY THREATS

The development and construction of a model of information security threats is an important and in some cases a mandatory element in an information security system. Based on the threat model, the requirements for applicable measures to protect information are determined. The article analyzes the methods, standards, and algorithms for assessing threats in order to determine the most appropriate approach for practical use. The result of the analysis, it was revealed that the most qualitative document for practical use in modeling information security threats is the project «Methods for determining information security threats in information systems» of the FSTEC. However, the process presented in the methodology is very time consuming and requires the creation of an expert group of sufficiently high qualification. The use of mathematical methods with the subsequent software implementation will solve the problems of labor-intensiveness and expert subjectivity.

Keywords: information security threat; threats model; information security risk; risk assessment methodology; assessment of the relevance of the threat.

В настоящее время деятельность любой организации связана с использованием больших объемов информации. Рано или поздно встает вопрос защиты информационных активов. Даже если и не используется информация ограниченного доступа потеря целостности или доступности ценной информации может привести к значительным негативным последствиям. Состояние защищен-

ности, т.е. информационная безопасность (ИБ) организации, подразумевает внедрение адекватных мер защиты способных нейтрализовать угрозы, которые влекут неприемлемый ущерб для организации. Соответственно вторым шагом при построении системы защиты информации, после идентификации и определения ценности информационных активов (далее – активов), является выявление угроз, подлежащих нейтрализации. Формализованным описанием свойств и характеристик угроз безопасности информации является модель угроз. Модель угроз необходима для определения требований к системе защиты. Разработка модели угроз в определенных случаях является обязательным условием. Так в соответствии с п. 2 ст. 19 ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз, т.е. разработкой модели угроз [1]. Определение угроз безопасности информации, и разработка на их основе модели угроз обязательное требование, установленное в отношении государственных информационных систем приказом ФСТЭК № 17 от 11.02.2013 г. [2, п. 14]. В соответствии с п. 11а приказа ФСТЭК № 239 от 25.12.2017 г. создание подсистемы безопасности значимого объекта критической информационной инфраструктуры должно включать анализ угроз безопасности информации и разработку модели угроз безопасности информации [3]. Приказ ФСТЭК № 31 от 14.03.2014 г. распространяет такое требование на автоматизированные системы управления производственными и технологическими процессами (АСУ ТП) [4, п. 13]. В остальных случаях моделирование угроз не является обязательным, но с точки зрения здравого смысла дает возможность специалисту по защите информации получить достаточно убедительные доводы для обоснования необходимых мер защиты.

Проблема информационной безопасности в условиях цифровизации экономики является актуальной и востребованной на сегодняшний день, о чем свидетельствуют труды и исследования ученых в этой сфере [16–19]. В настоящей работе сделана попытка определения наиболее приемлемой для практического применения методики моделирования угроз безопасности информации. Все существующие методики, стандарты, алгоритмы по оценке угроз можно разделить на две группы: основанные на оценке рисков ИБ и основанные на оценке актуальности угроз. Рассмотрим подробнее каждую группу.

Согласно ГОСТ Р ИСО 31000-2010 вся деятельность организации включает в себя риск [5]. При этом любой риск идентифицированный, оцененный и проанализированный управляем достаточно только установить его критерии и определить воздействия для его изменения. Оценка и анализ рисков ИБ рассматривается с точки зрения тесной зависимости деловой деятельности организации от информационных активов и соответственно от их безопасности. Соответственно риск нарушения информационной безопасности может привести к ущербу в том числе и финансовым потерям. Многие вопросы по определению и количественной оценке степени риска в любой сфере деятельности остались не изученными. Поэтому в настоящее время можно говорить лишь о существовании частичной качественной оценки степени риска предприятия в условиях России и о применении неадаптированных зарубежных методиках по определению и количественной оценке степени рисков предприятия [6]. Не яв-

ляется исключением риск информационной безопасности, вопросы его оценки освещены в основном в международных стандартах ИСО, рассматривающих деятельность по оценке риска частью его менеджмента.

Можно назвать ряд стандартов, предписывающих выбор и применение защитных мер осуществлять на основании определенной методологии управления рисками. Это стандарты ГОСТ Р ИСО/МЭК 13335-1 [7], ГОСТ Р ИСО/МЭК ТО 13335-5-2006 [8]. Выбор же подхода к методологии менеджмента риска осуществляется организацией и зависит, например, контекста менеджмента риска или сферы деятельности. Согласно ГОСТ Р ИСО/МЭК 27002-2012 оценка рисков должна включать систематический подход, заключающийся в количественной оценке рисков (анализ риска), и процесс сравнения количественно оцененных рисков с критериями значимыми для организации [9]. При этом риск информационной безопасности согласно [7] характеризуется комбинацией двух факторов: вероятностью возникновения инцидента и его разрушительным воздействием. В [8] представлены виды риска безопасности, с которыми может встретиться организация. Все перечисленные стандарты лишь поверхностно рассматривают основные аспекты информационной безопасности, носят общий характер и имеют низкую практическая ценность.

Выделяется из этого ряда ГОСТ Р ИСО/МЭК 27005-2010 [10]. В стандарте сформирована четкая концепция ИБ и начинают выделяться конкретные требования и рекомендации для практического применения. Обозначено, что риск измеряется исходя из комбинации последствий, вытекающих из нежелательного события и вероятности возникновения события. Установление значения риска может быть качественным, количественным или комбинированным, в зависимости от обстоятельств. Рекомендуется использовать качественные значения для получения общих сведений об уровне риска и затем переходить к количественным оценкам, как к более детальным. Сначала проводятся качественные оценки последствий (ценности активов) и степени вероятности возникновения угрозы затем им в соответствие ставятся численные значения по заранее определенной шкале. Количественное значение риска вычисляется путем умножения значения последствий и вероятности. К недостаткам подхода по оценке риска представленного в ГОСТ Р ИСО/МЭК 27005-2010 можно отнести следующие:

– отсутствуют рекомендации по формированию количественных шкал для последствий и вероятности инцидентов информационной безопасности;

– все оценки производятся на основании опросных листов, но отсутствуют практические рекомендации по их составлению и обработке;

– не определены лица, осуществляющие оценку и их квалификация.

Таким образом ГОСТ Р ИСО/МЭК 27005-2010 с практической точки зрения может рассматриваться, как хорошее методическое пособие для разработки собственной методики оценки риска информационной безопасности.

Следующим стандартом моделирования угроз на основе риска является Методика от Центрального банка РФ РС БР ИББС-2.2-2009 [11]. Оценка риска включает выполнение шести процедур:

– определение перечня типов информационных активов;

– определение перечня типов объектов среды в которых используются информационные активы;

– определение источников угроз;

– определение степени вероятности реализации угроз;

– определение степени тяжести последствий нарушения ИБ;

– оценка рисков нарушения ИБ.

Риск определяется на основании качественных экспертных оценок степени вероятности реализации угроз и степени тяжести последствий. Риски могут быть определены в количественной форме причем в денежном выражении. Имеется рекомендуемая шкала соответствия численным показателям. Явным преимуществом методики является оценка последствий путем анализа потери свойств ИБ (конфиденциальности, целостности и доступности) для каждого актива. Методика также содержит подробные рекомендации по формированию экспертной группы. В результате анализа РС БР ИББС-2.2–2009 можно сделать вывод, что методика имеет высокую практическую значимость, можно получить как качественные оценки, так и количественные оценки, имеются шаблоны, которые регламентируют результат работы каждой процедуры оценки рисков. Из недостатков стоит отметить то, что модель угроз формируется отдельно от процесса оценки. Для широкого применения данная методика малопригодна в силу узкой направленности стандарта на банковскую систему, в качестве информационных активов в основном рассматривается информация обеспечения банковских технологических операций. Отсюда и оценка последствий выражается в денежной форме, ущерб социальный, политический, репутационный, технологический, субъекту персональных данных (ПДн) по такой шкале оценить проблематично.

Подводя итог анализа методик моделирования угроз информационной безопасности основанных на риске можно утверждать, что наибольшей практической значимостью обладает стандарт Центрального банка РФ РС БР ИББС-2.2–2009. Однако применение его к областям вне банковской деятельности требует серьезной адаптации.

Рассмотрим вторую группу методик моделирования и анализа угроз, основанную на оценке актуальности угроз.

На сегодняшний день имеется две утвержденные ФСТЭК методики по моделированию угроз – это «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год» [12] и «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры». Второй документ имеет гриф «Для служебного пользования» и не может претендовать на практическое руководство для применения широким кругом пользователей в силу ограничения доступа к нему. Можно также добавить, что это сугубо специфический документ, направленный на моделирование угроз для АСУ ТП. Обеспечение безопасности обрабатываемой информации в таких системах заключается в первую очередь в обеспечении доступности и ее целостности и только при необходимости конфиден-

циальности. Такой подход не применим для информации ограниченного доступа, например, к персональным данным, коммерческой тайне и др.

Проанализируем применимость первого документа [12] регулятора к любой информации идентифицированной, как актив имеющий ценность для обладателя. Согласно данной методике составляется полный перечень угроз исходя из наличия источника угрозы и уязвимого звена. Перечень составляется на основе экспертного метода, в том числе путем опроса специалистов. Затем оценивается актуальность угроз. Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность для персональных данных (актива) [12]. Другими словами, мера актуальности – это функция двух аргументов: возможности реализации угрозы и опасности для актива. Возможности реализации согласно документу [12], соответствует коэффициент реализуемости угрозы, который рассчитывается на основе двух показателей: уровня исходной защищенности ИС (Y_1) и частоты (вероятности) реализации рассматриваемой угрозы (Y_2):

$$Y = (Y_1 + Y_2) / 20 .$$

Уровень исходной защищенности ИС это обобщенный показатель и зависит от технических и эксплуатационных характеристик ИС, перечисленных в методике. Всего представлено семь групп характеристик каждая из них имеет три уровня защищенности – высокий, средний и низкий. На основании суммирования положительных решений по каждому уровню определяется обобщенный показатель. Частота (вероятность) реализации угрозы определяется экспертным путем в качественных оценках с последующим переходом к соответствующим числовым значениям. Оценка опасности каждой угрозы производится так же на основе опроса экспертов и имеет вербальные градации. Далее определяется актуальность на основании матрицы соотнесения возможности реализации угроз и показателя опасности угроз.

Методика, представленная в [12] достаточно проста в применении, и имеет конкретные требования и рекомендации для практического применения. Вместе с тем следует отметить, что она предназначена только для определения угроз ПДн и ИСПДн. В информационных системах эксплуатируемые в различных организациях не всегда могут обрабатываться ПДн. Соответственно моделирование угроз должно применятся и для иной информации, в том числе для общедоступной и информации подлежащей обязательному опубликованию. Предлагаемая вербальная шкала оценки опасности каждой угрозы имеет критерии: незначительные негативные последствия, негативные последствия и значительные негативные последствия. Такие размытые критерии явно приведут к субъективным экспертным оценкам.

Имеется еще один документ, разработанный ФСТЭК пока еще не получивший официального статуса это проект «Методики определения угроз безопасности информации в информационных системах». Методика предусматривает идентификацию каждой угрозы. Идентифицированная угроза безопасности информации подлежит нейтрализации (блокированию), если она является актуальной для информационной системы [13]. Оценка актуальности угрозы рас-

сматривается как двухкомпонентный вектор, первый компонент которого характеризует вероятность реализации угрозы, а второй – степень возможного ущерба в случае ее реализации [13]. При этом вероятность может оцениваться либо на основе использования статистических данных, если они есть либо определением возможности реализации, которая зависит от исходной защищенности информационной системы и потенциала нарушителя. Ущерб, который может причинить реализованная угроза рассматривается с позиции нарушения свойств ИБ (конфиденциальности, целостности и доступности). При этом рассматриваются различные виды негативных последствий для обладателя информационного актива, а именно экономические (финансовые), социальные, политические, репутационные, технологические, субъекту персональных данных. В документе приводятся рекомендации по формированию экспертной группы, а именно кого следует включать в состав, количество экспертов, квалификация. Для снижения уровня субъективности и неопределенности описано проведение оценок по методу Дельфи, что снижает зависимость от человеческого фактора. Однако отмечается большая трудоемкость практического применения методики, анализ угроз вручную становится фактически нереальным либо нерентабельным [14; 15]. Подведем итог проведенного анализа и сведем все результаты в таблицу.

Результаты анализа

Наименование документа	Выходной параметр	Полнота и структурированность алгоритма оценки	Практическая значимость	Итоговый результат
ГОСТ Р ИСО/МЭК 13335-1 ГОСТ Р ИСО/МЭК 13335-5	Риск	Алгоритм отсутствует	Низкая	Не регламентировано
ГОСТ Р ИСО/МЭК 27002	Риск	Ограничивается перечислением параметров влияющих на риск	Низкая	Предписывает количественную оценку, но не регламентирует
ГОСТ Р ИСО/МЭК 27005	Риск	Алгоритм структурирован, не определены вопросы: формирования количественных значений, обработки опросных листов, требований к экспертам	Имеет практическую значимость для разработки собственной методики	Качественная оценка и количественные оценки
РС БР ИББС-2.2–2009	Риск	Четко структурированный алгоритм, необходима адаптация для активов имеющих не финансовую ценность	Высокая для банковского сектора	Качественная и количественная оценки
Методика определения актуальных угроз безопасности персональных данных при их обработке в инфор-	Актуальность угрозы	Четко структурированный алгоритм, не определены требования к экспертам. Критерии оценки опасности угрозы нечеткие	Высокая для ПДн	Качественная и количественная оценки

Наименование документа	Выходной параметр	Полнота и структурированность алгоритма оценки	Практическая значимость	Итоговый результат
мационных системах персональных данных				
Методики определения угроз безопасности информации в информационных системах (проект)	Актуальность угрозы	Алгоритм четко структурирован, но весьма трудоемкий	Высокая	Качественная и количественная оценки

Проведенный анализ позволяет сделать вывод, что наиболее качественным документом для практического применения при моделировании угроз безопасности информации является проект «Методики определения угроз безопасности информации в информационных системах» ФСТЭК. Документ по этапам подробно описывает процедуру определения актуальных угроз, подлежащих включению в модель угроз и нейтрализации. Трудоемкость же процесса оценки компенсируется четкой структуризацией, которая может способствовать применению математических методов.

Очевидно, что, имея математический аппарат его можно реализовать программно и весь процесс моделирования угроз автоматизировать. Кроме решения проблемы трудоемкости, также может быть решена проблема экспертной субъективности.

Список использованной литературы

1. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 г. № 152-ФЗ (ред. от 31.12.2017 г.) / Официальный сайт компании «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801.

2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс] : приказ ФСТЭК России от 11.02.2013 г. № 17 (ред. от 15.02.2017 г.) (зарег. в Минюсте России 31.05.2013 г. № 28 608) / ФСТЭК России. – Режим доступа: https://fstec.ru/component/attachments/download/566.

3. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : приказ ФСТЭК России от 25.12.2017 г. № 239 (ред. от 09.08.2018 г.) (зарег. в Минюсте России 26.03.2018 г. № 50524) / ФСТЭК России. – Режим доступа: https://fstec.ru/en/component/attachments/download/1879.

4. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жиз-

ни и здоровья людей и для окружающей природной среды [Электронный ресурс] : приказ ФСТЭК России от 14.03.2014 г. № 31 (ред. от 09.08.2018 г.) (зарег. в Минюсте России 30.06.2014 г. № 32919) / ФСТЭК России. – Режим доступа: https://fstec.ru/component/attachments/download/718.

5. ГОСТ Р ИСО 31000-2010. «Менеджмент риска. Принципы и руководство» (утв. и введен в действие приказом Росстандарта от 21.12.2010 г. № 883-ст). – М. : Стандартинформ, 2012.

6. Беликов А.Ю. Теория рисков : учеб. пособие / А.Ю. Беликов // М-во образования РФ, ИГЭА. – Иркутск : Изд-во ИГЭА, 2001. – 95 с.

7. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой)» (утв. и введен в действие приказом Росстандарта от 19.12.2006 г. № 317-ст). – М. : Стандартинформ, 2007.

8. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети» (утв. и введен в действие приказом Росстандарта от 19.12.2006 г. № 317-ст). – М. : Стандартинформ, 2007.

9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (утв. и введен в действие приказом Росстандарта от 24.09.2012 г. № 423-ст). – М. : Стандартинформ, 2014.

10. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утв. и введен в действие приказом Росстандарта от 30.11.2010 г. № 632-ст). – М. : Стандартинформ, 2011.

11. Рекомендация в области стандартизации Банка России. РС БР ИББС-2.2–2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. – М., 2009. – 23 с.

12. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008 г.) [Электронный ресурс] / ФСТЭК России. – Режим доступа: https://fstec.ru/component/attachments/download/290.

13. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс] / ФСТЭК России. Проект. – Режим доступа: http://fstec.ru/component/attachments/download/812.

14. Вихорев С. Не было ни гроша, да сразу алтын... [Электронный ресурс] / С. Вихорев // Сайт АО «ЭЛВИС-ПЛЮС» 20.05.2015. – Режим доступа: https://elvis.ru/competency/expert_comments/1244/.

15. Борисов С. СОИБ. Анализ. Определение угроз безопасности [Электронный ресурс] / С. Борисов // SecurityLab.ru. Часть 1. – Информационный портал. – Режим доступа: http://www.securitylab.ru/blog/personal/sborisov/139182.php.

16. Кузнецова Н.В. Безопасность персонала: терминологический аспект / Н.В. Кузнецова // Известия Иркутской государственной экономической академии. – 2011. – № 5. – С. 99–103.

17. Сачков Д.И. Оценка защищенности персональных данных в информационных системах / Д.И. Сачков, И.Г. Смирнова, В.Н. Быкова // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2015. – Т. 6. – № 3. – С. 21.

18. Шободоева А.В. Развитие понятия «информационная безопасность» в научно-правовом поле России / А.В. Шободоева // Известия Байкальского государственного университета. – 2017. – Т. 27, № 1. – С. 73–78.

19. Якимова Е.М. Правовые способы защиты экономической безопасности предпринимательской деятельности / Е.М. Якимова // Экономическая безопасность: государство, регион, предприятие : сб. ст. 3-й Междунар. науч.-практ. конф. – 2018. – С. 237–240.

Информация об авторе

Бусько Михаил Михайлович – кандидат технических наук, доцент, кафедра математики и информатики, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11, e-mail: buskomm@bgu.ru.

Author

Busko Mikhail Mikhailovich – PhD in Engineering, Associate professor, the Department of Mathematics and Informatics, Baikal State University, 664003, Irkutsk, 11 Lenina St., e-mail: buskomm@bgu.ru.