БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 2 (117). – 9–24

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-2-9-24

ПРОБЛЕМЫ ОЦЕНКИ АКТУАЛЬНОСТИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ*

И.В. НИКРОШКИН[1], А.В. САВЕНКОВА[2]

[1] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: i.nikroshkin@corp.nstu.ru*

[2] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: savenkova.2021@stud.nstu.ru*

Статья посвящена анализу проблемы оценки актуальности киберугроз в современных методиках информационной безопасности. Рассматриваются недостатки существующего подхода, в том числе ограниченность охвата сценариев реализации угроз, отсутствие механизмов регулярного обновления данных о тактиках и техниках атак, неунифицированная классификация нарушителей и субъективный характер оценок. Предлагается расширить источники информации об угрозах за счет интеграции данных из отечественных и зарубежных баз знаний (CAPEC, ATT&CK, OWASP, STIX, WASC), внедрить автоматизированные средства генерации сценариев на основе семантического анализа, усовершенствовать классификацию нарушителей и обеспечить систематическое обновление модели угроз. Реализация этих рекомендаций позволит повысить объективность, полноту и актуальность оценки киберугроз, улучшив эффективность принимаемых мер защиты.

Ключевые слова: информационная безопасность, модель угроз, экспертиза модели угроз, угрозы, защита информации, угрозы информационной безопасности

ВВЕДЕНИЕ

В условиях стремительного роста количества и сложности киберугроз проблема оценки их актуальности становится одной из ключевых задач в области информационной безопасности. Современные технологии способствуют появлению новых методов атак, что требует постоянного совершенствования подходов к анализу и оценке угроз. Одной из важных задач при обеспече-

* Статья получена 12 мая 2025 г.

нии информационной безопасности является разработка модели угроз и оценка рисков, которая позволяет определить требования к системе защиты. Такая оценка напрямую влияет на формирование модели угроз и определение набора необходимых мер защиты, позволяя оптимизировать ресурсы и обеспечивать устойчивость киберинфраструктуры к возникающим рискам.

Требование формировать модель угроз закреплено нормативными актами. Так, ФЗ № 149-ФЗ «Об информации, информационных технологиях и защите информации» и ФЗ № 152-ФЗ «О персональных данных» (статья 19) обязывают операторов анализировать угрозы безопасности информации и ПДн. Приказы ФСТЭК России № 17, № 21 и № 239, в свою очередь, требуют учитывать актуальные угрозы при выборе мер защиты для государственных информационных систем, информационных систем персональных данных и критически важных объектов.

Однако на практике применяемые методики разработки и актуализации модели угроз неизбежно сталкиваются с целым рядом проблем.

Во-первых, зачастую рассматривается ограниченный набор сценариев, не отражающий реальное многообразие возможных атак. Во-вторых, отсутствуют механизмы регулярного обновления данных, что приводит к использованию устаревшей информации об угрозах и снижению точности оценки. В-третьих, субъективность в определении актуальности угроз и оценке потенциала нарушителей усложняет принятие решений о приоритетах защиты.

Целью настоящей работы является анализ существующих проблем в оценке актуальности киберугроз и определение возможных направлений их решения, которые могли бы служить основой для дальнейшего совершенствования методик и инструментов.

Результатом выполненного исследования станет систематизация имеющихся проблем и набора потенциальных мер по их устранению, которая может быть использована в дальнейшем для доработки существующих методик оценки угроз, совершенствования нормативно-правовой базы, а также разработки новых инструментов, обеспечивающих более адекватную и своевременную оценку актуальности угроз в условиях динамично меняющегося киберпространства.

1. ОЦЕНКА ОДНОГО СЦЕНАРИЯ РЕАЛИЗАЦИИ УГРОЗ

На практике для оценки угрозы необходимо проанализировать все возможные сценарии ее реализации, однако методика ФСТЭК предполагает определение хотя бы одного сценария каждого способа реализации возможной угрозы безопасности информации (УБИ). Обнаружение хотя бы одного

сценария реализации УБИ считается достаточным основанием для того, чтобы признать угрозу актуальной и внести ее в модель угроз безопасности системы [20]. Это упрощает процесс анализа, но существенно снижает полноту и точность оценки. В итоге могут остаться незамеченными другие возможные сценарии реализации угроз. Такой подход делает систему уязвимой для атак, которые остаются незамеченными из-за одностороннего анализа. Для построения более надежной системы информационной безопасности необходимо рассматривать все возможные сценарии реализации. В методике описано, что в качестве исходных данных для оценки угроз безопасности можно использовать не только БДУ ФСТЭК, но и информацию с таких ресурсов, как CAPEC, ATT&CK, OWASP, STIX, WASC [1]. Для того чтобы сформировать правильную оценку актуальности угроз, необходимо использовать все имеющиеся ресурсы, а не ограничиваться только одним [19]. Также может быть полезно использование автоматизированных инструментов для генерации сценариев реализации угроз на основе семантического анализа текстов в перечисленных выше источниках данных [12].

2. НЕОБХОДИМОСТЬ АКТУАЛИЗАЦИИ МОДЕЛИ УГРОЗ

В соответствии с Методикой ФСТЭК модель угроз должна оставаться актуальной и пересматриваться при изменении условий функционирования системы. К таким изменениям относятся обновление конфигурации, внедрение новых компонентов или версий программного обеспечения, которые могут содержать ранее неизвестные уязвимости. Кроме того, необходимость пересмотра модели возникает при появлении новых угроз, не учтенных в изначальной модели.

Модель угроз является «живым» документом, который необходимо регулярно актуализировать. Рекомендуется пересматривать ее не только при значительных изменениях в системе, но и на регулярной основе (например, один раз в год). Такой подход позволяет своевременно учитывать новые факторы риска и адаптировать защитные меры, обеспечивая надежную защиту системы в условиях быстро меняющейся киберсреды [13].

3. ОТСУТСТВИЕ МЕХАНИЗМА РЕГУЛЯРНОГО ОБНОВЛЕНИЯ ДАННЫХ

Одной из серьезных проблем в оценке актуальности угроз безопасности информации является отсутствие механизма регулярного обновления данных о техниках и тактиках их реализации. Угрозы постоянно меняются, злоумыш-

ленники адаптируют свои методы, комбинируют известные подходы и разрабатывают новые. Однако информация об этих изменениях часто обновляется несвоевременно. Это приводит к тому, что существующие методики оценки угроз опираются на устаревшие данные, что снижает их актуальность. В методике ФСТЭК тактики и сценарии угроз не обновляются постоянно, тогда как в MITRE ATT&CK для учета новых методов атак изменения вносятся ежеквартально. Кроме того, для полного учета всех аспектов при моделировании угроз нельзя ограничиваться одной-единственной матрицей актуальных угроз [18].

Методика [1] систематизирует инструменты моделирования угроз: в приложении 11 перечислены 11 ключевых тактик и 41 типовая техника, применяемые при разработке сценариев их реализации [4]. В международной базе знаний MITRE ATT&CK представлено 14 тактик, каждая из которых включает множество техник и подтехник. По состоянию на ноябрь 2024 года матрица MITRE ATT&CK содержала более 200 техник и свыше 400 подтехник [6].

На данный момент Национальная база данных уязвимостей (NVD) насчитывает свыше 250 тысяч записей, тогда как российская БДУ ФСТЭК содержит более 70 тысяч описаний уязвимостей и 222 записи, посвященные угрозам информационной безопасности [14]. Для решения проблемы можно обязать организации регулярно предоставлять информацию о выявленных угрозах в централизованный реестр, а профильные ведомства – систематизировать эти данные и публиковать обновленные рекомендации ежеквартально. Такой подход позволит наладить процесс обмена информацией и актуализировать данные без значительных затрат.

Банк данных угроз безопасности информации ФСТЭК России преимущественно ориентирован на государственные информационные системы. Таким образом, уязвимости программного обеспечения не всегда представлены в полном объеме, что может ограничивать возможности специалистов по информационной безопасности при оценке рисков и разработке мер защиты для различных систем.

4. ОТСУТСТВИЕ ЧЕТКИХ АЛГОРИТМОВ ДЛЯ ОПРЕДЕЛЕНИЯ КЛАССИФИКАЦИИ НАРУШИТЕЛЕЙ

Одной из актуальных проблем текущей методики ФСТЭК является отсутствие четких алгоритмов для определения классификации нарушителей [3]. Согласно [16] под нарушителем информационной безопасности понимают физическое лицо, которое случайно или преднамеренно совершило действия, следствием которых стало нарушение информационной безопасности при ее обработке техническими средствами в информационных системах.

В БДУ ФСТЭК России выделяют низкий, средний и высокий потенциал нарушителей.

Однако методика ФСТЭК использует собственную шкалу потенциала нарушителей, которая не совпадает с классификацией, принятой в Банке данных угроз. В документе выделяются четыре уровня:

- базовый;
- расширенный базовый;
- средний;
- высокий.

Следовательно, классификацию нарушителей, применяемую в БДУ, следует унифицировать с классификацией, установленной методикой ФСТЭК [2]. Также в текущих моделях угроз акцент сделан на уязвимостях систем, а не на характеристиках атакующих, что снижает их применимость в практических задачах (например, при расследовании киберинцидентов).

Может быть использован метод анализа иерархий, который предложил Т. Саати: эксперты ранжируют критерии и альтернативы, задают им весовые коэффициенты и тем самым получают интегральную оценку потенциала нарушителя.

Таблица 1

Шкала отношений

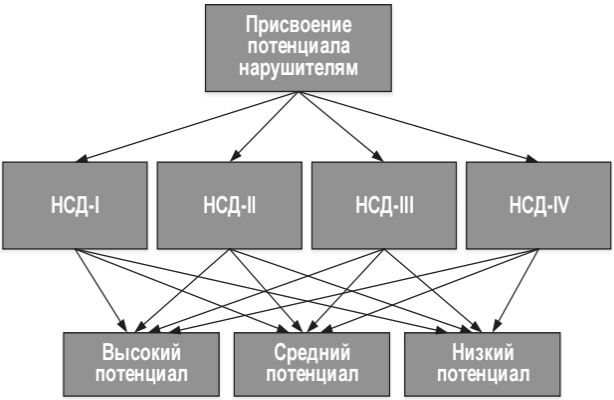
Степень важности	Значимость
1	Одинаковая
3	Слабая
5	Сильная
7	Очень сильная
9	Абсолютная
2, 4, 6, 8	Промежуточные значения между соседними значениями шкалы

Согласно данной методологии, для трех категорий нарушителей безопасности информации необходимо построить иерархическую модель.

На рисунке показана иерархическая модель внешнего нарушителя, в которой выделены четыре варианта несанкционированного доступа (НСД):

- НСД-I – проникновение через автоматизированные рабочие места, располагающиеся в сетях общего пользования;
- НСД-II – получение доступа с использованием специализированного ПО и вредоносных программ;

- НСД-III – атака через компоненты, находящиеся за пределами контролируемой зоны;
- НСД-IV – компрометация посредством смежных информационных систем.



Иерархической модель для определения потенциала внешнего нарушителя безопасности информации

После построения иерархической модели применяется ряд формул. Обратные значения в матрице рассчитываются по формуле

$$x_{nm} = \frac{1}{x_{mn}}.$$

Нормализация элементов производится по формуле

$$X_{ij} = \frac{X_{nj}}{S_j}.$$

Затем вычисляется вес для нормированной матрицы

$$D = \sum\left(\frac{x_i}{j}\right).$$

Нормированные матрицы, отображающие критерии и варианты потенциала злоумышленников, приведены в табл. 2 и 3. Для остальных критериев формируются таблицы того же формата.

Таблица 2

Попарное сравнение критериев возможностей нарушителей

Критерий	НСД-I	НСД-II	НСД-III	НСД-IV
НСД-I	1	0,2	3	4
НСД-II	5	1	7	0,33
НСД-III	0,33	0,14	1	0,2
НСД-IV	0,25	0,25	2	1
Вес в долях	0,31	0,49	0,06	0,13

Таблица 3

Попарное сравнение альтернатив по критерию

НСД-I	Низкий	Средний	Высокий
Низкий	0,13	0,14	0,10
Средний	0,50	0,57	0,60
Высокий	0,38	0,29	0,30
Вес в долях	0,12	0,56	0,33

Формула для расчета потенциала нарушителя:

$$A = (z_{ij})(y_j).$$

На примере табл. 2 рассчитаем потенциал нарушителя:

$$A = \begin{pmatrix} 0,12 & 0,1 & 0,1 & 0,1 \\ 0,56 & 0,57 & 0,57 & 0,57 \\ 0,32 & 0,33 & 0,33 & 0,33 \end{pmatrix} \begin{pmatrix} 0,31 \\ 0,49 \\ 0,06 \\ 0,13 \end{pmatrix} = \begin{pmatrix} 0,11 \\ 0,56 \\ 0,33 \end{pmatrix}.$$

Внешним нарушителям с весовой долей 0,56, вычисленной по формуле, приведенной выше, при использовании данных из табл. 3 присваивается средний потенциал.

Предложенная методика функционирует в полуавтоматическом режиме: по заданным критериям вычисляется интегральный показатель, который сопоставляется с установленными пороговыми значениями, что позволяет без существенного привлечения экспертов объективно присвоить нарушителю соответствующий уровень потенциальных возможностей.

5. ПРОБЛЕМА МОДЕЛИРОВАНИЯ УГРОЗ, СВЯЗАННЫХ С СКЗИ

Еще одной проблемой, влияющей на полноту оценки актуальности угроз, является то, что в существующих методиках недостаточно проработаны подходы к моделированию угроз, связанных с нарушением безопасности криптографических средств защиты информации, а также угроз, возникающих через технические каналы утечки информации. Недостаточное внимание к этим аспектам снижает полноту анализа угроз и может привести к недооценке рисков, особенно в системах, где используются средства криптографической защиты или имеются технические уязвимости, связанные с побочными электромагнитными излучениями и наводками [17].

6. СУБЪЕКТИВНОСТЬ В ОЦЕНКЕ УГРОЗ БЕЗОПАСНОСТИ

Субъективность в оценке угроз безопасности информации также является актуальной проблемой, которая влияет на определение приоритетных угроз безопасности. Одной из причин ее возникновения является различная квалификация аналитиков и их профессиональный опыт. Даже при использовании методики ФСТЭК, которая регламентирует подходы к оценке угроз, индивидуальный подход каждого специалиста может влиять на результаты. Для снижения субъективного влияния в методике предлагается формировать экспертные группы, чтобы учитывать мнения нескольких специалистов. Такой подход позволяет достичь более объективных оценок [15]. Недостаточная квалификация персонала приводит к ошибкам в классификации угроз. При подключении внешних аудиторов проблема усугубляется: не имея глубокого погружения в архитектуру обследуемой системы, режимы ее работы и межсистемные связи, они получают неполную картину рисков [20–25]. Кроме того, целесообразно использовать автоматизированные средства, способные сверять экспертные выводы с объективными данными и при необходимости их корректировать [18].

ЗАКЛЮЧЕНИЕ

Проведенный анализ показал, что существующие подходы к оценке актуальности киберугроз нуждаются в доработке. Ограниченность рассматриваемых сценариев, отсутствие систематического обновления данных, несогласованность в классификации нарушителей и влияние субъективных факторов снижают эффективность действующих методик. Такой упрощенный и статичный подход не соответствует динамичному характеру современной киберсреды, где методы атак совершенствуются чрезвычайно быстро.

Представленные в статье рекомендации позволяют повысить точность и актуальность оценки угроз. Для формирования более точной оценки актуальности угроз безопасности информации дополнительно к методике ФСТЭК необходимо предпринять ряд мер. Во-первых, важно проанализировать все возможные сценарии реализации угроз, а не ограничиваться только одним вариантом. Во-вторых, следует внедрить централизованный механизм регулярного обновления данных о техниках и тактиках атак. Кроме того, необходимо привести классификацию нарушителей в Банке данных угроз в соответствии с методикой ФСТЭК. Также для снижения субъективности в оценке угроз рекомендуется формировать экспертные группы и использовать автоматизированные инструменты анализа. Реализация этих мер позволит своевременно реагировать на меняющиеся условия, адаптировать защитные системы к новым вызовам и повысить их общую устойчивость.

Таким образом, рассмотренные способы совершенствования методов оценки актуальности киберугроз могут послужить основой для дальнейшего развития отраслевых стандартов, улучшения существующих решений и в конечном итоге для повышения уровня информационной безопасности на практике.

СПИСОК ЛИТЕРАТУРЫ

1. Методический документ ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации». – URL: https://sudact.ru/law/metodicheskii-dokument-metodika-otsenki-ugroz-bezopasnosti-informatsii/ (дата обращения: 05.06.2025).

2. *Комарова Т.А., Карачанская Е.А.* Анализ методики оценки угроз безопасности информации. Проблемные вопросы при разработке модели угроз // Информационные технологии в науке и образовании: материалы Всероссийской научно-практической конференции (Хабаровск, 15–16 декабря 2023 г.). – Хабаровск, 2024. – С. 183–185.

3. *Баронов О.Р., Марковина Е.Ю.* Практическое применение методических материалов ФСТЭК по определению актуальных угроз // Цифровая трансформация: тенденции и перспективы: сборник трудов I Международной научно-практической конференции. – М., 2022. – С. 245–249.

4. ФСТЭК России. Банк данных угроз безопасности информации. Раздел угроз. – URL: https://bdu.fstec.ru/threat-section (дата обращения: 05.06.2025).

5. *Жук Р.В.* Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. – 2021. – Т. 7, № 2. – С. 95–101.

6. MITRE Corporation. MITRE ATT&CK®: A Knowledge Base of Adversary Tactics and Techniques. – URL: https://attack.mitre.org (accessed: 05.06.2025).

7. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных». – URL: http://ivo.garant.ru/#/document/12148567/paragraph/24880:0/ (дата обращения: 05.06.2025).

8. Приказ ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17/ (дата обращения: 05.06.2025).

9. Приказ ФСТЭК России от 18 февраля 2013 № 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: 05.06.2025).

10. Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 15.03.2021) «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 природной среды». – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 05.06.2025).

11. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «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: 05.06.2025).

12. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В.И. Васильев, А.М. Вуль-

фин, А.Д. Кириллова, Н.В. Кучкарова // Системы управления, связи и безопасности. – 2021. № 3. – С. 110–134.

13. *Иванов К.А., Солдатов А.Ю., Селифанов В.В.* Моделирование процессов управления угрозами // Интерэкспо Гео-Сибирь. – 2024. – Т. 7, № 3. – С. 95–101.

14. Национальная база данных уязвимостей. Раздел уязвимостей. – URL: https://nvd.nist.gov/vuln/search (дата обращения: 06.06.2025).

15. *Пашков Н.Н., Дрозд В.Г.* Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. – 2020. – № 1. – URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 06.06.2025).

16. ГОСТ Р 53113.1–2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения: введ. 2009–10–01. – М.: Стандартинформ, 2018. – 12 с.

17. *Мельников П.В., Ешенко Р.А.* Проблемы формирования модели угроз информационной безопасности в информационных системах // Вестник науки. – 2020. – Т. 1, № 6 (27). – С. 185–189.

18. *Степанов В.А., Андреев Н.Д.* Моделирование угроз безопасности информации по новой методике ФСТЭК, используя средства автоматизации // Информационные технологии. Проблемы и решения. – 2021. – № 4 (17). – С. 95–101.

19. *Смирнов Р.А., Новиков С.Н.* Исследование методик оценки угроз безопасности информации // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 250–257.

20. *Ерышов В.Г.* Подход к оценке актуальности угроз безопасности информации в автоматизированных системах организации // Перспективные исследования в технических и естественных науках: сборник статей международной научной конференции, Великий Новгород, 22 декабря 2022 г. – СПб., 2022. – С. 18–20.

21. *Иванов А.В., Огнев И.А., Селифанов В.В.* Вопросы оценки эффективности аудита информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 4 (54). – С. 37–48.

22. *Мартыненко К.К., Ценина А.В., Селифанов В.В.* Моделирование процесса управления рисками и оценка его эффективности // Интеллектуальный потенциал Сибири: 32-я Региональная научная студенческая конференция, Новосибирск, 20–25 мая 2024 года. В 5 ч. Ч. 3. – Новосибирск: НГТУ, 2024. – С. 506–508.

23. *Солдатов А.Ю., Иванов А.В., Селифанов В.В.* Вопросы построения модели системы управления угрозами информационной безопасности // Ин-

терэкспо Гео-Сибирь. – 2024. – Т. 6. – С. 248–255. – DOI: 10.33764/2618-981X-2024-6-248-255.

24. Метод оценивания рисков в системах принятия решений с учетом защиты информации / В.В. Селифанов, А.Ю. Солдатов, Е.Ю. Солдатов, Подлегаев А.П., Скориков В.С. // Вестник СибГУТИ. – 2023. – Т. 17, № 2. – С. 84–92. – DOI: 10.55648/1998-6920-2023-17-2-84-92.

25. *Селифанов В.В.*, *Аникеева В.В.*, *Огнев И.А.* Вопросы оценки доверия к системе управления рисками // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 69–82. – DOI: 10.17212/2782-2230-2023-1-69-82.

Никрошкин Иван Владимирович, ассистент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – кибербезопасность, мониторинг событий безопасности, экспертные системы. E-mail: I.nikroshkin@corp.nstu.ru

Савенкова Анжелика Викторовна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: savenkova.2021@stud.nstu.ru

DOI: 10.17212/2782-2230-2025-2-9-24

Problems of assessing the relevance of information security threats*

I.V. Nikroshkin[1], A.V. Savenkova[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, assistant at the Department of Information Security. E-mail: i.nikroshkin@ corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: savenkova.2021@stud.nstu.ru*

The article is devoted to the analysis of problematic aspects of assessing the relevance of cyber threats in modern information security techniques. The disadvantages of the existing approach are considered, including the limited coverage of threat scenarios, the lack of mechanisms for regularly updating data on attack tactics and techniques, the non-unified classification of violators, and the subjective nature of assessments. It is proposed to expand the sources of threat information by integrating data from domestic and foreign knowledge bases (CAPEC, ATT&CK, OWASP, STIX, WASC), introduce automated scenario generation tools

* *Received 12 May 2025.*

based on semantic analysis, improve the classification of violators and ensure systematic updating of the threat model. The implementation of these recommendations will improve the objectivity, completeness and relevance of cyber threat assessment, improving the effectiveness of the protection measures taken.

Keywords: information security, threat model, threat model expertise, threats, information protection, threats to information security

REFERENCES

1. Methodological document FSTEC of Russia dated 02.05.2021 “Methodology for assessing information security threats”. (In Russian). Available at: https://sudact.ru/law/metodicheskii-dokument-metodika-otsenki-ugroz-bezopasnosti-informatsii/ (accessed 05.06.2025).

2. Komarova T.A., Karachanskaya E.A. [Analysis of the methodology for assessing information security threats. Problem issues when developing a threat model]. *Informatsionnye tekhnologii v nauke i obrazovanii* [Information technologies in science and education]. Proceedings of the All-Russian Scientific and Practical Conference (Khabarovsk, December 15–16, 2023). Khabarovsk, 2024, pp. 183–185. (In Russian).

3. Baronov O.R., Markovina E.Yu. [Practical application of the FSTEC methodological materials for the identification of current threats]. *Tsifrovaya transformatsiya: tendentsii i perspektivy* [Digital transformation: trends and prospects]. Proceedings of the First International Scientific and Practical Conference. Moscow, 2022, pp. 245–249. (In Russian).

4. FSTEC of Russia. Bank dannykh ugroz bezopasnosti informatsii. Razdel ugroz [Threats to information security. Threat section]. (In Russian). Available at: https://bdu.fstec.ru/threat-section (accessed 05.06.2025).

5. Zhuk R.V. Sposob opredeleniya potentsiala narushitelya bezopasnosti informatsii i realizuemykh im uyazvimostei programmnogo obespecheniya [Method for determining the potential of an information security intruder and realizable software vulnerabilities]. *Trudy uchebnykh zavedenii svyazi = Proceedings of Telecommunication Universities*, 2021, vol. 7, no. 2, pp. 95–101.

6. MITRE Corporation. MITRE ATT&CK®: A Knowledge Base of Adversary Tactics and Techniques. Available at: https://attack.mitre.org (accessed 05.06.2025).

7. Federal Law No. 152-FZ of July 27, 2006 “On Personal Data”. (In Russian). Available at: http://ivo.garant.ru/#/document/12148567/paragraph/24880:0 (accessed 05.06.2025).

8. FSTEC of Russia Order No. 17 dated February 11, 2013 “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/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (accessed 05.06.2025).

9. FSTEC of Russia Order No. 21 February 18, 2013 "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 05.06.2025).

10. FSTEC of Russia Order No. 31 March 14, 2014 (as amended on 15.03.2021) "On Approval of Requirements for Information Security in Automated Control Systems for Production and Technological Processes at Critical Facilities, Potentially Dangerous Facilities, as well as Facilities that pose an Increased Danger to Human Life and Health and to the Environment". (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed 05.06.2025).

11. FSTEC of Russia Order No. 239 December 25, 2017 (as amended on 20.02.2020) "On Approval of Requirements for Ensuring the Security 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 05.06.2025).

12. Vasiliev V.I., Vulfin A.M., Kirillova A.D., Kuchkarova N.V. Metodika otsenki aktual'nykh ugroz i uyazvimostei na osnove tekhnologii kognitivnogo modelirovaniya i Text Mining [Methodology for assessing current threats and vulnerabilities based on cognitive modeling technologies and Text Mining]. *Sistemy upravleniya, svyazi i bezopasnosti = Systems of Control, Communication and Security*, 2021, no. 3, pp. 110–134.

13. Ivanov K.A., Soldatov A.Yu., Selifanov V.V. Modelirovanie protsessov upravleniya ugrozami [Modelling of threat management processes]. *Interekspo Geo-Sibir' = Interexspo Geo-Siberia*, 2024, vol. 7, no. 3, pp. 95–101.

14. National Vulnerability Database. Vulnerability Section. Available at: https://nvd.nist.gov/vuln/search (accessed 06.06.2025).

15. Pashkov N.N., Drozd V.G. Analiz riskov informatsionnoi bezopasnosti i otsenka effektivnosti sistem zashchity informatsii na predpriyatii [Information security risk analysis and assessment of the effectiveness of information security systems at enterprises]. *Sovremennye nauchnye issledovaniya i innovatsii = Modern scientific research and innovations*, 2020, no. 1. Available at: https://web.snauka.ru/issues/2020/01/90380 (accessed 06.06.2025).

16. State Standard R 53113.1–2008. *Information technology. Protection of information technologies and automated systems against security threats posed by*

use of covert channels. Pt. 1. *General principles*. Moscow, Standartinform Publ., 2018. 12 p. (In Russian).

17. Melnikov P.V., Yeshenko R.A. Problemy formirovaniya modeli ugroz informatsionnoi bezopasnosti v informatsionnykh sistemakh [Problems of forming a model of information security threats in information systems]. *Vestnik nauki*, 2020, vol. 1, no. 6 (27), pp. 185–189. (In Russian).

18. Stepanov V.A., Andreev N.D. Modelirovanie ugroz bezopasnosti informatsii po novoi metodike FSTEK, ispol'zuya sredstva avtomatizatsii [Modeling information security threats using the new FSTEC methodology using automation tools]. *Informatsionnye tekhnologii. Problemy i resheniya = Information technology*, 2021, no. 4 (17), pp. 95–101.

19. Smirnov R.A., Novikov S.N. Issledovanie metodik otsenki ugroz bezopasnosti informatsii [Research on information security risk assessment techniques]. *Interekspo Geo-Sibir' = Interexpo Geo-Siberia*, 2022, vol. 6, pp. 250–257.

20. Eryshov V.G. [An approach to assessing the relevance of information security threats in an organization's automated systems]. *Perspektivnye issledovaniya v tekhnicheskikh i estestvennykh naukakh* [Prospective research in technical and natural sciences]. A collection of articles from an international scientific conference. St. Petersburg, 2022, pp. 18–20. (In Russian).

21. Ivanov A.V., Ognev I.A., Selifanov V.V. Voprosy otsenki effektivnosti audita informatsionnoi bezopasnosti [Issues of assessing the effectiveness of information security audit]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information Security*, 2024, no. 4 (54), pp. 37–48.

22. Martynenko K.K., Tsenina A.V., Selifanov V.V. [Modeling of the risk management process and evaluation of its effectiveness]. *Intellektual'nyi potentsial Sibiri* [Intellectual potential of Siberia]. The 32nd Regional Scientific Student Conference. In 5 pt. Pt. 3. Novosibirsk, NSTU Publ., 2024, pp. 506–508. (In Russian).

23. Soldatov A.Yu., Ivanov A.V., Selifanov V.V. Voprosy postroeniya modeli sistemy upravleniya ugrozami informatsionnoi bezopasnosti [Issues of building a model of information security threat management system]. *Interekspo Geo-Sibir' = Interexpo Geo-Siberia*, 2024, vol. 6, pp. 248–255. DOI: 10.33764/2618-981X-2024-6-248-255.

24. Selifanov V.V., Soldatov A.Yu., Soldatov E.Yu., Podlegaev A.P., Skorikov V.S. Metod otsenivaniya riskov v sistemakh prinyatiya reshenii s uchetom zashchity informatsii [Risk assessment method in decision-making systems taking into account information protection]. *Vestnik SibGUTI = The Herald of the Siberian State University of Telecommunications and Information Science*, 2023, vol. 17 (2), pp. 84–92. DOI: 10.55648/1998-6920-2023-17-2-84-92.

25. Selifanov V.V., Anikeeva V.V., Ognev I.A. Voprosy otsenki doveriya k sisteme upravleniya riskami [Issues of assessing the credibility of the risk management system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 69–82. DOI: 10.17212/2782-2230-2023-1-69-82.

Для цитирования:

Никрошкин И.В., Савенкова А.В. Проблемы оценки актуальности угроз безопасности информации // Безопасность цифровых технологий. – 2025. – № 2 (117). – С. 9–24. – DOI: 10.17212/2782-2230-2025-2-9-24.

For citation:

Nikroshkin I.V., Savenkova A.V. Problemy otsenki aktual'nosti ugroz bezopasnosti informatsii [Problems of assessing the relevance of information security threats]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 2 (117), pp. 9–24. DOI: 10.17212/2782-2230-2025-2-9-24.