УДК 004.056.5
DOI 10.33764/2618-981X-2022-6-250-257

Исследование методик оценки угроз безопасности информации

Р. А. Смирнов[1]*, *С. Н. Новиков*[1,2]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: smirroma98@mail.ru

Аннотация. Появление новых технологий не только порождает новые способы атак, но и расширяет существующий перечень угроз, а, как известно, каждая угроза может быть осуществлена большим количеством различных атак. На сегодняшний день существуют методики, основанные на различных подходах к исследованию угроз безопасности информации такие, как: оценка актуальности угроз безопасности информации по методике ФСТЭК России, по ATT&CK Matrix for Enterprise, по таксономии инцидентов Ховарда-Лонгстаффа, исследование оценки угроз безопасности информации, основанное на модели безопасности. Все вышеперечисленные методики можно разбить на две группы оценки угроз: количественная и качественная. В связи с чем возникает необходимость провести их исследование. В статье представлено исследование методик оценки угроз безопасности информации, проведённое разными способами.

Ключевые слова: информационная безопасность, угроза, методика

Research on Information Security Risk Assessment Techniques

R. A. Smirnov[1]*, *S. N. Novikov*[1, 2]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: smirroma98@mail.ru

Abstract. The emergence of new technologies not only generates new methods of attacks, but also expands the existing list of threats, and, as you know, each threat can be carried out by a large number of different attacks. To date, there are methods based on various approaches to the study of information security threats, such as: assessment of the relevance of information security threats according to the FSTEC methodology of Russia, ATT&CK Matrix for Enterprise, Howard-Longstaff incident taxonomy, information security threat assessment study based on a security model. All of the above methods can be divided into two groups of threat assessment: quantitative and qualitative. In this connection, there is a need to conduct their research. The article presents a study of methods for assessing information security threats, conducted in various ways.

Keywords: information security, threat, methodology

Введение

Появление новых технологий снижает уровень защищенности существующих систем. В связи с этим на первый план выходит необходимость формирования полного перечня угроз информации, однако данная проблема не имеет про-

стого решения. Для решения этой задачи создаются различные модели угроз, в основе которых лежат всевозможные математические аппараты и информационные модели.

Значительный вклад в развитие теории и практики защиты информации в информационных системах, внесли: А.А. Грушо, Н.А. Гайдамакин, В.А. Герасименко, П.Д. Зегжда, А.М. Ивашко, С.М. Климов, И.Д. Королев, А.И. Костогрызов, А.С. Кузьмин, А.И. Куприянов, В.В. Меньших, О.Б. Макаревич, В.Ф. Макаров, С.Н. Новиков, А. М. Сычев, А.А. Стрельцов, Л.М. Ухлинов, А.В. Черемушкин, В.Ф. Шаньгин, и др. В их исследованиях разработана концепция защиты информации, обоснованы принципы обеспечения информационной безопасности и построения систем защиты информации объектов информатизации, а также сформулированы основы построения моделей угроз и нарушителей безопасности информации.

Цель работы: провести исследование методик оценки угроз безопасности информации.

Для достижения цели, необходимо решить ряд задач:

1) провести оценку актуальности угроз безопасности информации по методике ФСТЭК России;

2) исследовать оценку угроз безопасности информации по ATT&CK Matrix for Enterprise;

3) провести анализ методики оценки угроз безопасности информации по таксономии инцидентов Ховарда-Лонгстаффа;

4) исследовать оценку угроз безопасности информации, основанную на модели безопасности.

1 Оценка актуальности угроз безопасности информации по методике ФСТЭК России

Исходными данными для оценки актуальности угроз безопасности информации являются [1]:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов компьютерных атак, содержащихся в базах данных и иных информационных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с методикой ФСТЭК России;

г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с методикой ФСТЭК России;

д) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с методикой ФСТЭК России;

е) актуальные способы реализации (возникновения) угроз безопасности информации.

Приведем пример определения актуальных угроз безопасности информации, определенный по методике ФСТЭК России, на примере условной организации «Х» (табл. 1) [2,3].

Таблица 1

Актуальные угрозы безопасности информации, определенные по методике ФСТЭК России

Код	Название	Источник угрозы	Объект воздействия	Последствия, реализации угрозы
1	2	3	4	5
УБИ. 008	Угроза восстановления и/или повторного использования аутентификационной информации	Внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	Нарушение конфиденциальности
УБИ. 014	Угроза длительного удержания вычислительных ресурсов пользователями	Внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Нарушение доступности
УБИ. 034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Нарушение конфиденциальности, целостности, доступности

Методика оценки угроз безопасности информации ФСТЭК России имеет следующие достоинства и недостатки:

а) достоинства:

– методика ориентирована на оценку антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей;

– методика разделяет угрозы на возможные и актуальные.

б) недостатки:

– методика имеет качественную оценку (экспертная оценка);

– методика не имеет возможности определения степени ущерба последствий реализации угрозы.

2 Исследование оценки угроз безопасности информации по ATT&CK Matrix for Enterprise

Матрица MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) – это глобально доступная база знаний о тактике и технике злоумышленника, основанная на реальных наблюдениях. Данная база знаний ATT&CK используется в качестве основы для разработки моделей и методологий угроз [4, 5].

Матрица позволяет строить модели угроз для разных типов компаний и показывать, какие из известных угроз можно закрыть конкретными решениями. В теории это выглядит так: компания, выбирающая решения для защиты своей инфраструктуры, проецирует возможности злоумышленника на матрицу ATT&CK и смотрит, какие актуальные угрозы остались незакрытыми.

По данной методике рассмотрена база знаний и выбраны наиболее подходящие угрозы безопасности информации для условной организации «Х» (табл. 2).

Таблица 2

Анализ оценки угроз безопасности информации
по ATT&CK Matrix for Enterprise [4]

Характеристика	Этап жизненного цикла			
	Проектирование	Построение/реконструкция	Эксплуатация	Вывод из эксплуатации
1	2	3	4	5
Аппаратные дополнения	-	-	+	+
Доверенные отношения	+	+	+	+
Действительные аккаунты	-	+	+	+
Управление учетными записями	-	-	+	+
Внешние удаленные сервисы	-	-	+	+
Избыточный доступ	-	-	+	+
Использование уязвимостей для повышения привилегий	-	-	+	+
Отключение средств безопасности	-	-	+	+
Учетные данные в файлах	-	+	+	+
Эксплуатация уязвимостей для доступа к учетным записям	-	-	+	+
Обнаружение политики паролей	-	+	+	+
Обнаружение информации о конфигурации сети	+	+	+	+
Обнаружение сетевых подключений системы	-	-	+	-
Эксплуатация удаленных сервисов (эксплуатация уязвимостей в программном обеспечении)	-	-	+	+
Внутренний фишинг	-	-	+	+
Удаление доступа к аккаунту	-	-	+	-
Уничтожение данных	-	-	+	+
Шифрование данных	-	-	+	+
Отказ в обслуживании	-	-	+	-

Методика оценки угроз безопасности информации по ATT&CK Matrix for Enterprise имеет следующие достоинства и недостатки:

а) достоинства:

– методика позволяет строить модели угроз для разных типов компаний и показывать, какие из известных угроз можно закрыть конкретными решениями. Помогает понять, какие инструменты используют злоумышленники, ознакомиться с их техниками и тактиками. Эти знания позволяют прогнозировать вероятную точку входа в организации. Активное и повсеместное применение базы знаний ATT&CK позволит унифицировать подход всего сообщества кибербезопасности — как бы поможет говорить на общем языке.

б) недостатки:

– методика имеет качественную оценку (экспертная оценка).

3 Исследование оценки угроз безопасности информации, основанное на модели безопасности

Третий вариант анализа оценки угроз безопасности информации основан на модели безопасности.

В данном способе для исследования оценки угроз безопасности информации используются такие характеристики, как мотивация, цели, уровень квалификации, используемые программно-технические средства, осведомленность (наличие достаточно необходимой информации об объекте разрушающего деструктивного воздействия (РДВ)), локация (пути проникновения в защищаемую сеть), пространственно-временные характеристики [6, 7].

В табл. 3 приведен анализ угроз безопасности информации по данным характеристикам для условной организации «X» [6].

Таблица 3

Анализ угроз безопасности информации, основанный на модели безопасности

Характеристика	Этап жизненного цикла			
	Проектирование	Построение/реконструкция	Эксплуатация	Вывод из эксплуатации
1	2	3	4	5
1. Мотивация				
Случайные, непреднамеренные действия, ошибки использования доверенной системы	+	+	+	+
Преднамеренные действия (злой умысел, сговор)	+	+	+	+
2. Цели				
РДВ связанные с уничтожением сетевого элемента	-	-	+	-
РДВ связанные с несанкционированным доступом к критически важной информации, служебному трафику и т.д.	-	-	+	+

Окончание табл. 3

Характеристика	Этап жизненного цикла			
	Проектирование	Построение/реконструкция	Эксплуатация	Вывод из эксплуатации
Неспецифические РДВ решающие сторонние задачи	+	+	+	+
3. Уровень квалификации				
Дилетант	+	+	+	-
Начинающий специалист	+	+	+	+
Профессионал (группа профессионалов)	+	+	+	+
4. Используемые программно-технические средства				
Персональный компьютер	+	+	+	+
Группа серверов	-	-	+	+
Мобильное устройство	+	+	+	+
Специальная техника для НСД, РДВ	+	+	+	+
5. Осведомлённость, наличие достаточно необходимой информации об объекте РДВ				
Внешний субъект относительно сети	+	+	+	+
Внутренний субъект относительно сети	+	+	+	+
6. Локация/Пути проникновения в защищаемую сеть				
Из внешних сетей по отношению к атакуемому объекту	-	-	+	-
Из родительской сети связи (пользователь, имеющий доступ к доверенной системе)	-	-	+	+
Случайный доступ по случайным маршрутам	-	-	+	+
7. Пространственно-временные характеристики				
Последовательное воздействие по каналу РДВ на определенном уровне модели сети связи	-	-	+	+

Методика оценки угроз безопасности информации, основанный на модели безопасности имеет следующие достоинства и недостатки:

а) достоинства: достаточно объемный перечень характеристик, по которым определяются угрозы;

б) недостатки: методика имеет качественную оценку (экспертная оценка).

4 Анализ методики оценки угроз безопасности информации по таксономии инцидентов Ховарда-Лонгстаффа

Четвертый способ анализа методики оценки угроз безопасности информации проведён с помощью таксономии «Common Language for Computer Security Incidents (Общий язык для инцидентов компьютерной безопасности)», авторами которого являются Джон Ховард и Томас Лонгстафф. Данная таксономия была подготовлена в Национальной лаборатории Сандиа (Sandia National Laboratories) по заказу энергетического департамента правительства США и используется по настоящий момент [8, 9].

В таксономии авторы выделили семь характеристик, с помощью которых проводится анализ угроз безопасности информации: атакующий, средства, уязвимости, действия, объекты воздействия, результат несанкционированных действий, цели.

На основании данных характеристик был проведен анализ угроз безопасности информации на примере условной организации «Х» (табл. 4).

Таблица 4

Актуальные угрозы безопасности информации, определенные по таксономии инцидентов Ховарда-Лонгстаффа [8, 10]

Характеристика	Этап жизненного цикла			
	Проектирование	Построение/реконструкция	Эксплуатация	Вывод из эксплуатации
1	2	3	4	5
1. Атакующие				
Хакеры	+	-	+	-
Шпионы	-	-	-	-
Террористы	-	-	-	-
Корпоративные мошенники	+	+	+	+
Злоумышленники	+	+	+	+
Вандалы	+	+	+	+
Маньяки	+	+	+	+
2. Средства				
Средство физической атака	+	+	+	+
Средство обмена информацией	+	+	+	+
Сценарий или программа	-	-	+	+
Средство перехвата данных	-	-	+	+
3. Уязвимости				
Уязвимости проектирования	+	+	+	+
Уязвимости реализации	-	+	+	+
Уязвимости конфигурирования	-	+	+	+
4. Действия				
Сканирование	-	-	+	-
Копирование	+	+	+	+
Аутентификация	-	-	+	+

Методика оценки угроз безопасности информации по таксономии инцидентов Ховарда-Лонгстаффа имеет следующие достоинства и недостатки:

а) достоинства: достаточно хорошая проработка категорий определения угроз;

б) недостатки:

– построение классификации для уже осуществленных атак;

– методика имеет качественную оценку (экспертная оценка).

Заключение

Исходя из проделанной работы при исследовании методик оценки угроз безопасности информации, были определены как достоинства, так и недостатки.

Методики ФСТЭК России, ATT&CK Matrix for Enterprise, таксономии инцидентов Ховарда-Лонгстаффа, модели безопасности – каждая из них, имеет свою уникальность. Но при этом, все вышеперечисленные методики имеют один общий недостаток: качественную оценку (экспертную оценку) определения угроз безопасности информации. Как известно, данная оценка является неточной, так как носит субъективный характер.

На основании вышеизложенного, можно сделать вывод о том, что применение только качественных методик оценки угроз безопасности информации недостаточно, необходимо осуществлять количественную оценку, основанную на математических подходах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Методика оценки угроз безопасности ФСТЭК России: официальный сайт. – Москва. - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения: 05.01.2022) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

2. Банк данных угроз безопасности информации: официальный сайт. – Москва. - URL: https://bdu.fstec.ru/threat (дата обращения: 25.01.2022) – Текст: электронный. – Режим доступа: для авторизир. пользователей.

3. ГОСТ Р 56546-2015 Национальный стандарт российской федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2018 г., официальный сайт – Россия - URL: https://docs.cntd.ru/document/1200123702 (дата обращения: 03.02.2022) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

4. ATT&CK Matrix for Enterprise: официальный сайт. – США. – URL: https://attack.mitre.org/ (дата обращения: 15.02.2022) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

5. *Горбачев И.Е., Глухов А.П.* Моделирование процессов нарушения информационной безопасности критической инфраструктуры// Труды СПИИРАН. – Москва, 2015. – Вып. 1(38). – С. 112 – 135.

6. Попков Г.В. Применение нестационарных гиперсетей в методах проектирования мультисервисных сетей связи в условиях разрушающих деструктивных воздействий. официальный сайт – Новосибирск – URL: https://elibrary.ru/item.asp?id=39937096& (дата обращения: 20.02.2022) – Текст: электронный. – Режим доступа: для зарегистрир. пользователей.

7. *Котенко И. В.* Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. – Москва, 2004. – № 1. – С. 56–72.

8. A Common Language for Computer Security Incidents: официальный сайт. – США. – URL: https://prod-ng.sandia.gov/techlib-noauth/access control.cgi/1998/988667.pdf (дата обращения: 19.03.2022) – Текст: электронный. – Режим доступа: для авторизир. пользователей.

9. *Щеглов А.Ю.* «Защита компьютерной информации от несанкционированного доступа». – СПб.: Наука и Техника, 2004. – 384 с.

10. *Астахов А.* Введение в аудит информационной безопасности., 2018 г. официальный сайт –Россия – URL: http://globaltrust.ru (дата обращения: 20.03.2022). – Текст: электронный. – Режим доступа: для авторизир. пользователей.