DOI 10.36622/1682-7813.2024.27.2.012
УДК 004.056

КИБЕРАТАКИ ВИДА «АНАЛИЗ ЦЕЛЕВОГО ОБЪЕКТА»: РИСК-ЛАНДШАФТ ВЕКТОРОВ АТАК И УЯЗВИМОСТЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В.В. Смирнов, А.П. Васильченко, А.А. Остапенко, А.В. Гречишкин, С.С. Куликов, Д.Н. Рахманин

Анализируются широко распространённые атаки, обеспечивающие сбор, накопление информации атакуемом объекте в целях подготовки кибератак на телекоммуникационные системы и сети. Для многочисленных типов таких нападений идентифицируются соответствующие им уязвимости, классифицированные в базе знаний CVE. В работе проанализированы сочетания векторов атак и уязвимостей, предусмотрено использование калькулятора CVSS. Выявлены наиболее опасные пары сочетаний «вектор атаки-уязвимость». Оценены потенциальный ущерб кибератаки «анализ целевого объекта» и его вероятность. Построен риск-ландшафт сечений рассматриваемых пар атака-уязвимость. В результате выявлены наиболее опасные сочетания, которые требуют первоочередного противодействия для обеспечения безопасности защищаемых телекоммуникационных сетей.

Ключевые слова: уязвимость, атака, безопасность, риск, ущерб, вероятность, телекоммуникационные сети, анализ целевого объекта.

Введение

Обилие кибератак, постоянно обрушающихся на отечественное информационное пространство, объективно требует обеспечения необходимой технической и организационно-правовой защиты современных телекоммуникационных сетей (ТКС) от сочетаний векторов (сценариев) реализации атак и уязвимостей ТКС, используемых злоумышленниками [1]. В этой связи персоналу, защищающему ТКС, приходится иметь дело с сотнями известных злоумышленных сценариев и тысячами выявленных уязвимостей, порождающими десятки тысяч их сочетаний, каждое из которых имеет свою специфику реагирования средств и органов защиты [2-6]. Однако эффективность этого противодействия может быть существенно повышена при наличии адекватных риск-оценок, регламентации мер противоборства [1] через построение риск-ландшафтов, которые представляли собой трехмерную поверхность риска, построенную на плоскости уязвимостей и векторов атак. Для атак вида «анализ целевого объекта» представляет интерес построение сечений, связанных с векторами атак и уязвимостями с целью выявления наиболее опасных сочетаний «вектор атаки-уязвимость» и построения на этой основе риск-ландшафта. Именно в этом контексте представляется актуальным настоящее исследование, посвященное атакам класса «анализ целевого объекта», активно реализуемых в современном киберпространстве.

Таким образом, цель исследования состоит в повышении защищенности ТКС за счет построения риск-ландшафта и выявления наиболее опасных сочетаний атак «анализ целевого объекта» и уязвимостей.

1 Формирование множества векторов атак и соответствующих им уязвимостей для атак вида «анализ целевого объекта»

Вектора атак этой категории направлены на сбор, накопление и кражу информации злоумышленником. Полученная информация может помочь противнику сделать выводы о потенциальных слабостях, уязвимостях или методах, способствующих достижению его целей. Эта информация может включать в себя сведения о конфигурации или возможностях объекта, сведения о времени и характере действий, а также другую конфиденциальную информацию. Зачастую такие атаки проводятся в рамках подготовки к другим видам вторжений, хотя в некоторых случаях сбор информации сам по себе может быть конечной целью злоумышленника.

CISA KEV (Cybersecurity and Infrastructure Security Agency Known Exploited Vulnerabilities) – это каталог известных уязвимостей, которые активно эксплуатируются злоумышленниками [6].

Используя CISA KEV, мы отбраковываем уязвимости, которые не актуальны и отбираем наиболее часто эксплуатируемые уязвимости, таким образом сокращая их количество для каждого вектора.

Анализ осуществим для множества векторов атак, отобранных по вышеуказанному принципу. Полученное множество атак для анализа представлено в табл. 1.

Таблица 1

Векторы атак класс «анализ целевого объекта»

Вектор атак	Описание
CAPEC-127	Индексирование каталогов
CAPEC-215	Фаззинг для отображения приложений
CAPEC-143	Обнаружение непубличных веб-страниц
CAPEC-157	Атаки с использованием сниффинга
CAPEC-31	Доступ/перехват/изменение HTTP Cookies
CAPEC-57	Использование доверия к системному ресурсу REST для получения конфиденциальных данных
CAPEC-634	Периферийные устройства Probe Audio и Video
CAPEC-462	Временные рамки междоменного поиска
CAPEC-285	ICMP Echo Request Ping
CAPEC-619	Отслеживание силы сигнала
CAPEC-291	Передача зон DNS
CAPEC-85	AJAX Footprinting
CAPEC-646	Периферийный отпечаток
CAPEC-694	Обнаружение местоположения системы
CAPEC-170	Отпечатки в веб-приложениях
CAPEC-191	Чтение чувствительных констант внутри исполняемого файла
CAPEC-463	Атака Padding Oracle Crypto
CAPEC-383	Сбор информации с помощью мониторинга событий API
CAPEC-639	Проверка системных файлов
CAPEC-586	Инъекция объектов

2 Оценка рисков успешной реализации атак

Воспользуемся методикой, предложенной в [1].

Для оценки опасности применения того или иного вектора атаки и соответствующих ему уязвимостей в базе знаний (данных) NIST [5] предусмотрено использование калькулятора CVSS.

В основе третьей версии калькулятора CVSS для оценки вероятностей использования уязвимостей могут быть использованы следующие показатели:

1) тип доступа (сетевой, локальный, через смежную сеть, физический доступ);

2) сложность выпуска кода (низкий, высокий);

3) необходимый уровень привилегий (не нужен, низкий, высокий);

4) взаимодействие с пользователем (требуется, не требуется).

Отсюда вероятность успешного использования j-ой уязвимости посредством i-ой атаки имеет вид:

$$P_{AY} = P_{Ai} \prod_{m=1}^{4} P_{Yj}(m),$$

где $P_{Yj}(m)$ для m = 1(1)4 определяется из вышеперечисленных показателей;

P_{Ai} – вероятность успеха i-ой атаки, определяется по шкале {0; 0,1; 0,3; 0,5; 0,7; 0,9} по полям калькулятора.

При этом ущербы оцениваются по шкале {0; 0,2; 0,5} раздельно для каждого вида (конфиденциальность, целостность, доступность) $\overline{U_{\text{к}}}$, $\overline{U_{\text{ц}}}$, $\overline{U_{\text{д}}}$, которые можно интерпретировать как доли утраченного информационного ресурса (соответствующего качества). Алгебраическое суммирование данных ущербов некорректно ввиду различия их сущностей.

Тогда риск необходимо рассчитать раздельно для каждого вида ущерба по следующим выражениям:

$$\begin{aligned} \overline{Risk_{\text{к}}} &= P_{AY}\,\overline{U_{\text{к}}}; \\ \overline{Risk_{\text{ц}}} &= P_{AY}\,\overline{U_{\text{ц}}}; \\ \overline{Risk_{\text{д}}} &= P_{AY}\,\overline{U_{\text{д}}}. \end{aligned} \qquad (1)$$

Занесем в табл. 2 исходные данные, необходимые для риск-анализа для уязвимостей наибольшей опасности из табл. 1.

Таблица 2

Исходные данные, необходимые для риск-анализа

CAPEC	P(Ai)	P(Yj)	AV	AC	PR	UI	U(к)	U(ц)	U(д)	CVE
CAPEC-127	0,7	0,4745	0,85	0,77	0,85	0,85	0,5	0,5	0,5	CVE-2023-46747
		0,4745	0,85	0,77	0,85	0,85	0,5	0,5	0,5	CVE-2023-42793
CAPEC-285	0,5	0,4745	0,85	0,77	0,85	0,85	0,5	0,5	0,2	CVE-2016-6415
CAPEC-462	0,5	0,4745	0,85	0,77	0,85	0,62	0,5	0,5	0,5	CVE-2016-6277
CAPEC-586	0,5	0,4745	0,85	0,77	0,85	0,85	0,5	0,5	0,5	CVE-2023-27350
CAPEC-31	0,7	0,4745	0,85	0,77	0,85	0,62	0,5	0,5	0,5	CVE-2023-41266
CAPEC-463	0,7	0,4729	0,85	0,77	0,85	0,85	0,5	0,5	0,5	CVE-2020-2021
CAPEC-383	0,5	0,4745	0,85	0,77	0,85	0,85	0,5	0,5	0,5	CVE-2023-34441
CAPEC-170	0,7	0,4745	0,85	0,77	0,85	0,85	0,5	0,5	0,5	CVE-2022-1902

Далее рассчитаем риски раздельно для каждого вида ущерба (конфиденциальность, целостность, доступность). Ниже приведены результаты вычислений (табл. 3).

Таблица 3

Риски для каждой пары VA-CVE

CVE	Risk U(к)	Risk U(ц)	Risk U(д)
CVE-2023-46747	0,166058394	0,166058394	0,166058394
CVE-2023-42793	0,166058394	0,166058394	0,166058394
CVE-2016-6415	0,118613139	0,118613139	0,059306569
CVE-2016-6277	0,118613139	0,118613139	0,118613139
CVE-2023-27350	0,118613139	0,118613139	0,118613139
CVE-2023-41266	0,166058394	0,166058394	0,166058394
CVE-2020-2021	0,165506688	0,165506688	0,165506688
CVE-2023-34441	0,118613139	0,118613139	0,118613139
CVE-2022-1902	0,166058394	0,166058394	0,166058394

На основе полученных данных построены (рис. 1-8) графики сечений риск-ландшафта для наиболее опасных сочетаний «вектор атаки-уязвимость».

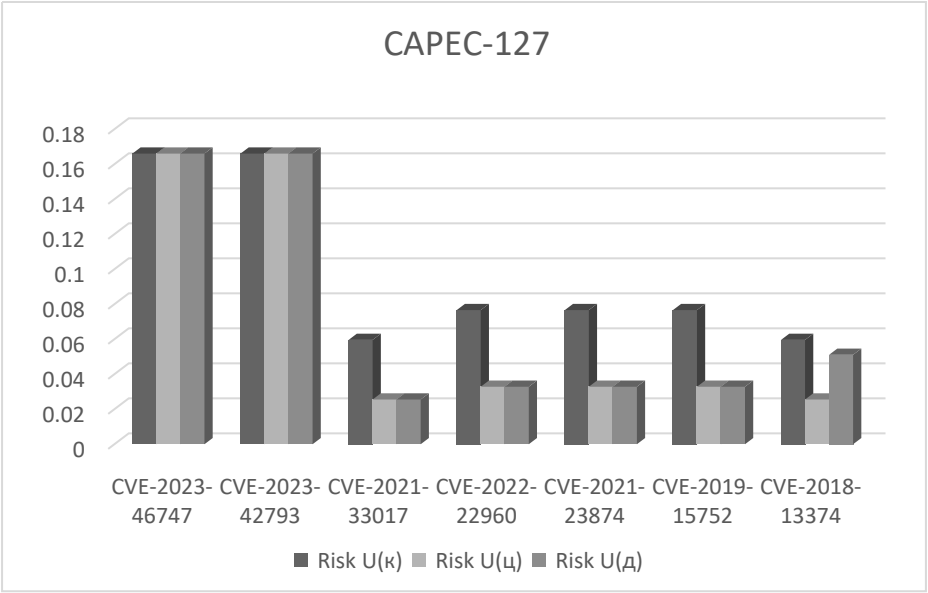

Рис. 1. Риск-ландшафт для CAPEC-127

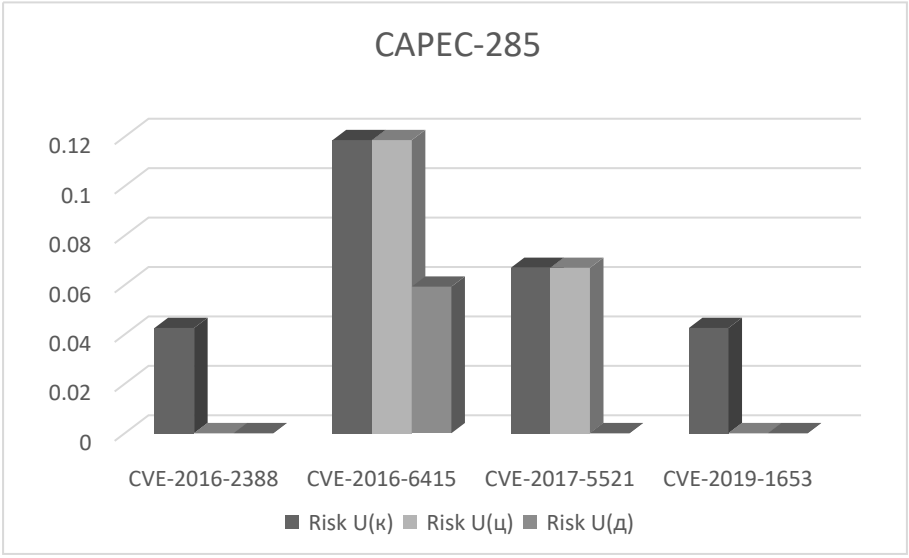

Рис. 2. Риск-ландшафт для CAPEC-285

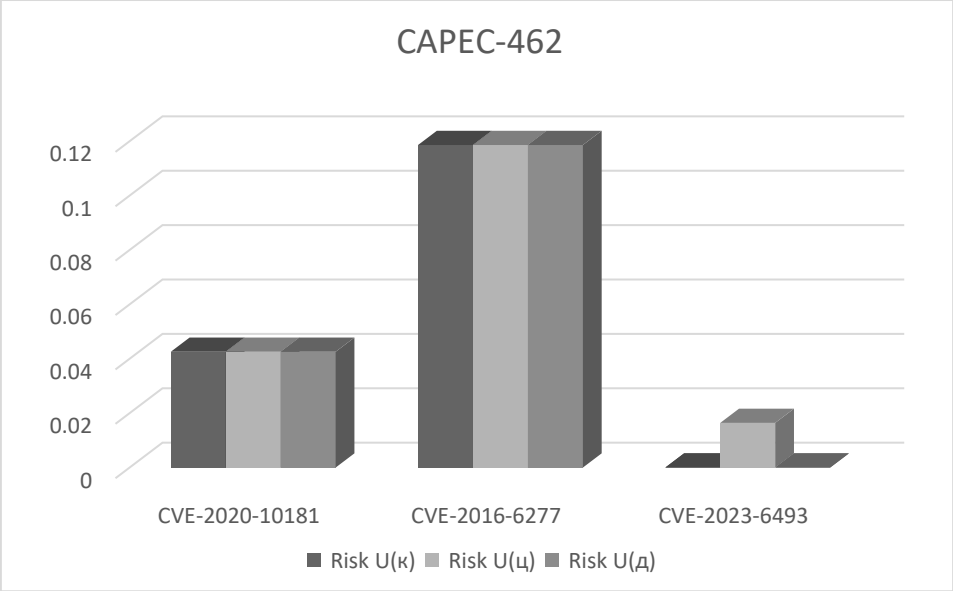

Рис. 3. Риск-ландшафт для CAPEC-462

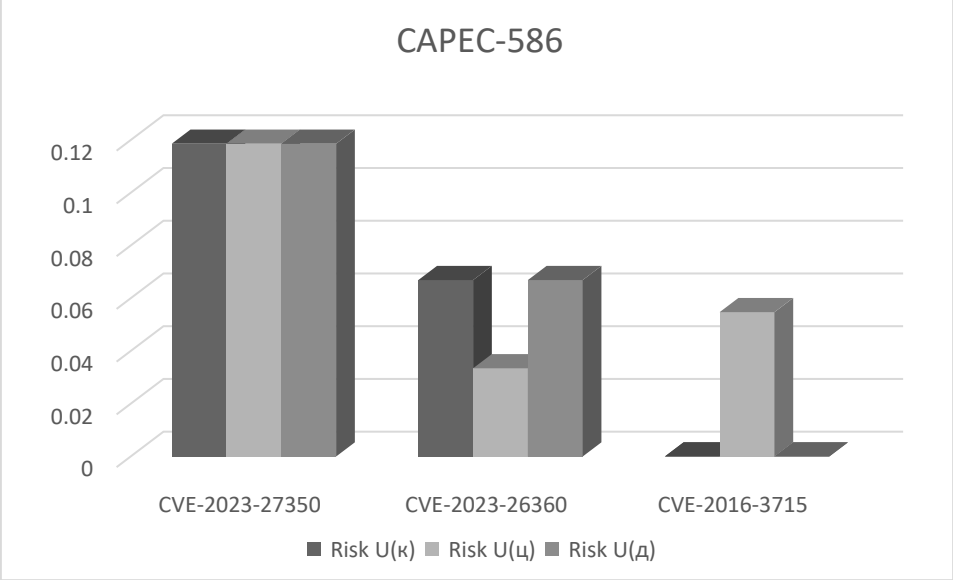

Рис. 4. Риск-ландшафт для CAPEC-586

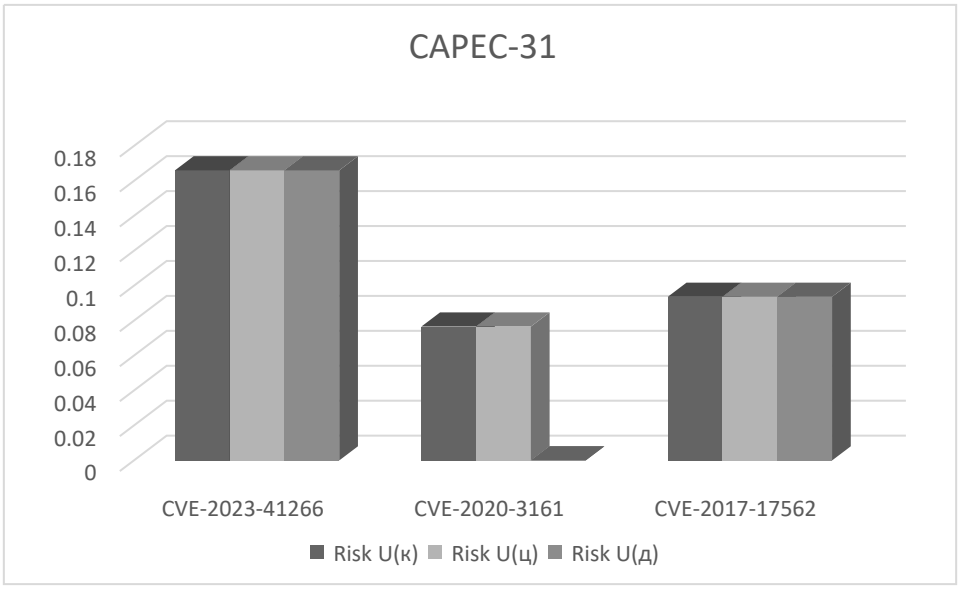

Рис. 5. Риск-ландшафт для CAPEC-31

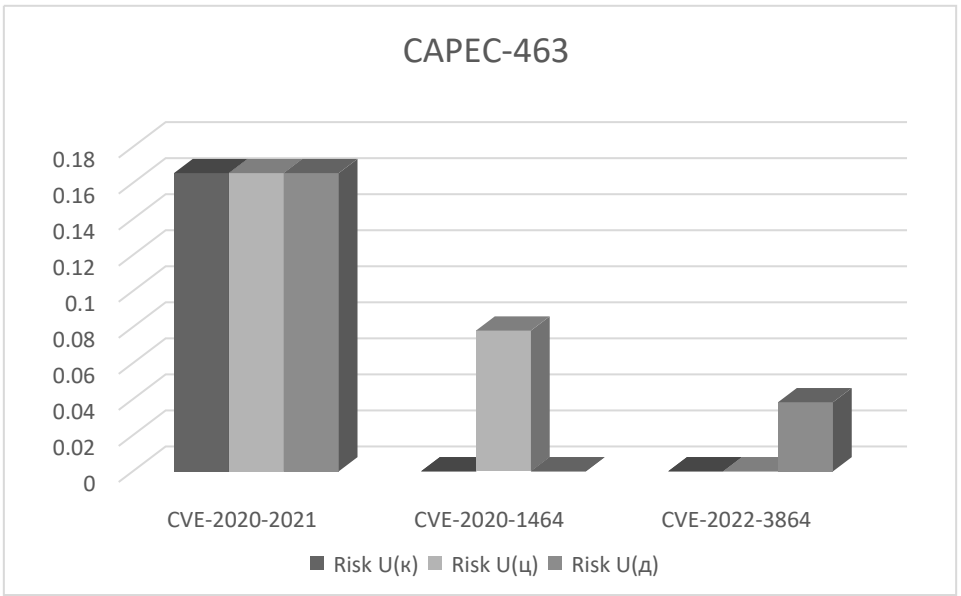

Рис. 6. Риск-ландшафт для CAPEC-463

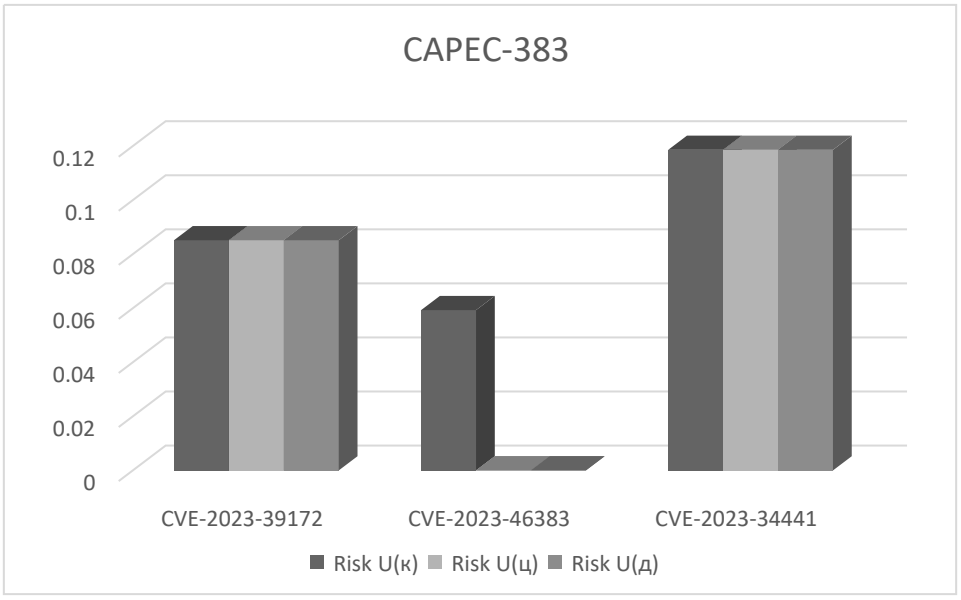

Рис. 7. Риск-ландшафт для CAPEC-383

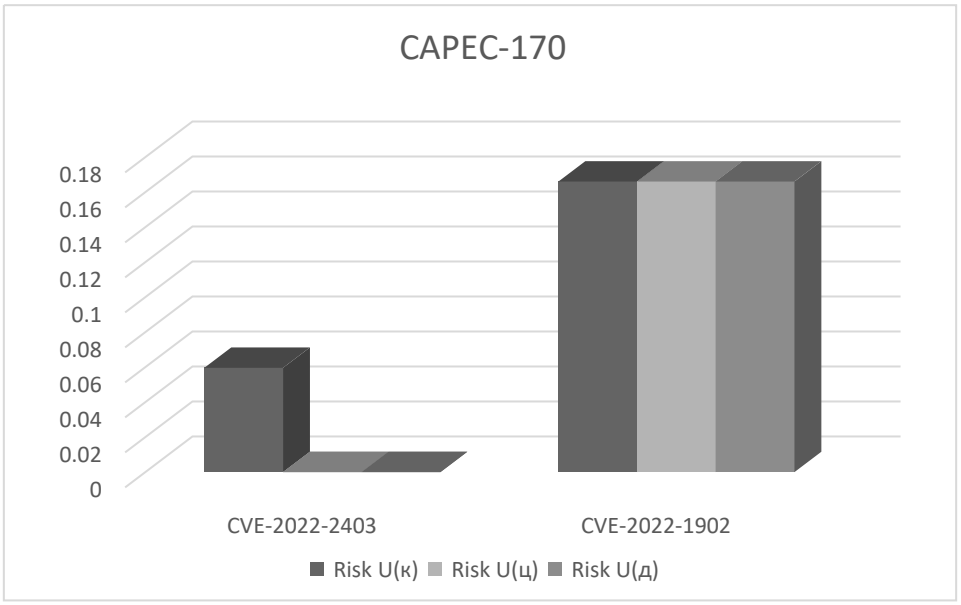

Рис. 8. Риск-ландшафт для CAPEC-170

Полученные графики сечений риск-ландшафта для наиболее опасных сочетаний «вектор атаки-уязвимость» (рис. 1-8) дают возможность наглядно и наиболее точно выявить самые опасные сочетания, противодействие которым имеет первостепенное значение. Выбранные опасные пары атака-уязвимость приведены ниже (табл. 4).

Таблица 4

Множество наиболее опасных пар «вектор атаки – уязвимость»

Вектор атаки	Уязвимость	Идентификатор уязвимости
CAPEC-127	Нераскрытые запросы могут обойти аутентификацию конфигурационной утилиты, что позволит злоумышленнику, имеющему сетевой доступ к системе BIG-IP через порт управления и/или собственные IP-адреса, выполнить произвольные системные команды.	CVE-2023-46747
CAPEC-127	НВ JetBrains TeamCity до версии 2023.05.4 был возможен обход аутентификации, приводящий к RCE на сервере TeamCity Server.	CVE-2023-42793
CAPEC-285	Реализация сервера IKEv1 в Cisco IOS 12.2-12.4 и 15.0-15.6, IOS XE до версии 3.18S, IOS XR 4.3.x и 5.0.x-5.2.x, а также PIX до версии 7.0 позволяет удаленным злоумышленникам получить конфиденциальную информацию из памяти устройства через запрос на согласование ассоциации безопасности (SA), идентификаторы ошибок CSCvb29204 и CSCvb36055 или BENIGNCERTAIN.	CVE-2016-6415
CAPEC-462	NETGEAR R6250 до 1.0.4.6.Beta, R6400 до 1.0.1.18.Beta, R6700 до 1.0.1.14.Beta, R6900, R7000 до 1.0.7.6.Beta, R7100LG до 1.0.0.28.Beta, R7300DST до 1.0.0.46.Beta, R7900 до 1. 0.1.8.Beta, R8000 до 1.0.3.26.Beta, D6220, D6400, D7000 и, возможно, другие маршрутизаторы позволяют удаленным злоумышленникам выполнять произвольные команды с помощью метасимволов shell в информации о пути к cgi-bin/.	CVE-2016-6277
CAPEC-586	Уязвимость позволяет удаленным злоумышленникам обойти аутентификацию на затронутых установках PaperCut NG 22.0.5 (Build 63914).	CVE-2023-27350
CAPEC-31	Уязвимость обхода пути, обнаруженная в Qlik Sense Enterprise для Windows для версий May 2023 Patch 3 и ранее, February 2023 Patch 7 и ранее, November 2022 Patch 10 и ранее и August 2022 Patch 12 и ранее, позволяет удаленному	CVE-2023-41266

Продолжение табл. 4

Вектор атаки	Уязвимость	Идентификатор уязвимости
CAPEC-463	Когда включена аутентификация Security Assertion Markup Language (SAML) и отключена опция 'Validate Identity Provider Certificate', неправильная проверка подписей при аутентификации PAN-OS SAML позволяет неаутентифицированному сетевому злоумышленнику получить доступ к защищенным ресурсам.	CVE-2020-2021
CAPEC-383	Baker Hughes - Прошивка Bently Nevada 3500 System TDI версии 5.05 содержит уязвимость передачи открытого текста, которая может позволить злоумышленнику украсть секрет аутентификации из трафика связи с устройством и использовать его для произвольных запросов.	CVE-2023-34441
CAPEC-170	Обнаружен изъян в Red Hat Advanced Cluster Security for Kubernetes. Секреты Notifier не были должным образом обработаны в GraphQL API. Этот недостаток позволяет аутентифицированным пользователям ACS получать Notifiers из GraphQL API, раскрывая секреты, которые могут повысить их привилегии.	CVE-2022-1902

Для выбранных опасных пар атака-уязвимость (табл. 4) по формулам (1) вычисляем риски для ущербов конфиденциальности, целостности и доступности. Полученные результаты вычисления рисков для самых опасных сочетаний уязвимостей и векторов атак вида «анализ целевого объекта» представлены в табл. 5.

Таблица 5

Риск-оценка опасных сочетаний

Идентификатор CAPEC	Идентификатор CVE	$Risk_к$	$Risk_ц$	$Risk_д$
CAPEC-127	CVE-2023-46747	0,166058	0,166058	0,166058
CAPEC-127	CVE-2023-42793	0,166058	0,166058	0,166058
CAPEC-285	CVE-2016-6415	0,1186131	0,118613	0,059306

Продолжение табл. 5

Идентификатор CAPEC	Идентификатор CVE	$Risk_к$	$Risk_ц$	$Risk_д$
CAPEC-462	CVE-2016-6277	0,118613	0,118613	0,118613
CAPEC-586	CVE-2023-27350	0,118613	0,118613	0,118613
CAPEC-31	CVE-2023-41266	0,166058	0,166058	0,166058
CAPEC-463	CVE-2020-2021	0,166058	0,166058	0,166058
CAPEC-383	CVE-2023-34441	0,118613	0,118613	0,118613
CAPEC-170	CVE-2022-1902	0,166058	0,166058	0,166058

Риск-ландшафт для атак класса «анализ целевого объекта» в виде совокупности наиболее опасных сочетаний указывает на необходимость усиления мер защиты для снижения данных рисков до приемлемого уровня.

Заключение

В представленной работе был построен риск-ландшафт в виде его сечений по векторам и уязвимостям для самых опасных сочетаний атак класса «анализ целевого объекта», которые обычно предваряют кибервторжения.

Ответственность противодействия на данном его этапе особенно высока, ибо по процедурам, реализуемым в данном случае злоумышленником, возможно спрогнозировать цели его устремлений. Фактически, проводя сетевую разведку, он пытается определить направление главного удара по наиболее уязвимым компонентам атакуемой системы. В этой связи, риск-ландшафт даёт администратору безопасности возможность оценить наиболее ущербные сочетания «вектор-уязвимость», которые нуждаются в особой защите. Специфика защищаемых в этом случае объектов позволит осуществить оперативные настройки и предложить превентивные меры, предупреждающие успешность будущих кибератак, подготовкой которых на этапе анализа целевого объекта занят злоумышленник. Инциденты таких злоумышленных действий, зафиксированные администрацией защищаемой системы, однозначно укажут службе информационной безопасности на участки повышенной опасности, где следует прежде всего организовывать управление рисками с использованием риск-ландшафта, построенного для всего известного многообразия пар «вектор-уязвимость» в отношении рассматриваемого класса кибератак «анализ целевого объекта».

Новизна полученных результатов заключается в том, что впервые построен риск-ландшафт для атак класса «анализ

целевого объекта» и выявлены наиболее опасные сочетания векторов, рассматриваемые в представленной работе, кибератак и используемых ими уязвимостей.

Практическая ценность результатов видится в том, что построенный риск-ландшафт в силу его организации в виде совокупности сечений позволяет наглядно выявить наиболее опасные сочетания векторов и уязвимостей в отношении атак класса «анализ целевого объекта».

Теоретическая значимость результатов просматривается в том, что предложенные риск-метрики имеют перспективу своего теоретического развития в плане их адаптации к специфике защищаемых ТКС и анализа опасности векторов атак класса «анализ целевого объекта» для одновременного использования нескольких уязвимостей.

Автоматизация предлагаемых методик позволит создать инструментарий, удобный для специалистов по защите информации при обеспечении безопасности телекоммуникационных сетей различного назначения.

Список литературы

1. Организационно-правовая защита сетей / Г. А. Остапенко, Д. В. Щербакова, А. О. Калашников и др.; под ред. Академика РАН Д. А. Новикова. -: Горячая линия Телеком, 2023.-228с.:

2. The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org/ (дата обращения: 9.01.2024).

3. NIST Information Technology Laboratory National Vulnerability Database. URL: https://nvd.nist.gov/vuln (дата обращения: 9.01.2024).

4. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 9.01.2024).

5. База данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения: 9.01.2024).

6. Каталог известных эксплуатируемых уязвимостей (CISA KEV). URL: https://www.cisa.gov/known-vulnerabilities-catalog (дата обращения: 9.01.2024).

Воронежский государственный технический университет
Voronezh State Technical University

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Поступила в редакцию 10.01.2024

Информация об авторах

Смирнов Владислав Вячеславович – студент, Воронежский государственный технический университет, e-mail: smirnovchib@yandex.ru

Васильченко Алексей Павлович – аспирант, Финансовый университет при Правительстве Российской Федерации, e-mail: zainichek@uandex.ru

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Гречишкин Александр Владимирович – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Куликов Сергей Сергеевич – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Рахманин Дмитрий Николаевич – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

CYBER ATTACKS OF THE "TARGET OBJECT ANALYSIS" TYPE: RISK LANDSCAPE OF ATTACK VECTORS AND VULNERABILITIES OF TELECOMMUNICATION NETWORKS

V.V. Smirnov, A.P. Vasilchenko, A.A. Ostapenko, A.V. Grechishkin, S.S. Kulikov, D.N. Rakhmanin

Widespread attacks are analyzed that ensure the collection and accumulation of information on the attacked object in order to prepare other types of cyberattacks on telecommunication systems and networks. The purpose of the study is to increase the security of the telecommunications network by identifying the most dangerous “attack vector-vulnerability” combinations and building their risk landscape. For numerous types of such attacks, corresponding vulnerabilities are identified and classified in the CVE knowledge base. The work analyzes combinations of attack vectors and vulnerabilities, and provides for the use of the CVSS calculator. Potential damage and its probability are assessed. The risk landscape of the attacks under consideration has been constructed. As a result, the most dangerous combinations have been identified that require priority counteraction to ensure the security of protected telecommunication networks.

Keywords: vulnerability, attack, security, risk, damage, probability, telecommunication networks, analysis of the target object.

Submitted 07.01.2024

Information about the authors

Vladislav V. Smirnov – student, Voronezh State Technical University, e-mail: smirnovchib@yandex.ru
Alexey P. Vasilchenko – graduate student, Financial University under the Government of the Russian Federation, e-mail: zainichek@uandex.ru
Alexander A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com
Alexander V. Grechishkin – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Sergey S. Kulikov – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Dmitry N. Rakhmanin – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com