УДК 004.056.5
DOI 10.33764/2618-981X-2023-6-191-196

А. Р. Пашинин[1], В. В. Селифанов[1,2], П. А. Звягинцева[2,3], Е. А. Плахотникова[3],*

Экспертиза модели угроз безопасности информации для информационных систем

[1] Новосибирский государственный технический университет, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[3] Управление ФСТЭК России по Сибирскому федеральному округу, г. Новосибирск, Российская Федерация
*e-mail: a.pashinin@internet.ru

Аннотация. Основой работы является разработка автоматизированного программного средства для проведения экспертизы модели угроз безопасности информации, разрабатываемых для различных информационных систем, обрабатывающих данные на соответствие требованиям нормативным правовым актам и нормативно методической документации, инициированных Постановлением Правительства, ФСБ России и ФСТЭК России. В данной работе большое внимание уделяется реализации алгоритма построения модели угроз и созданию программного обеспечения, так как на данный момент нет аналогов данному приложению, а проверка документов оператором занимает большое количество времени. Основным продуктом в результате работы с разработкой автоматизированного средства является приложение, которое позволяет существенно сократить временные расходы за счет автоматизации процессов. Также разработанное программное обеспечение уменьшает количество ошибок, связанных с человеческим фактором.

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

A. R. Pashinin[1], V. V. Selifanov[1,2], P. A. Zvyagintseva[2,3], E. A. Plakhotnikova[3]*

Expertise of the Information Security Threat Model for Information Systems

[1] Novosibirsk State Technical University, Novosibirsk, Russian Federation
[2] Siberian State University of Geosystems and Technologies, г. Novosibirsk, Russian Federation
[3] The Office of the Federal service for technical and export control in the Siberian Federal District, Novosibirsk, Russian Federation
*e-mail: a.pashinin@internet.ru

Abstract. The basis of the work is the development of an automated software tool for the expertise of information security threat models developed for various information systems that process data for compliance with the requirements of regulatory legal acts and regulatory methodological documentation initiated by the Decree of the Government, the Federal security service and the Federal service for technical and export control. In this work, much attention is paid to the implementation of the algorithm for building a threat model and the creation of software, since at the moment there are no analogues to this application, and the verification of documents by the operator takes a lot of time. The main product as a result of working with the development of an automated tool is an application that allows you to significantly reduce time costs by automating processes. Also, the developed software reduces the number of errors associated with the human factor.

Keywords: threat model, state information system, threat model expertise, threats, protection of information

Введение

Для любых информационных систем, так или иначе подлежащих защите, необходимо разрабатывать и актуализировать модель угроз, что является требованием соответствующих нормативных правовых документов [1, 2, 3].

Модель угроз содержит описание информационной системы и ее структурно-функциональные характеристики, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможные уязвимости информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации [3, 4], и разрабатывается в соответствии с методическими документами ФСТЭК России [5, 6].

Обязательным требованием для модели угроз государственных информационных систем является проведение государственной экспертизы документов и их согласование с ФСТЭК России и ФСБ России [6]. Это весьма трудоемкая работа, при этом сроки проведения ограничены 10 рабочими днями. Все это требует автоматизации процессов экспертизы. Задачей настоящей работы является разработка программного средства для автоматизации процессов экспертизы моделей угроз.

Разрабатываемое программное средство должно решить данные проблемы и уменьшить временные затраты на проведение экспертизы модели угроз за счет автоматизации процессов, позволив в условиях ограниченного времени на проведение экспертизы модели угроз составить заключение и позволить оператору проверить документ быстрее с минимизацией ошибок, связанных с человеческим фактором.

Требования к модели угроз для проведения экспертизы

Корректное создание модели угроз требует выявления актуальных угроз, так как именно они влияют на устанавливаемые средства защиты информации (далее – СЗИ).

Анализ требований к модели угроз [3-8], опыт работы, накопленный в Управлении ФСТЭК России по Сибирскому федеральному округу, показывает, что для проведения экспертизы достаточным условием будет оценка правильности определения класса защищенности, объекта воздействия и технологий, используемых для обработки информации, возможных негативных последствий от реализации угроз безопасности информации и их источника. Определяется вид нарушителей, их категории и уровень возможностей, а также совокупность тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность [10, 11 – 13]. При оценке возможности реализации угрозы должны присутствовать: объект воздействия, источник угрозы, способ реализации, возможные негативные последствия.

Указанная последовательность действий детально описана в Методике определения угроз безопасности информации [6] и хорошо алгоритмизируется. Программное обеспечение включает стандартные пункты методики [6], необходимые для сохранения общего вида стандартной модели угроз.

В ходе оценки угроз безопасности информации определяются информационные ресурсы, компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям.

Разработка программного средства на базе алгоритма для автоматизированного проведения экспертизы модели угроз

Для решения поставленной задачи было разработано программное обеспечение для проведения экспертизы модели угроз безопасности информации в информационных системах и ориентировано как на операторов, специалистов по защите информации, так и неопытных пользователей.

По результатам работы с программным обеспечением выдается отчет с базовым заполнением документа, актуальными угрозами и подобранными для них тактиками, и соответствующими им типовыми техниками, предлагаемые ФСТЭК России и матрицей MITRE ATT&CK [8 – 9].

Программное обеспечение включает в себя девять диалоговых окон:

1) начальная страница;
2) определение класса защищенности;
3) определение объектов воздействия;
4) выбор видов риска;
5) негативные последствия, после выбора риска;
6) определение нарушителя;
7) выбор источника угрозы;
8) возможность реализации угрозы безопасности информации;
9) завершение работы программы. Формирование и сохранение отчета.

Для начала необходимо выбрать уровень значимости информации и масштаб системы (рис. 1).

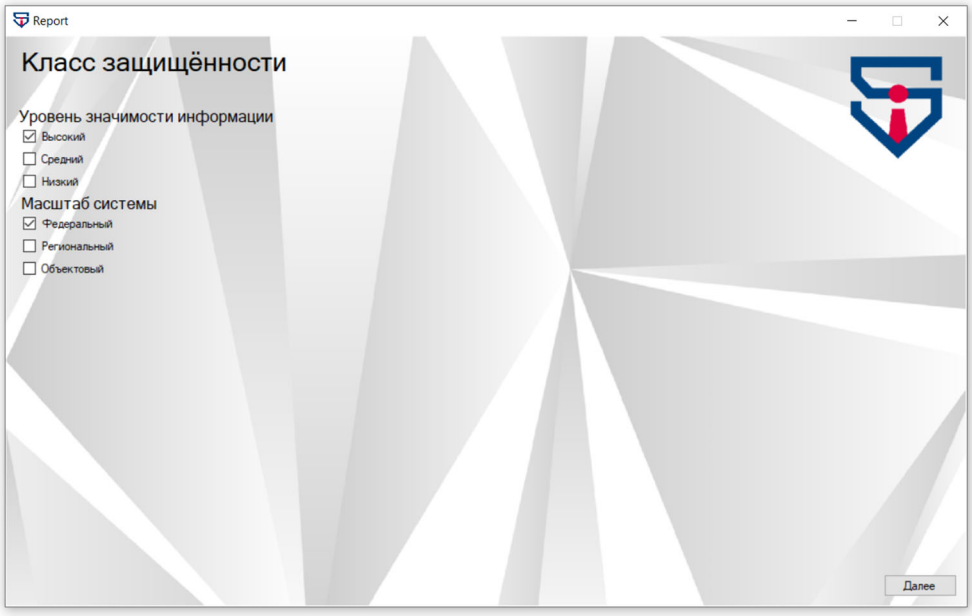

Рис. 1. Определение класса защищенности

Далее программа предложит выбор из списка объектов воздействия (рис. 2).

Рис. 2. Выбор объектов воздействия

Следующим этапом выбирается источник угроз и формируется список возможных угроз. Оператор выбирает угрозы, актуальные для конкретной системы и исключая лишние из проверяемой модели угроз (рис. 3).

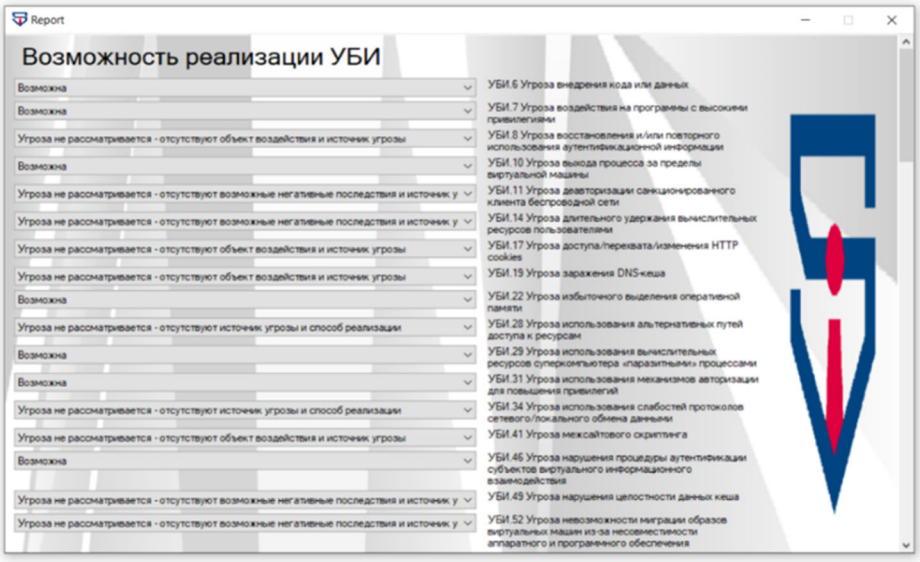

Рис. 3. Выбор объектов воздействия

Время заполнение отчета индивидуально и зависит от списка актуальных угроз, так как при заполнении отчета заполняются и таблицы с тактиками и соответствующими им типовыми техниками, используемыми для построения сценариев реализации угроз безопасности информации по методике ФСТЭК России и матрице MITRE ATT&CK [8 – 9]. Выбор тактик и техник осуществляется по

методическому документу «Методика оценки угроз безопасности информации» с помощью приложения 11, с перечнем основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации [4], а также с помощью матрицы MITRE ATT&CK. В MITRE было выделено двенадцать тактических задач (тактик), которые приходится решать нарушителю и из которых складывается сценарий. В ATT&CK из публично доступных отчетов об инцидентах и исследованиях угроз компьютерной безопасности выделяются общие Тактики, Техники и Процедуры. Также используются публично доступные исследования новых техник, схожих с уже известными поведениями, и потому регулярно обновляются.

Заключение

В процессе работы было разработано программное обеспечение для создания модели угроз безопасности информации информационных систем. Данный продукт позволяет существенно сократить временные расходы за счет автоматизации процессов и уменьшить количество ошибок, связанных с человеческим фактором, поскольку все данные уже внесены в программу, и нельзя пропустить или не указать важные характеристики.

Приложение может использовать любая организация, которая занимается построением или проведением экспертиз модели угроз безопасности информации информационных систем. Благодаря универсальности, ее используют как для проведения экспертизы, так и для разработки самой модели угроз. программа служит хорошим помощником и помогает существенно сократить время на выполнение поставленных задач.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и защите информации» URL: https://docs.cntd.ru/document/901990051 (дата обращения: 15.02.2022 г.).

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных». URL: https://docs.cntd.ru/document/901990046 (дата обращения: 15.02.2023 г.).

3. 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-g-n-17 (дата обращения: 5.05.2023 г.).

4. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методический документ. Методика оценки угроз безопасности информации» URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2169-informatsionnoe-soobshchenie-fstek-rossii-ot-15-fevralya-2021-g-n-240-22-690 (дата обращения: 5.05.2023 г.).

5. Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» URL: https://docs.cntd.ru/document/420285955 (дата обращения: 15.02.2023 г.).

6. Методика определения угроз безопасности информации: методич. материал - Москва, ФСТЭК, 2021. - 83 с. URL: https://docs.cntd.ru/document/607749876 (дата обращения: 13.06.2023 г.).

7. Методический документ. Утвержден ФСТЭК России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах» URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 15.02.2023 г.).

8. Интернет-ресурс «Банк данных угроз безопасности информации». URL: https://bdu.fstec.ru (дата обращения: 3.05.2022 г.).

9. Интернет-ресурс Матрица MITRE ATT&CK, адрес URL: https://attack.mitre.org (дата обращения: 3.02.2023 г.);

10. Хабр. О моделировании угроз. URL: https://habr.com/ru/company /cloud4y/blog/350228/ (дата обращения: 10.06.2022 г.).

11. Степанов В.А. Моделирование угроз безопасности информации по новой методике ФСТЭК, используя средства автоматизации Информационные технологии. Проблемы и решения. 2021. № 4 (17). С. 95-101.

12. Дорошенко И.Е. Вопросы описания возможных сценариев угроз при разработке моделей угроз безопасности информации. /Дорошенко И.Е., Максудов М.О., Селифанов В.В.// Интерэкспо Гео-Сибирь. 2021. Т. 7. № 1. С. 16-21.

13. Стариковская Н.А. Разработка модели угроз для государственной информационной системы. / Стариковская Н.А., Слепухина Ю.В.// Материалы Афанасьевских чтений. 2022. № 2 (39). С. 36-41.