БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 1 (112). – 42–51

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-1-42-51

ВОПРОСЫ ОРГАНИЗАЦИИ ЭКСПЕРТИЗЫ МОДЕЛИ УГРОЗ*

А.А. АФАНАСЬЕВ

630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: a.afanasev.2019@stud.nstu.ru

В настоящее время существует необходимость разработки модели угроз, регулируемой рядом нормативно-правовых документов, для различных информационных систем, которые подлежат защите в соответствии с текущим законодательством. Сама по себе модель угроз представляет собой документ, основным назначением которого является определение актуальных угроз для конкретной системы. Однако существуют различные типы информационных систем, для каждой из которых задача по составлению модели угроз может иметь разную ресурсоемкость. Также важным аспектом является правильность разработанной модели угроз, поскольку существует закон об ответственности за правонарушения в сфере защиты информации. Исходя из этого возникает потребность в рассмотрении особенностей построения модели угроз для разных типов информационных систем с целью упрощения ее экспертизы. В работе представлен структурированный алгоритм построения модели угроз с особенностями для разных типов информационных систем.

Ключевые слова: защита информации, модель угроз, экспертиза модели угроз, информационная система персональных данных, государственная информационная система

* Статья получена 05 декабря 2023 г.

ВВЕДЕНИЕ

В современном цифровом обществе, в котором информационные технологии проникают во все сферы человеческой деятельности, процесс обеспечения безопасности информации приобретает всё более критическое значение. Многогранные преимущества цифровизации сопряжены с рисками, связанными с угрозами безопасности информации, которые становятся всё более сложными и утонченными. Эти угрозы охватывают различные аспекты информационной безопасности, включая атаки на программные и аппаратные ресурсы, социальную инженерию, фишинг и другие формы манипуляций, направленных на службы и системы обработки данных.

Для обеспечения безопасности информационных систем персональных данных [1], государственной информационной системы [2], автоматизированных систем, а также управления техническим процессом [3], критической информационной инфраструктуры [4] необходимо создание и регулярное обновление модели угроз в соответствии с нормативно-правовыми документами [5].

Согласно законодательству [6], в модели угроз должно быть описание информационной системы и ее структурно-функциональных характеристик, описание угроз безопасности, включающее описание модели нарушителя, возможных уязвимостей информационной системы, способов реализации угроз и последствий от нарушения свойств безопасности информации.

В связи с этим существует необходимость рассмотрения вопросов по организации экспертизы модели угроз, а именно особенности построения модели угроз, без которой невозможно построить надлежащую систему защиты информации и соответствовать действующей законодательной базе.

1. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Разработка модели угроз производится для разных систем – от ИСПДн до КИИ. В зависимости от системы, для которой разрабатывается модель, меняется список нормативно-правовой документации. Например, при разработке модели угроз для АСУ ТП необходимо руководствоваться приказом ФСТЭК России от 14 марта 2014 г. № 31 [3], отложив приказ ФСТЭК России от 11 февраля 2013 г. № 17 [2] и приказ ФСТЭК России от 18 февраля 2013 г. № 21 [1].

При использовании в системе криптографических средств необходимо руководствоваться нормативными документами ФСБ, регламентирующими

обращение с шифровальными средствами. Если криптосредства не используются в системе, то такие документы не актуальны.

Также стоит обратить внимание на то, что нет необходимости в использовании различных ГОСТов и прочих нормативных документов, не имеющих отношения к моделированию угроз. К тому же стоит обращать внимание на то, не был ли отменен тот или иной документ.

2. АЛГОРИТМ РАЗРАБОТКИ

2.1. ОБЩИЕ ПОЛОЖЕНИЯ

Раздел алгоритма содержит вводную информацию о модели угроз: назначение и область действия документа; различные документы, стандарты и акты, которые используются для оценки угроз и разработки модели угроз; наименование обладателя информации, заказчика, оператора систем и сетей; лица, ответственные за обеспечение защиты информации; наименование организации, привлекаемой для разработки модели угроз при ее наличии.

2.2. ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В этом разделе указываются общие сведения о самой информационной системе: ее название, местоположение, задачи, архитектура, описание групп пользователей, какие данные и какого класса (уровней защищенности, категории) обрабатываются в ней, в целом информация о функционале данной системы. Однако не стоит заниматься переписыванием технических паспортов с указанием серийных номеров различных технических средств. Описание должно быть таким, чтобы человек абсолютно незнакомый с данной системой смог понять принцип ее работы.

2.3. МОДЕЛЬ НАРУШИТЕЛЯ

Модель нарушителя представляет собой описательную модель потенциальных нарушителей, которая классифицируется согласно их опыту, знаниям, возможности использования ресурсов, мотивации и способов осуществления угроз (рисунок) [8].

Тип	Категория	Подготовленность								
		Психофизическая			Техническая			Осведомленность		
		Высокая	Средняя	Низкая	Высокая	Средняя	Низкая	Высокая	Средняя	Низкая
Внешний	Специалист									
	Любитель									
	Дилетант									
Внутренний	Сотрудник									

Составление типовой модели нарушителя

Making a standard model of the violator

Во время разработки модели угроз необходимо провести анализ информационной системы с целью составления примерного списка актуальных нарушителей для данной ИС. К сожалению, конкретных методологий отбора не существует. В соответствии с банком данных угроз нарушители делятся на три типа по уровню опасности:

- низкий – обычный человек вне зависимости от его навыков владения различными инструментами;
- средний – человек, имеющий доступ к некоторым конфиденциальным данным (например, информация о свойствах и данных функционирования ИС);
- высокий – человек или группа лиц, имеющих доступ к разработке и использованию средств эксплуатации уязвимостей (например, спецслужбы).

Также на основании [6] нарушителей подразделяют на внешних нарушителей (тип I) – лиц, которые не имеют доступа к ИС и осуществляют угрозы извне, и внутренних нарушителей (тип II) – лиц, которые имеют единовременный или постоянный доступ к ИС.

Наибольший риск для ИС несут внутренние нарушители [9]. Для оценки их возможностей следует проводить анализ принимаемых мер по допуску лиц для работы с ИС. Внешний нарушитель рассматривается в том случае, когда ИС взаимодействует с другой ИС или пользователями за пределами контролируемой (защищаемой) зоны, другими словами, подключена к сети Интернет.

Если в информационной системе реализовано использование криптографических средств, то для разделов «Обобщенные возможности источников атак» и «Реализации угроз безопасности информации, определяемых по возможности источников атак» все исходные данные и таблицы данных разделов находятся в нормативном документе ФСБ «Методические рекомендации по

разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России от 31 марта 2015 г. №149/7/2/6-432). Конечная цель разделов алгоритма заключается в установке класса средств криптографической защиты информации (СКЗИ), который напрямую зависит от возможностей нарушителя и устанавливается в соответствии с Приказом ФСБ от 10 июля 2014 г. № 378 [7], но только для персональных данных, для других видов информации таких требований нет.

2.4. ВОЗМОЖНЫЕ УЯЗВИМОСТИ

Так как по своей сути раздел с моделью угроз является документом, которому свойственна статичность со своими подлежащими изменениями, то решение составлять список уязвимостей при помощи сканера угроз будет иметь неточный результат из-за динамичности результатов сканера. Лучшим решением будет представление списка возможных уязвимостей в формате классов уязвимостей для каждой конкретной информационной системы. Для этого нужно воспользоваться ГОСТ Р 56546–2015, классифицирующим угрозы и уязвимости относительно: области происхождения, типов недостатков ИС, места возникновения уязвимости.

2.5. ОПАСНОСТЬ УГРОЗ

В разделе описывается «определение последствий от нарушения свойств безопасности информации». Существует три типа опасности угрозы: низкая, средняя или высокая. Тип зависит от степени негативности последствий. Методикой не оговорено, должна ли опасность угроз определяться один раз или быть константой для всех угроз. Представлен подход по определению опасности угроз в зависимости от нарушения конфиденциальности, целостности или доступности при реализации конкретной угрозы [10].

В предложенном подходе негативные последствия не зависят от способа нарушения конфиденциальности, целостности и доступности. К примеру, по факту утечки персональных данных из базы неважен способ нарушения конфиденциальности.

2.6. ОПИСАНИЕ УГРОЗ

Раздел алгоритма со способами реализации угроз заполняется с использованием банка данных угроз ФСТЭК. Способы реализации указаны в текстовом блоке «Описание угрозы».

ЗАКЛЮЧЕНИЕ

Модель угроз – это структурированное представление всей информации, влияющей на безопасность информационной системы, которое включает в себя расчет вероятности воплощения угроз, а также оценку предполагаемых последствий. По своей сути, это взгляд на приложение и его окружение через призму безопасности.

В настоящей работе представлен алгоритм построения модели угроз различных информационных систем для дальнейшей разработки методики организации экспертизы модели угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 07.03.2024).

2. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-gn-17 (дата обращения: 07.03.2024).

3. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «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 жизни и здоровья людей и для окружающей природ-

ной среды». – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 07.03.2024).

4. Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 07.03.2024).

5. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных». – URL: https://docs.cntd.ru/document/901990046 (дата обращения: 07.03.2024).

6. Методический документ. Методика оценки угроз безопасности информации: утв. ФСТЭК России 5 февраля 2021 г. – URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2169-informatsionnoe-soobshcheniefstek-rossii-ot-15-fevralya-2021-g-n-240-22-690 (дата обращения: 07.03.2024).

7. Приказ ФСБ от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». – URL: https://base.garant.ru/70727118 (дата обращения: 07.03.2024).

8. *Маковский К.Е.* Анализ методик разработки модели угроз и модели нарушителя // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей XXVII Международной научно-практической конференции. – Пенза, 2019. – С. 37–39.

9. *Веденеев И.А., Коновалов М.В.* К вопросу о разработке модели угроз и модели нарушителя с целью создания системы технической защиты информации // Аллея науки. – 2018. – № 10 (26), т. 2. – С. 979–982.

10. *Ерышов В.Г.* Рекомендации по структуре и содержанию современных моделей угроз безопасности информации // Методики фундаментальных и прикладных научных исследований: сборник статей Всероссийской научной конференции. – СПб., 2022. – С. 38–40.

Афанасьев Александр Андреевич, лаборант кафедры зашиты информации Новосибирского государственного технического университета. E-mail: a.afanasev.2019@stud.nstu.ru

DOI: 10.17212/2782-2230-2024-1-42-51

Issues of organization of threat model expertise*

A.A. Afanasev

Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Information Security Department. E-mail: a.afanasev.2019@stud.nstu.ru

Currently, there is a need to develop a threat model regulated by a number of regulatory documents for various information systems that are subject to protection in accordance with current legislation. The threat model itself is a document whose main purpose is to identify current threats to a particular system. However, there are different types of information systems, for each of which the task of compiling a threat model may have different resource intensity. Also, an important aspect is the correctness of the developed threat model, since there is a law on liability for offenses in the field of information protection. Based on this, there is a need to consider the features of building a threat model for different types of information systems in order to simplify its examination. The paper presents a structured algorithm for building a threat model with features for different types of information systems.

Keywords: information protection, threat model, threat model expertise, personal data information system, state information system

REFERENCES

1. Order of the FSTEC of Russia dated February 18, 2013 No. 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems". (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 07.03.2024).

2. Order of the FSTEC of Russia dated February, 2013 No. 17 "On approval of requirements for the protection of information not constituting a state secret contained in state information systems". (In Russian). Available at: https://fstec.ru/

* *Received 05 December 2023.*

normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-gn-17 (accessed 07.03.2024).

3. Order of the FSTEC of Russia dated March 14, 2014 No. 31 "On approval of the requirements for ensuring the protection of information in automated control systems for production and technological processes at critically important facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to life and human health and for the environment". (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed 07.03.2024).

4. Order of the FSTEC of Russia dated December 25, 2017 No. 239 "On approval of requirements for ensuring the safety of significant objects of the critical information infrastructure of the Russian Federation". (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 07.03.2024).

5. Federal Law of the Russian Federation No. 152 of July 27, 2006 "On Personal Data". (In Russian). Available at: https://docs.cntd.ru/document/901990046 (accessed 07.03.2024).

6. Methodological document. Information security threat assessment methodology. Approved by the FSTEC of Russia on February 5, 2021. (In Russian). Available at: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2169-informatsionnoe-soobshcheniefstek-rossii-ot-15-fevralya-2021-g-n-240-22-690 (accessed 07.03.2024).

7. FSB Order No. 378 dated July 10, 2014 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems using cryptographic information protection tools necessary to comply with the requirements established by the government of the Russian Federation for the protection of personal data for each one of the security levels". (In Russian). Available at: https://base.garant.ru/70727118 (accessed 07.03.2024).

8. Makovskii K.E. [Analysis of methods for developing a threat model and an intruder model]. Fundamental'nye i prikladnye nauchnye issledovaniya: aktual'nye voprosy, do-stizheniya i innovatsii [Fundamental and applied scientific research: current issues, achievements and innovations]. Collection of articles of the XXVII International Scientific and Practical Conference. Penza, 2019, pp. 37–39. (In Russian).

9. Vedeneev I.A., Konovalov M.V. K voprosu o razrabotke modeli ugroz i modeli narushitelya s tsel'yu sozdaniya sistemy tekhnicheskoi zashchity informatsii [On the issue of developing a threat model and an intruder model in order to create

a system of technical protection of information.]. Alleya nauki, 2018, no. 10 (26), vol. 2, pp. 979–982. (In Russian).

10. Eryshov V.G. [Recommendations on the structure and content of modern information security threat models]. Metodiki fundamental'nykh i prikladnykh nauchnykh issledovanii [Methods of fundamental and applied scientific research]. Collection of articles of the All-Russian Scientific Conference. St. Petersburg, 2022, pp. 38–40. (In Russian).

Для цитирования:

Афанасьев А.А. Вопросы организации экспертизы модели угроз // Безопасность цифровых технологий. – 2024. – № 1 (112). – С. 42–51. – DOI: 10.17212/2782-2230-2024-1-42-51.

For citation:

Afanasev A.A. Voprosy organizatsii ekspertizy modeli ugroz [Issues of organization of threat model expertise]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 1 (112), pp. 42–51. DOI: 10.17212/2782-2230-2024-1-42-51.