УДК 004.056.053

***С.П. Серёдкин*[1]**

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

ПРАКТИКА ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННОГО СПОСОБА МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Аннотация. В работе предложен подход к рассмотрению опытной эксплуатации моделированного раздела угроз безопасности который позволяет существенно облегчить процесс проведения методики угроз безопасности для информационных систем в соответствии с методикой оценки угроз Федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 5 февраля 2021 г.

Ключевые слова: Федеральная служба по техническому и экспортному контролю (ФСТЭК), угрозы безопасности информации (УБИ), информационная безопасность (ИБ), информационные системы (ИС), способы реализации угроз, негативные последствия.

***S.P. Seryodkin*[1]**

[1]*Irkutsk State Transport University, Irkutsk, Russian Federation*

THE PRACTICE OF USING AN AUTOMATED METHOD FOR MODELING INFORMATION SECURITY THREATS

Annotation. The paper proposes an approach to considering the trial operation of the simulated security threats section, which makes it possible to significantly facilitate the process of conducting a security threat methodology for information systems in accordance with the threat assessment methodology of the Federal Service for Technical and Export Control (FSTEC) of Russia dated February 5, 2021.

Keywords: Federal Service for Technical and Export Control (FSTEC), threats to information security (UBI), information security (IS), information systems (IS), ways to implement threats, negative consequences.

Введение. Моделирование угроз безопасности информации является обязательной процедурой при построении системы защиты информации которая позволяет определить актуальные угрозы, от которых и необходимо защищать ценные информационные активы. Без моделирования угроз либо будет построена избыточная система защиты, защищающая в том числе от угроз, которых нет. Либо неэффективная система защиты, не охватывающая все актуальные угрозы [16]. Создание и модернизация системы защиты информации на основе модели угроз в условиях роста числа угроз является актуальной задачей для владельцев информационных систем. По оценкам экспертов в 2022 году внимание киберпреступников привлекали все ключевые отрасли экономики. Так, эксперты Positive Technologies [1] отмечают следующее:1. Государственный сектор — был целью № 1. Всего за 2022 год зафиксировано 403 атаки, что на 25% больше, чем за 2021 год; 2. Промышленность сектор — хакеры стремятся остановить технологические процессы. Всего за год зафиксировано 223 атаки что на 7% больше по сравнению с 2021 годом; 3. Медицина — лидирует по утечкам данных. Медучреждения уже пятый год подряд остаются в тройке самых атакуемых отраслей: в 2022 году доля атак на них составила 9% среди всех организаций, а количество атак держится примерно на уровне 2021 года; 4. Финансовый сектор — наилучшая подготовленность к атакам, но в целом уровень защиты недостаточный. По итогам 2022 года общее число атак на финансовые организации снизилось на 7% по сравнению с аналогичным периодом 2021 года; 5. IT-компании — осторожность в использовании открытого ПО и контроль цепочек поставок. Число атак на IT-компании в 2022-м несколько уменьшилось по сравнению с 2021 годом, однако на них все еще приходится 6% атак на организации; 6. Наука и образование. Учреждения из сферы науки и образования входят в топ-5 самых часто атакуемых организаций. Количество атак на них сопоставимо с результатами 2021 года.

За 2022 год увеличилась доля атак на веб-ресурсы: с 11% до 20%;7. Пользователи — масштабные утечки данных. Количество атак на частных лиц увеличилось на 44%. На обычных пользователей пришлось 17% от числа всех атак. Традиционно основной вектор атаки — это различные приемы социальной инженерии, которые использовались в 93% случаев. Для проведения таких атак злоумышленники создавали фишинговые сайты (56%), отправляли вредоносные письма по электронной почте (39%), искали жертв в социальных сетях (21%) и мессенджерах (18%).

Необходимость моделирования угроз безопасности информации. Приведенная статистика говорит не только о возрастании количества атак на информационные ресурсы учреждений и организаций, но и на своевременность и результативность мер, направленных на повышения уровня информационной безопасности принятых Президентом и Правительством РФ [2,3]. Для поддержания системы защиты информации в режиме противодействия актуальным угрозам безопасности учреждения и предприятия должны своевременно и качественно проводить моделирование угроз с целью выработки актуальных мер защиты по противодействию кибератакам. Для достижения данных целей необходимо поддерживать модель угроз безопасности информации в актуальном режиме т.е. в режиме реального времени.

Методика оценки угроз безопасности информации, утверждённая 05.02.2021. ФСТЭК России применяется на стадии создания и модернизации информационной систем и информационно-телекоммуникационных сетей, для определения предъявляемых к ним требований безопасности информации. Данная процедура проводиться субъектом информационной системы силами специалистов по защите информации и требует определенного уровня подготовки и квалификации. Документ [4] требует обязательного согласования моделей угроз безопасности информации и технических заданий на создание государственных информационных систем со ФСТЭК России. С учетом сложившейся практик по разработке моделей угроз государственные учреждения недостаточно квалифицированно выполняют данную процедуру, по этим причинам регулятор довольно часто возвращает собственникам ИС модели угроз на доработку и повторное согласование [6]. Все эти причины послужили на наш взгляд причиной размещения на официальном сайте ФСТЭК России ресурса - «опытной эксплуатации моделированного раздела угроз безопасности» рис.1. На сайте в разделе БДУ «моделированный раздел угроз безопасности» пользователь имеет возможность провести моделирование угроз безопасности по предложенному алгоритму рис.2.

Рис. 1. Новый раздел угроз безопасности

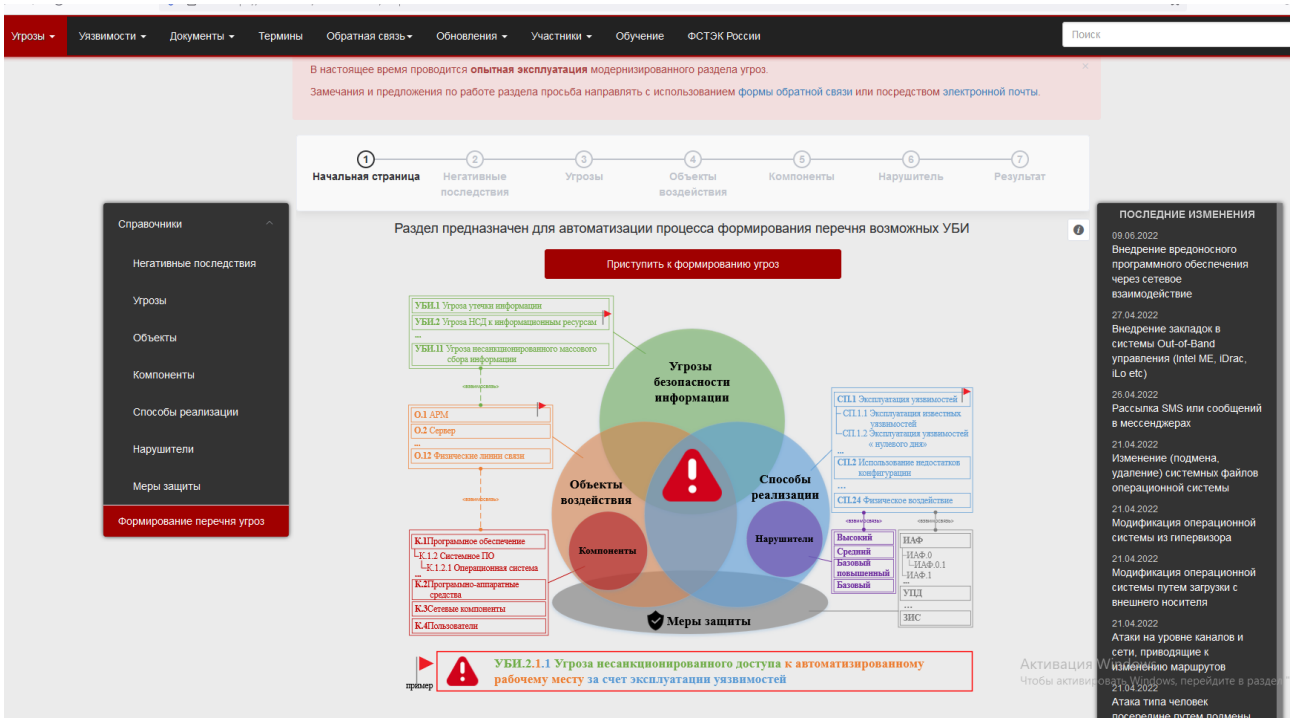

Рис. 2. Схема автоматизации процесса формирования перечня возможных УБИ

Предложенный процесс формирования перечня угроз безопасности информации подготовлен на основании требований «Методики оценки угроз безопасности информации» [5]. Использование в разделе данных справочника позволяет в автоматическом режиме приступить к процедуре формирования угроз рис.3. Справочник содержит актуальный на данное время следующий перечень исходных данных:

- перечень негативных последствий;
- наименование актуальных угроз;
- перечень объектов воздействия,
- перечень компонентов объектов воздействия;
- перечень способов реализации угроз,
- уровни возможностей потенциальных нарушителей.

Вводя поэтапно актуальные данные исследуемой информационной системы, формируется модель угроз безопасности информации (рисунок 3).

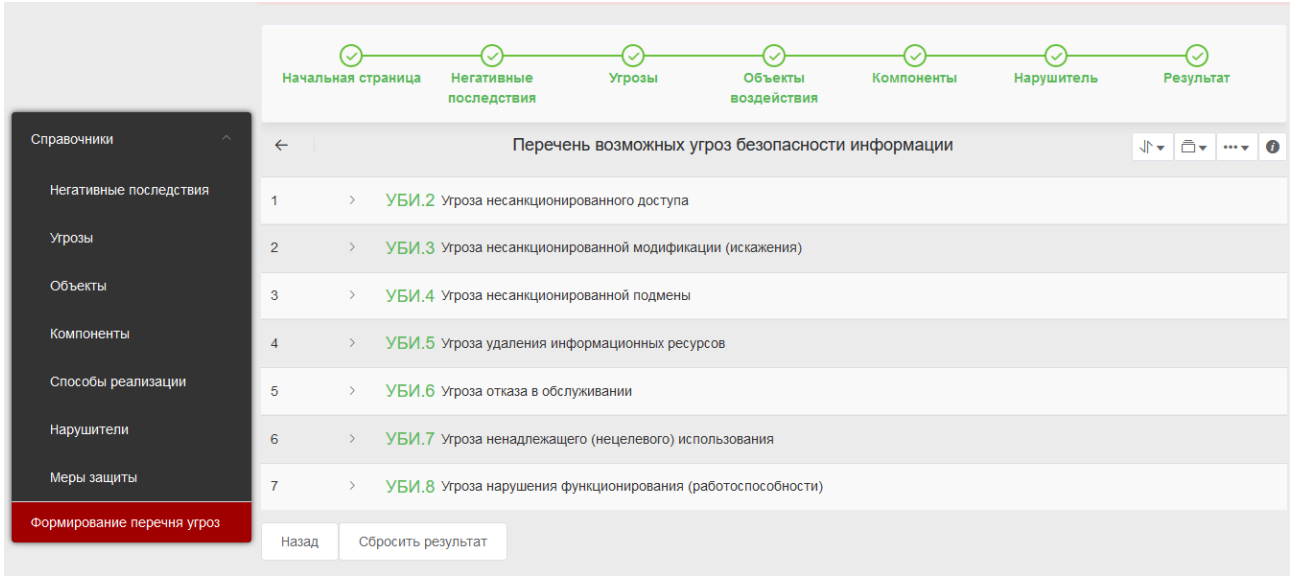

Рис. 3. Результат моделирования угроз

Выводы. Предложенный метод позволяет существенно снизить время формирования моделей угроз безопасности, своевременно и квалифицированно пересматривать актуальные угрозы с целью противодействия кибератакам для обеспечения штатного режима функционирования информационной системы.

Надеемся, что изложенные в статье информация найдет понимание в различных сферах образования для студентов и преподавателей, а также возможность практического применения материала статьи для специалистов по защите информации организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://www.ptsecurity.com/ru-ru.
2. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".
3. Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации".
4. Информационное сообщение «О ПОРЯДКЕ РАССМОТРЕНИЯ И СОГЛАСОВАНИЯ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ТЕХНИЧЕСКИХ ЗАДАНИЙ НА СОЗДАНИЕ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ» ФСТЭК России от 22 июня 2017 г. N 240/22/3031 - https://fstec.ru.
5. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ»- https://fstec.ru/.
6. https://fstec.ru/en/gniii-ptzi-fstek-rossii/kontakty-gniii/64-normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1340-informatsionnoe-soobshchenie-fstek-rossii-ot-22-iyunya-2017-g-n-240-22-3031?ysclid=lcyon26rg831685390.
7. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента РФ от 25.11.2017 N 569 "О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. N 1085".
9. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации.
11. https://attack.mitre.org/matrices/enterprise/
12. https://mitre-attack.github.io/attack-navigator/
13. https://apt.securelist.com
14. https://fstec.ru/
15. https://www.vesti.ru/hitech/article/2671915
16. https://www.corpsoft24.ru/about/blog/modelirovanie-ugroz-chto-novogo/?ysclid=ld2j6m7x9y320456447

REFERENCES

1. https://www.ptsecurity.com/ru-ru.
2. Decree of the President of the Russian Federation No. 250 dated 01.05.2022 "On additional measures to ensure information security of the Russian Federation".
3. Decree of the President of the Russian Federation No. 166 dated 30.03.2022 "On measures to ensure the Technological Independence and security of the Critical Information Infrastructure of the Russian Federation".

4. Information Message "On THE PROCEDURE FOR CONSIDERATION AND APPROVAL OF INFORMATION SECURITY THREAT MODELS AND TECHNICAL SPECIFICATIONS FOR THE CREATION OF STATE INFORMATION SYSTEMS" of the FSTEC of Russia dated June 22, 2017 N 240/22/3031 - https://fstec.ru.

5. Methodological document. Approved by the FSTEC of Russia on February 5, 2021, "METHODOLOGY for ASSESSING INFORMATION SECURITY THREATS"- https://fstec.ru.

6. https://fstec.ru/en/gniii-ptzi-fstek-rossii/kontakty-gniii/64-normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1340-informatsionnoe-soobshchenie-fstek-rossii-ot-22-iyunya-2017-g-n-240-22-3031?ysclid=lcyon26rg831685390.

7. Decree of the President of the Russian Federation No. 1085 dated 16.08.2004 "Issues of the Federal Service for Technical and Export Control".

8. Decree of the President of the Russian Federation No. 569 of 11/25/2017 "On Amendments to the Regulations on the Federal Service for Technical and Export Control, approved by Decree of the President of the Russian Federation No. 1085 of August 16, 2004".

9. The Order of the FSTEC of Russia of February 11, 2013 No. 17 "On approval of requirements for the protection of information not constituting a state secret contained in state information systems".

10. Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection".

11. https://attack.mitre.org/matrices/enterprise/

12. https://mitre-attack.github.io/attack-navigator/

13. https://apt.securelist.com

14. https://fstec.ru/

15. ttps://www.vesti.ru/hitech/article/2671915

16. https://www.corpsoft24.ru/about/blog/modelirovanie-ugroz-chto-novogo/?ysclid=ld2j6m7x9y320456447

Информация об авторе

Серёдкин Сергей Петрович – к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Seryodkin Sergei Petrovich – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Практика применения автоматизированного способа моделирования угроз безопасности информации// «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2023. – №1(17). – С.36-40– DOI: 10.26731/2658-3704.2023.1(17).36-40 – Режим доступа: http://ismm-irgups.ru/toma/117-2023, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 31.03.2023)

For citations

Seryodkin S.P. The practice of using an automated method for modeling information security threats // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: elektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the man-agement of complex systems: electronic scientific journal], 2023. No. 1(17). P. 36-40. DOI: 10.26731/2658 3704.2023.1(17).36-40 [Accessed 31/03/23]