УДК 004.056
DOI 10.33764/2618-981X-2023-8-1-134-141

Е. Д. Бобриков[1], В. В. Селифанов[1]

Разработка сервиса по созданию модели угроз информационной безопасности

[1]Новосибирский государственный технический университет, г. Новосибирск, Российская Федерация
* e-mail: sfo1@mail.ru

Аннотация. В данной работе было описано, для чего нужна разрабатываемая программа, как она поможет рядовому сотруднику по информационной безопасности (ИБ), либо же обычному пользователю, который решит воспользоваться программой, облегчить задачу по составлению модели угроз. Вместе с тем будут затронуты ее отличительные достоинства, в том числе наличие сценариев атак от MITRE ATT&CK, выбор нескольких информационных систем, реализация программы в виде веб-ресурса, а также сопоставление уровней нарушителей из Банка данных угроз (БДУ) Федеральной служба по техническому и экспортному контролю (ФСТЭК) и методики по оценке угроз безопасности информации. В результате моделирования были выявлены актуальные угрозы и сценарии их возникновения, присущие конкретной информационной системе (ИС). Также были рассмотрены аналоги разрабатываемой программы, разобраны их функционал, достоинства и недостатки.

Ключевые слова: информационная безопасность, модель угроз, банк данных угроз, защита информации, средства защиты информации, стандарт, ФСТЭК, техники тактики

E. D. Bobrikov[1], V. V. Selifanov[1]

Development of a Service for Creating an Information Security Threat Model

[1]Novosibirsk State Technical University, Novosibirsk, Russian Federation
* e-mail: sfo1@mail.ru

Abstract. In this paper, it was described why the program being developed is needed, how it will help an ordinary information security officer, or an ordinary user who decides to use the program, to facilitate the task of compiling a threat model. At the same time, its distinctive advantages will be touched upon, including the presence of attack scenarios from MITRE ATT&CK, the choice of several information systems, the implementation of the program in the form of a web resource, as well as a comparison of the levels of violators from the FSTEC database and methods for assessing information security threats. As a result of modeling, actual threats and scenarios of their occurrence inherent in a specific information system (IS) were identified. The analogues of the developed program were also considered, their functionality, advantages and disadvantages were analyzed.

Keywords: information security, threat model, threat database, information protection, information security tools, standard, FSTEC, tactics techniques

Введение

Каждая организация сталкивается с огромным количеством потенциальных информационных угроз, которые могут нанести ей вред. Однако, из-за сложно-

сти процедуры определения и моделирования угроз, перед многими компаниями встает ряд трудностей, который может быть, в частности, связан с недостатком ресурсов. Процесс создания модели угроз требует значительных затрат времени и сил, что особенно трудно для малых и средних предприятий. Поэтому автоматизация этих процессов поможет организациям значительно сократить время на составление моделей угроз и понизить вероятность несанкционированного воздействия на объекты защиты [15,16]. Ведь любой организации важно позаботиться о своей информационной безопасности, чтобы избежать возможных угроз и сохранить репутацию и доверие клиентов.

Также, согласно утвержденному приказу ФСТЭК России от 12 мая 2005 года № 167, определенный срок рассмотрения проектов моделей угроз безопасности информации и технических заданий на создание государственных информационных систем не должен превышать 30 дней. Положения данного приказа распространяются также на критическую информационную инфраструктуру (КИИ), либо информационные системы персональных данных (ИСПДн), которые входят в состав государственных информационных систем (ГИС). Для специалиста по информационной безопасности, который занимается проверкой моделей угроз и технических заданий для приемо-сдаточных испытаний, либо аттестации, этот вопрос, в связи с вышеописанным доводом, тоже является актуальным.

Алгоритм создания программного обеспечения (ПО)

Сложность в создании рассматриваемого ПО заключается в том, что необходимо подобрать к каждой отдельно взятой угрозе сценарии возникновения атаки, а угроз, в свою очередь, насчитывается уже 222. И если в методологии ФСТЭК России [11] пишут, что достаточно лишь одного сценария, то с точки зрения полезности это совершенно не так. Особенно, когда речь идет о программном обеспечении, в которое необходимо заранее внести все возможные вариации проведения компьютерной атаки, чтобы они соответствовали каждой отдельно взятой ИС.

Основной задачей, как говорилось выше, является определение сценариев возникновения угроз. Сценарий угрозы – это совокупность тактики и соответствующей ей техники [11].

Основной плюс разрабатываемой программы заключается в том, что будут использованы не только техники тактики от ФСТЭК, но и от MITRE ATT&CK [18].

ATT&CK представляет собой базу знаний и систему классификаций действий злоумышленников, предпринимаемых ими в ходе кибератак. MITRE разработала ATT&CK в 2013 году для документирования Тактик, Техник и Процедур (ТТП), которые злоумышленники использовали для целенаправленных кибератак на корпоративные инфраструктуры под управлением операционной системы Windows. Фреймворк был создан с целью документирования действий злоумышленников [18]. Основным достоинством является то, что главными источниками данных в ATT&CK являются публично доступные отчеты об инцидентах и исследованиях киберугроз. Из них выделяются общие ТТП. Также ис-

пользуются публично доступные исследования новых техник, схожих с уже известными вредоносными действиями. Это необходимо, поскольку новые ТТП быстро принимаются на вооружение действующими преступными группировками.

Если же сравнивать указанные техники с техниками от ФСТЭК, то можно заметить большие различия. Как минимум, в ФСТЭК делали свои техники, опираясь как раз на MITRE, и их версия вышла более урезанной и неполной в сравнении с зарубежным аналогом. К примеру, техника Т4.1 ФСТЭК описывает несанкционированное создание или кражу учетных записей [11]. У MITRE это является отдельной тактикой «доступ к учетным записям» (Credential Access), в которой 15 основных и 52 второстепенных техники. То есть, можно сказать, что MITRE ATT&CK является более обширной и точной версией техник тактик от ФСТЭК. Руководствоваться при определении сценариев возникновения угрозы по MITRE ATT&CK можно переводом, который был сделан компанией Positive Technologies, пример которого предоставлен на рис. 1.

Рис. 1. Перевод примера сценария реализации угрозы безопасности информации от Positive Technologies с помощью матрицы MITRE ATT&CK

Одним из важных преимуществ разрабатываемой программы является и то, что сотрудник ИБ сможет в ходе создания модели угроз выбрать одну либо несколько информационных систем, для которых и будут подбираться актуальные угрозы из предоставленных на выбор. А именно ИСПДн, ГИС, либо же КИИ. Это будет полезно для целого пласта объектов таких как, к примеру, Государственная муниципальная больница, которая одновременно может являться ГИС и ИСПДн и КИИ [8,3,1]. Специалист ИБ сможет с помощью наводящих вопросов определить уровень защищенности ИСПДн, класс защищенности для ГИС, либо же категорию значимости КИИ.

Важно упомянуть и то, что при разработке ПО было принято решение создать свой собственный сайт, на котором и можно будет составить модель угроз для выбранной информационной системы. Основных причин для создания сайта было несколько. Во-первых, с помощью веб ресурса будет возможность не просто один раз построить модель угроз, а при помощи регистрации, которая будет

встроена на сайте, пользователь сможет смотреть в личном кабинете историю своих отчетов.

Во-вторых, пользователю не нужно будет каждый раз скачивать новую версию приложения при внесении в ПО новых сценариев либо же угроз, ведь все обновления будут загружаться на сайт по мере их поступления.

Если говорить про дальнейшее поддержание работы сайта, то на нем будет реализован механизм обновления ПО, с помощью которого можно будет добавлять новые техники тактики и корректировать список имеющиеся.

Выбор угроз для конкретной ИС будет проводиться по нескольким параметрам, таким как объект воздействия и модель нарушителя. Эти два пункта являются основополагающими при выделении угроз, которые могут в дальнейшем оказаться актуальными. Ко всему прочему, в разрабатываемом ПО будет реализовано соотнесение уровней нарушителя из методологии ФСТЭК с БДУ ФСТЭК, так как в БДУ – 3 потенциала нарушителя (низкий, средний, высокий) [19], а, в свою очередь, в методологии – 4 уровня возможностей нарушителей (базовый, базовый с повышенными возможностями, средний, высокий) [11]. Соотнесение выполнено при помощи скриншота, взятого из онлайн выступления ФСТЭК на ТБ – Форум 2022, который представлен на рис. 2.

Рис. 2. Соотнесение уровней нарушителей

Нельзя не отметить и то, что все объекты воздействия заранее были распределены по группам, как пример можно привести такие категории, как: «прикладное ПО», «системное ПО», «облачная система» и «нейросети». В дальнейшем к этим категориям были составлены компоненты объектов воздействий. Это было

сделано для того, чтобы пользователь смог выбрать только нужные ему компоненты для составления более точной модели угроз.

Обзор аналогов

Проанализировав Российский рынок, авторы пришли к выводу, что аналогов разрабатываемому ПО нет, не считая нового раздела угроз ФСТЭК, о котором дальше и пойдет речь. В мае 2022 года на сайте ФСТЭК был добавлен раздел (рис. 3), в котором можно сформировать перечень возможных угроз безопасности информации (УБИ).

Рис. 3. Начальная страница раздела по формированию актуальных угроз

Он имеет хороший функционал, к примеру, на сайте можно выбрать категории объектов воздействия, что является плюсом и дает большую гибкость при формировании перечня угроз (рис. 4).

Но есть один решающий фактор, по которому можно сказать, что этот раздел не готов к введению в эксплуатацию, а находится лишь на этапе разработки. Возможных угроз для выбора представлено всего 11 штук (рис. 5), что является критически малым количеством, учитывая то, что список угроз состоит из 222 наименований.

Также можно выделить и то, что рассматриваться эти угрозы будут только по сценариям, разработанным самой ФСТЭК. Это означает, что техники тактики MITRE рассмотрены в этом веб ресурсе не будут, что является еще одним весомым недостатком.

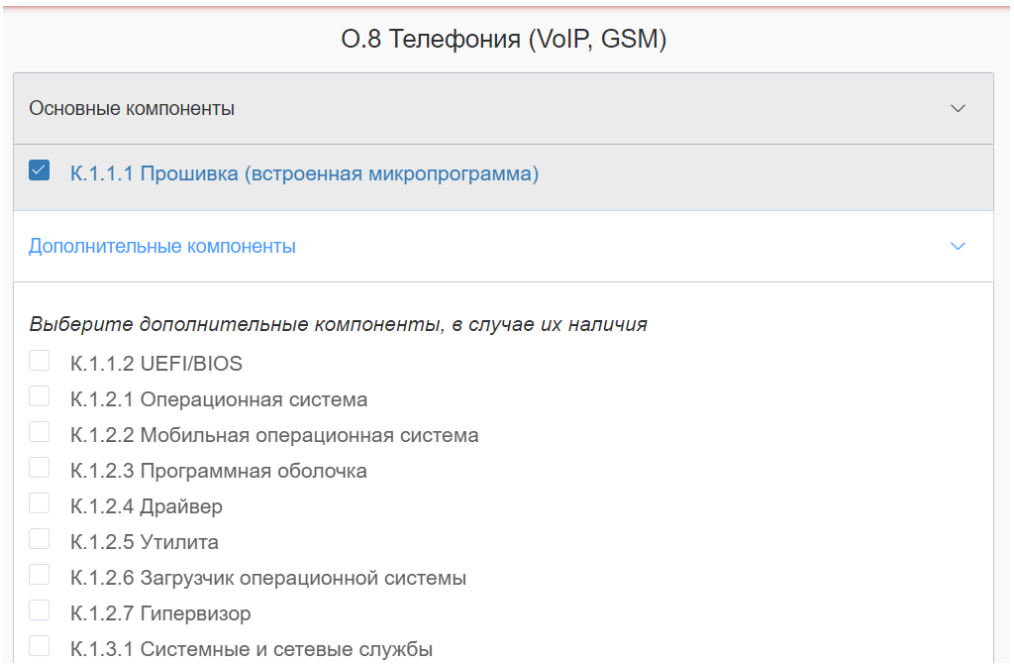

Рис. 4. Выбор компонентов объектов воздействия, реализованный на сайте ФСТЭК

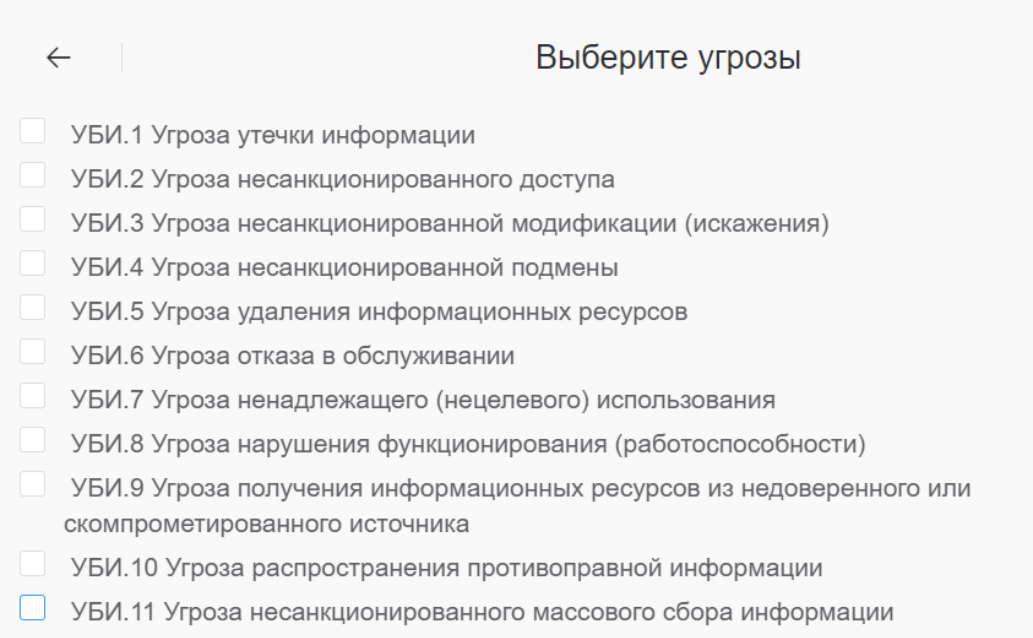

Рис. 5. Перечень доступных к выбору угроз на сайте ФСТЭК

Заключение

В заключении можно выделить, что разрабатываемое ПО, вследствие озвученных доводов, является актуальной разработкой для нашего времени, ведь на российском рынке не найти аналогов этому продукту, а актуальность создания модели угроз с каждым годом только растет.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/901990046 (дата обращения 10.05.2023г.).

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и защите информации» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/901990051 (дата обращения 10.05.2023г.).

3. Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения 10.05.2023г.).

4. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» [Электронный ресурс]. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=334098 (дата обращения 08.05.2023г.).

5. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – URL: https://pd.rkn.gov.ru/docs/Postanovlenie_Pravitel6stva_RF_1119.pdf (дата обращения 09.05.2023 г.).

6. Постановление Правительства Российской Федерации от 6 июля 2016 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» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/420285955 (дата обращения 15.04.2023 г.).

7. Постановление правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127 (дата обращения 13.04.2023 г.).

8. 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» [Электронный ресурс]. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossiiot-11-fevralya-2013-g-n-17 (дата обращения 13.04.2023 г.).

9. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 11.03.2023 г.).

10. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77 (дата обращения 16.05.2023 г.).

11. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методический документ. Методика оценки угроз безопасности информации» [Электронный ресурс]. – 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 17.05.2023 г.).

12. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200058320 (дата обращения 11.05.2023 г.).

13. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. [Электронный ресурс]. – URL: http://www.fa.ru/org/div/uank/Documents/2019/%D0%93%D0%9E%D0%A1%D0%A2%20%D0%A0%2051624-2000.pdf (дата обращения 08.04.2023 г.).

14. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200006924 (дата обращения 12.03.2023 г.).

15. Голушко, А. П. Автоматизация работы с источником данных о тактиках и техниках проведения компьютерных атак / А. П. Голушко, В. Г. Жуков // Актуальные проблемы авиации и космонавтики: Сборник материалов VII Международной научно-практической конференции, посвященной Дню космонавтики: в 3 томах, Красноярск, 12–16 апреля 2021 года / Под общей редакцией Ю. Ю. Логинова. Том 2. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2021. – С. 374–376.

16. Грибанова-Подкина, М. Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования / М. Ю. Грибанова-Подкина // Вопросы безопасности. – 2017. – № 2. – С. 25–34.

17. Консультант Плюс [Электронный ресурс]. – URL: http://www.consultant.ru (дата обращения 20.04.2023 г.).

18. The MITRE Corporation. Cyber Analytics Repository [Электронный ресурс]. – URL: https:// car.mitre.org/ wiki/Main_Page (дата обращения 20.04.2023 г.).

19. Банк данных угроз безопасности информации [Электронный ресурс]. – URL: www.bdu.fstec.ru (дата обращения 28.03.2023 г.).

20. Positive technologies [Электронный ресурс]. – URL: https://mitre.ptsecurity.com/ru-RU/techniques?utm_source=seclab&utm_medium=news (дата обращения 24.04.2023 г.).