DOI 10.36622/1682-7813.2024.27.2.013
УДК 004.056

КИБЕРАТАКИ ВИДА «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»: РИСК-ЛАНДШАФТ ВЕКТОРОВ АТАК И УЯЗВИМОСТЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Э.И. Жидков, А.П. Васильченко, А.А. Остапенко, А.С. Кольцов, Е.А. Шварцкопф, А.С. Щеголеватых

Рассматриваются широко распространенные атаки в киберпространстве, которые сосредоточены на манипулировании людьми и их эксплуатации. В работе установлено соответствие векторов атак CAPEC и используемых ими уязвимостей CVE. Для полученных в результате сочетаний «вектор атаки – уязвимость» предлагается вычисление ожидаемых ущербов и вероятностей их наступления с использованием полей CVSS-калькуляции. Таким способом удалось построить риск-ландшафт рассматриваемого многообразия атак в виде совокупности сечений поверхностей рисков по векторам и уязвимостям. Предлагаемый подход предоставляет возможность выявления наиболее опасных сечений, которые нуждаются в первоочередном регулировании в целях обеспечения безопасности защищаемых телекоммуникационных сетей.

Ключевые слова: уязвимость, атака, безопасность, риск, ущерб, вероятность, телекоммуникационные сети, социальная инженерия.

Введение

Кибератаки вида «социальная инженерия» ориентированы на манипулирование людьми для того, чтобы убедить цель атаки совершить действия или разгласить конфиденциальную информацию, которые приносят пользу злоумышленнику.

Атаки класса «социальная инженерия» наносят значительный ущерб телекоммуникационным сетям (ТКС). В известных классификациях кибератак [1-6] эта категория выделена в отдельный вид, борьба с которыми требует особого внимания и эффективность противодействия может быть существенно повышена с помощью адекватной оценки рисков [1,7,8]. Поэтому, в дополнении к регламентации мер противоборства [1] предлагается построение риск-ландшафтов, которые представляют собой трехмерную поверхность риска, построенную на плоскости уязвимостей и векторов атак. Для атак вида «социальная инженерия» такой ландшафт еще не строился и практический интерес представляют прежде всего сечения такой поверхности по ее «хребтам», что позволит выявить наиболее опасные сочетания вектор-уязвимость. При этом необходимо первоначально потребуется найти всевозможные такие сочетания из баз знаний и данных [2-6].

1 Формирование множества векторов атак и соответствующих им уязвимостей для атак вида «социальная инженерия»

Объектом исследования является пространство функционирования ТКС, подвергающихся кибератакам вида «социальная инженерия».

Предметом исследования является оценка рисков возникновения киберинцидентов для атак вида «социальная инженерия».

Целью исследования является повышение защищенности атакуемых ТКС, за счет построения и исследования риск-ландшафта атак вида «социальная инженерия».

Для достижения поставленной цели необходимо решить следующие задачи:

– в виде сечений по векторам и уязвимостям построить риск-ландшафт для атак вида «социальная инженерия», реализуемых в отношении ТКС;

– выявление наиболее опасных сочетаний вектор-уязвимость для атак вида «социальная инженерия».

Для решения поставленных задач необходимо воспользоваться следующими базами данных и знаний:

1. Вектор атаки (CAPEC – Common Attack Pattern Enumeration and Classification):

CAPEC представляет собой систематизированную базу данных, разработанную Open Web Application Security Project (OWASP) в сотрудничестве с международным сообществом экспертов по безопасности.

2. Тип ошибки (CWE – Common Weakness Enumeration):

База данных CWE – это каталог известных типов ошибок, которые могут возникнуть в программном обеспечении при его разработке, эксплуатации или обслуживании. CWE является общедоступным и совместно разрабатываемым проектом, который помогает в разработке безопасного программного обеспечения и повышает осведомленность о возможных типах ошибок

3. Уязвимость (CVE – Common Vulnerabilities and Exposures):

CVE — это список записей, каждая из которых идентифицирует конкретную уязвимость в программном обеспечении или системе. CVE предоставляет уникальный идентификатор, называемый CVE ID. CVE описывает известные уязвимости, которые уже были обнаружены и оценены экспертами.

Так с учетом вышеперечисленного, уместно отобрать самые наиболее эксплуатируемые уязвимости (на основе базы данных CISA KEV [6]) для множества векторов атак, представленного в табл. 1.

Таблица 1

Векторы атак класса «социальная инженерия»

Вектор атаки
CAPEC-182: Flash-инъекция
CAPEC-178: Межсайтовая Flash-инъекция
CAPEC-98: Фишинг
CAPEC-89: Фарминг
CAPEC-691: Поддельные метаданные программного обеспечения с открытым исходным кодом
CAPEC-473: Подделка подписи
CAPEC-616: Установление местоположения
CAPEC-103: Кликджэкинг
CAPEC-501: Перехват активности Android
CAPEC-504: Олицетворение задачи
CAPEC-506: Тапджэкинг
CAPEC-185: Загрузка вредоносного программного обеспечения
CAPEC-186: Обновление вредоносного программного обеспечения
CAPEC-697: DHCP-спуфинг
CAPEC-695: Подключение к репозиторию
CAPEC-587: Межкадровый скриптинг
CAPEC-383: Сбор информации с помощью мониторинга событий API

2 Расчет рисков реализации векторов атак в отношении уязвимостей

Воспользуемся методикой, предложенной А. А. Остапенко, введя следующие обозначения:

$Risk_{ij}$– это риск относительно пары «вектор атаки – используемая уязвимость»;

P_{ij}–вероятность успешности атаки для *i*-ой атаки и *j*-ой уязвимости;

P_i – вероятность успешной реализации *i*-ой атаки;

P_j – вероятность успешности эксплуатации *j*-ой уязвимости;

U_{ij} – ущерб *i*-ой атаки на *j*-ю уязвимость,

Получим следующее выражение для расчета риска:

$$Risk_{ij} = (P_i \times P_j) \times U_{ij},$$

При этом вероятность успешного использования j-ой уязвимости посредством i-ой атаки (на основе полей калькулятора CVSS) 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} – как вероятность успеха i-ой атаки определяется по шкале: очень низкая (0,1), низкая (0,3), средняя (0,5), высокая (0,7), очень высокая (0,9) по полям калькулятора соответственно.

В свою очередь, ущербы оцениваются раздельно для каждого их вида (конфиденциальность, целостность, доступность) $\overline{U_к}$, $\overline{U_ц}$, $\overline{U_д}$ по шкале: нет (0), низкий (0,2), высокий (0,5). Тогда риск необходимо рассчитать раздельно для каждого вида в следующем виде:

$$\overline{Risk_к} = P_{AY}\,\overline{U_к};$$
$$\overline{Risk_ц} = P_{AY}\,\overline{U_ц};$$
$$\overline{Risk_д} = P_{AY}\,\overline{U_д}.$$

Отсюда для заданного вида атак имеем расчетные данные (табл. 2).

Таблица 2

Исходные данные для риск-анализа

Вектор атаки	Уязвимость	$P_{Yj}(m)$	P_{Ai}	$\overline{U_к}$	$\overline{U_ц}$	$\overline{U_д}$
CAPEC-182	*CVE-2018-0112*	0,197098	0,5	0,5	0,5	0,5
	CVE-2016-9263	0,197098		0,2	0,2	0
	CVE-2015-0313	0,344922		0,5	0,5	0,5
CAPEC-178	*CVE-2022-31657*	0,472876	0,5	0,5	0,5	0,5
	CVE-2023-23860	0,472876		0,5	0,5	0
	CVE-2023-20263	0,344922		0,2	0,2	0
	CVE-2023-22797	0,344922		0,2	0,2	0
CAPEC-98	*CVE-2022-23646*	0,275937	0,7	0	0,5	0
	CVE-2023-36026	0,275937		0	0,2	0
	CVE-2023-6211	0,344922		0	0,5	0
CAPEC-89	*CVE-2023-3654*	0,472876	0,7	0,5	0,5	0,5
	CVE-2023-28794	0,344922		0,2	0	0
	CVE-2023-5859	0,344922		0	0,2	0
	CVE-2021-34561	0,197098		0,5	0,5	0,5
	CVE-2020-11091	0,15895		0	0,5	0
CAPEC- 691	*CVE-2008-3438*	0,223185	0,5	0,5	0,5	0
	CVE-2023-45799	0,344922		0,5	0,5	0,5
	CVE-2019-9534	0,344922		0,5	0,5	0,5
	CVE-2021-45027	0,15895		0,5	0	0

Продолжение табл. 2

Вектор атаки	Уязвимость	$P_{Yj}(m)$	P_{Ai}	$\overline{U_к}$	$\overline{U_ц}$	$\overline{U_д}$
CAPEC- 473	*CVE-2020-12852*	0,109563	0,5	0,5	0,5	0,5
	CVE-2018-9142	0,127534		0,5	0,5	0,5
	CVE-2018-1000125	0,472876		0,5	0,5	0,5
	CVE-2022-30273	0,472876		0,5	0,5	0,5
	CVE-2019-16378	0,472876		0,5	0,5	0,5
CAPEC- 616	*CVE-2022-20821*	0,344922	0,5	0,5	0,5	0
	CVE-2019-1653	0,472876		0,5	0	0
	CVE-2017-0059	0,344922		0,2	0	0
CAPEC-103	*CVE-2022-28889*	0,344922	0,5	0	0,2	0
	CVE-2022-27220	0,344922		0	0,2	0
	CVE-2023-41897	0,472876		0,5	0,5	0,5
	CVE-2021-43048	0,344922		0,5	0,5	0,5
CAPEC- 504	*CVE-2017-7440*	0,344922	0,5	0	0,5	0
	CVE-2022-20226	0,15895		0,2	0,2	0
	CVE-2022-28649	0,25159		0,2	0,2	0
CAPEC-501	*CVE-2012-5810*	0,344922	0,5	0,5	0,5	0,5
	CVE-2022-30319	0,344922		0,5	0,5	0
	CVE-2022-4390	0,472876		0,5	0,5	0,5
CAPEC-506	*CVE-2022-20212*	0,223185	0,3	0,5	0,5	0,5
	CVE-2021-39691	0,15895		0,5	0,5	0,5
	CVE-2021-39669	0,223185		0,5	0,5	0,5
	CVE-2021-39702	0,344922		0,5	0,5	0,5
CAPEC-185	*CVE-2022-27438*	0,275937	0,7	0,5	0	0,5
	CVE-2022-28944	0,344922		0,5	0,5	0
	CVE-2022-24644	0,344922		0,5	0	0
	CVE-2021-45027	0,472876		0,5	0,5	0,5
CAPEC-186	*CVE-2022-24140*	0,085833	0,7	0,5	0,5	0,5
	CVE-2022-27438	0,270215		0,5	0,5	0,5
	CVE-2023-40254	0,472876		0,5	0,5	0,5
	CVE-2023-22635	0,223185		0,5	0,5	0,2
CAPEC-697	*CVE-2022-30319*	0,344922	0,3	0,5	0,5	0,5
	CVE-2022-2663	0,472876		0	0,2	0
	CVE-2022-22547	0,275937		0,5	0	0
CAPEC-695	*CVE-2021-41037*	0,25159	0,5	0,2	0,2	0,2
	CVE-2022-1161	0,472876		0,5	0,5	0,5
	CVE-2022-23630	0,197098		0,5	0,5	0,5
CAPEC-587	*CVE-2018-18496*	0,344922	0,7	0,5	0,5	0,5
	CVE-2023-3140	0,344922		0	0,2	0
	CVE-2019-5243	0,344922		0	0,2	0
CAPEC-383	*CVE-2021-27779*	0,472876	0,3	0,5	0,5	0
	CVE-2022-24045	0,344922		0,5	0	0
	CVE-2022-26157	0,472876		0,2	0	0
	CVE-2022-21798	0,472876		0,5	0,5	0,5

Используя поля калькулятора CVSS и используемая уязвимость» получаем табл. 2 для каждой пары «вектор атаки – значения рисков (табл. 3).

Таблица 3

Риски для каждой пары VA-CVE

Вектор атаки	Уязвимость	$Risk_{к}$	$Risk_{ц}$	$Risk_{д}$
CAPEC-182	*CVE-2018-0112*	0,049275	0,049275	0,049275
	CVE-2016-9263	0,01971	0,01971	0
	CVE-2015-0313	0,08623	0,08623	0,08623
CAPEC-178	*CVE-2022-31657*	0,118219	0,118219	0,118219
	CVE-2023-23860	0,118219	0,118219	0
	CVE-2023-20263	0,034492	0,034492	0
	CVE-2023-22797	0,034492	0,034492	0
CAPEC-98	*CVE-2022-23646*	0	0,096578	0
	CVE-2023-36026	0	0,038631	0
	CVE-2023-6211	0	0,120723	0
CAPEC-89	*CVE-2023-3654*	0,165507	0,165507	0,165507
	CVE-2023-28794	0,048289	0	0
	CVE-2023-5859	0	0,048289	0
	CVE-2021-34561	0,068984	0,068984	0,068984
	CVE-2020-11091	0	0,055633	0
CAPEC-691	*CVE-2008-3438*	0,055796	0,055796	0
	CVE-2023-45799	0,08623	0,08623	0,08623
	CVE-2019-9534	0,08623	0,08623	0,08623
	CVE-2021-45027	0,039738	0	0
CAPEC-473	*CVE-2020-12852*	0,027391	0,027391	0,027391
	CVE-2018-9142	0,031884	0,031884	0,031884
	CVE-2018-1000125	0,118219	0,118219	0,118219
	CVE-2022-30273	0,118219	0,118219	0,118219
	CVE-2019-16378	0,118219	0,118219	0,118219
CAPEC-616	*CVE-2022-20821*	0,08623	0,08623	0
	CVE-2019-1653	0,118219	0	0
	CVE-2017-0059	0,034492	0	0

Продолжение табл. 3

Вектор атаки	Уязвимость	$Risk_{к}$	$Risk_{ц}$	$Risk_{д}$
CAPEC-103	*CVE-2022-28889*	0	0,034492	0
	CVE-2022-27220	0	0,034492	0
	CVE-2023-41897	0,118219	0,118219	0,118219
	CVE-2021-43048	0,08623	0,08623	0,08623
CAPEC-504	*CVE-2017-7440*	0	0,08623	0
	CVE-2022-20226	0,015895	0,015895	0
	CVE-2022-28649	0,025159	0,025159	0
CAPEC-501	*CVE-2012-5810*	0,08623	0,08623	0,08623
	CVE-2022-30319	0,08623	0,08623	0
	CVE-2022-4390	0,118219	0,118219	0,118219
CAPEC-506	*CVE-2022-20212*	0,033478	0,033478	0,033478
	CVE-2021-39691	0,023843	0,023843	0,023843
	CVE-2021-39669	0,033478	0,033478	0,033478
	CVE-2021-39702	0,051738	0,051738	0,051738
CAPEC-185	*CVE-2022-27438*	0,096578	0	0,096578
	CVE-2022-28944	0,120723	0,120723	0
	CVE-2022-24644	0,120723	0	0
	CVE-2021-45027	0,165507	0,165507	0,165507
CAPEC-186	*CVE-2022-24140*	0,030042	0,030042	0,030042
	CVE-2022-27438	0,094575	0,094575	0,094575
	CVE-2023-40254	0,165507	0,165507	0,165507
	CVE-2023-22635	0,078115	0,078115	0,031246
CAPEC-697	*CVE-2022-30319*	0,051738	0,051738	0,051738
	CVE-2022-2663	0	0,028373	0
	CVE-2022-22547	0,041391	0	0

Окончание табл. 3

Вектор атаки	Уязвимость	$Risk_к$	$Risk_ц$	$Risk_д$
CAPEC-695	*CVE-2021-41037*	0,025159	0,025159	0,025159
	CVE-2022-1161	0,118219	0,118219	0,118219
	CVE-2022-23630	0,049275	0,049275	0,049275
CAPEC-587	*CVE-2018-18496*	0,120723	0,120723	0,120723
	CVE-2023-3140	0	0,048289	0
	CVE-2019-5243	0	0,048289	0
CAPEC-383	*CVE-2021-27779*	0,070931	0,070931	0
	CVE-2022-24045	0,051738	0	0
	CVE-2022-26157	0,028373	0	0
	CVE-2022-21798	0,070931	0,070931	0,070931

С использованием полученных данных, построен риск-ландшафт в виде сечений для векторов атак вида «социальная инженерия (рис. 1-9).

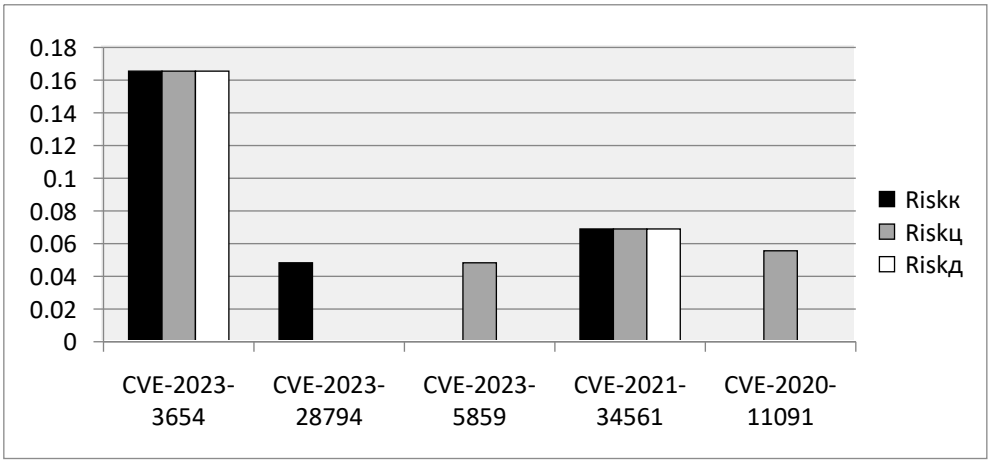

Рис. 1. Сечение риск-ландшафта для CAPEC 89

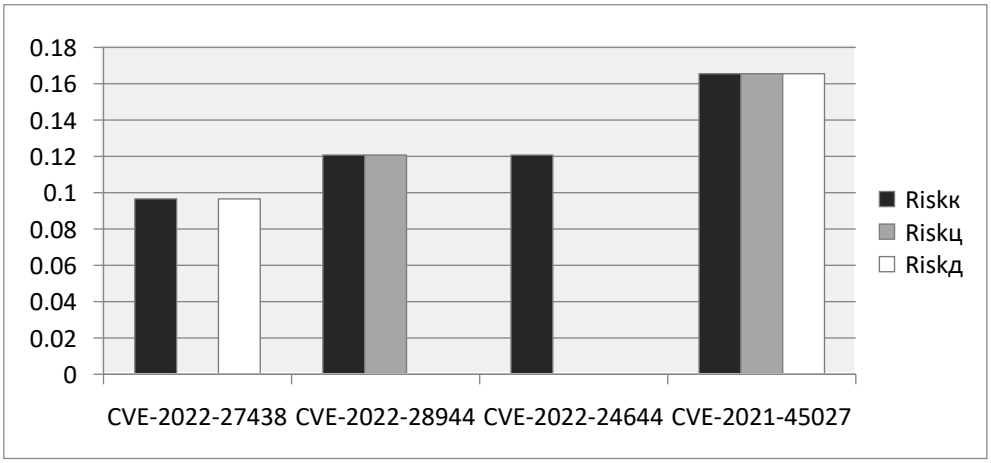

Рис. 2. Сечение риск-ландшафта для CAPEC 185

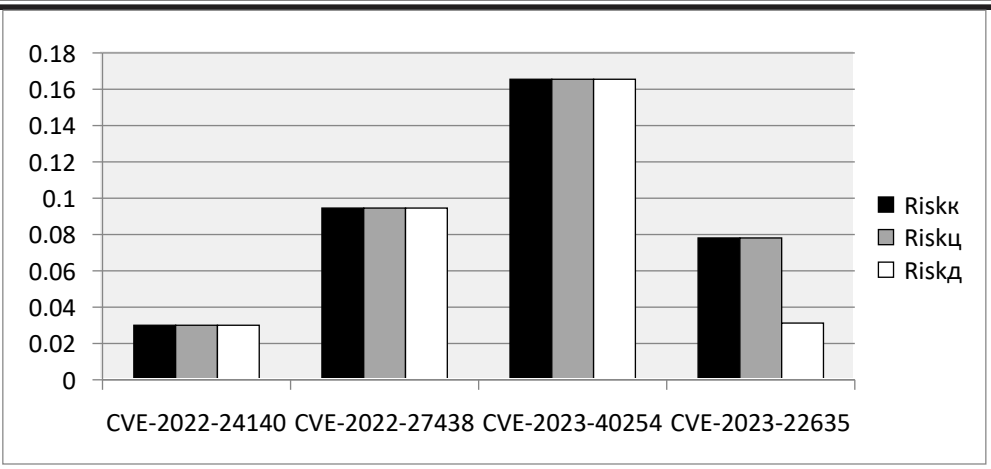

Рис. 3. Сечение риск-ландшафта для CAPEC 186

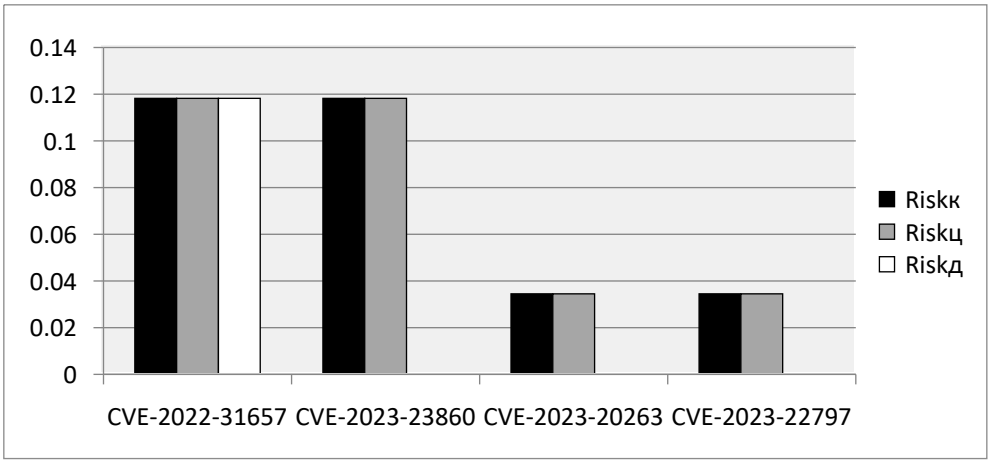

Рис. 4. Сечение риск-ландшафта для CAPEC 178

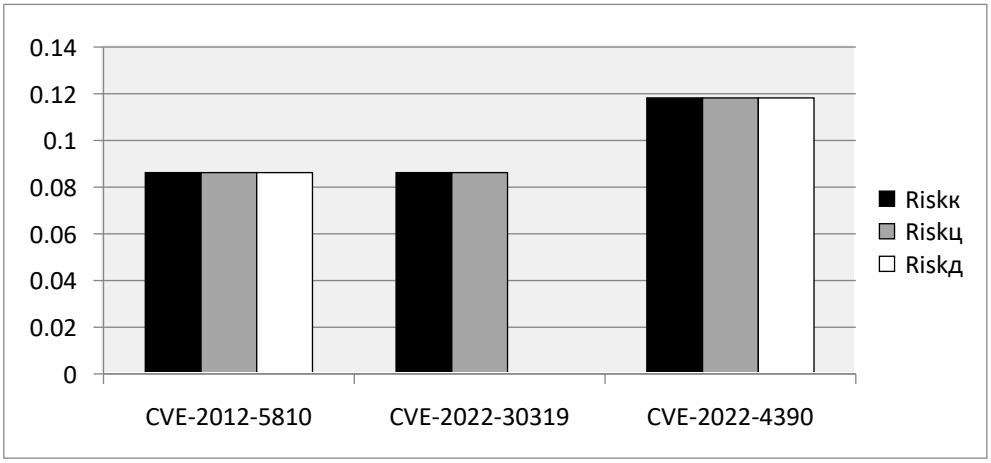

Рис. 5. Сечение риск-ландшафта для CAPEC 501

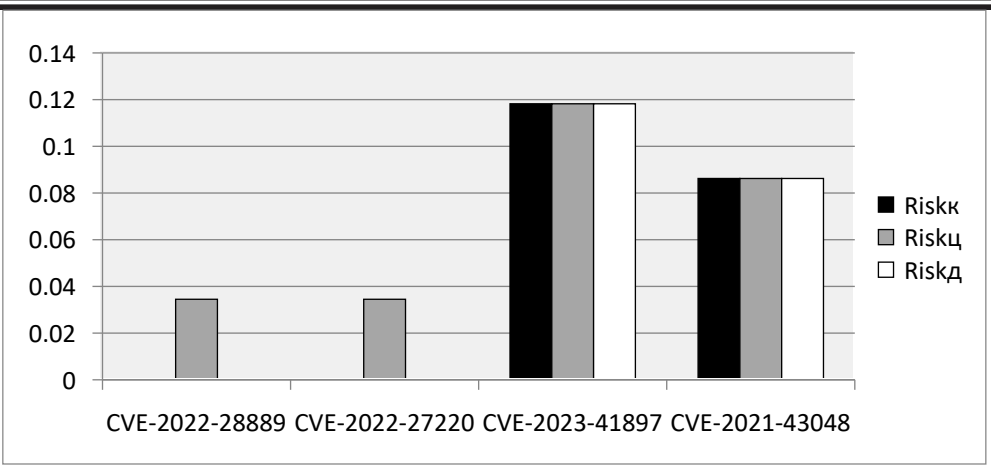

Рис. 6. Сечение риск-ландшафта для CAPEC 103

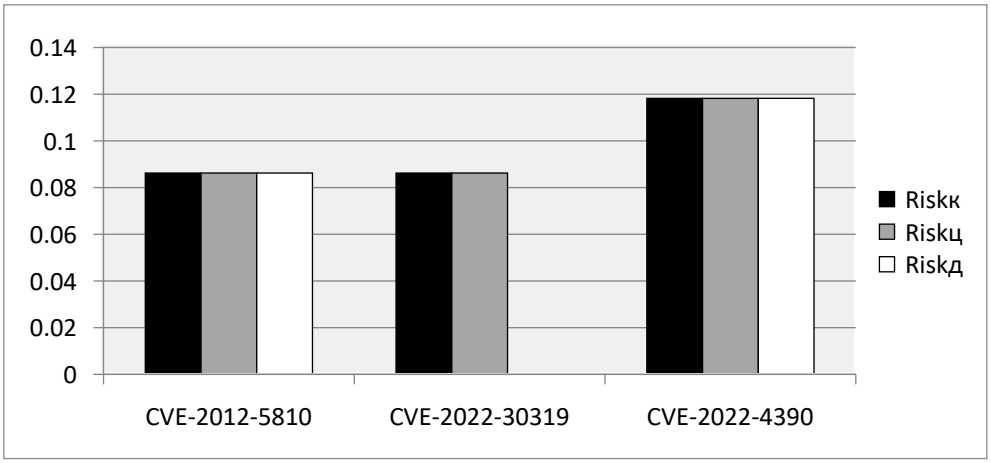

Рис 7. Сечение риск-ландшафта для CAPEC 501

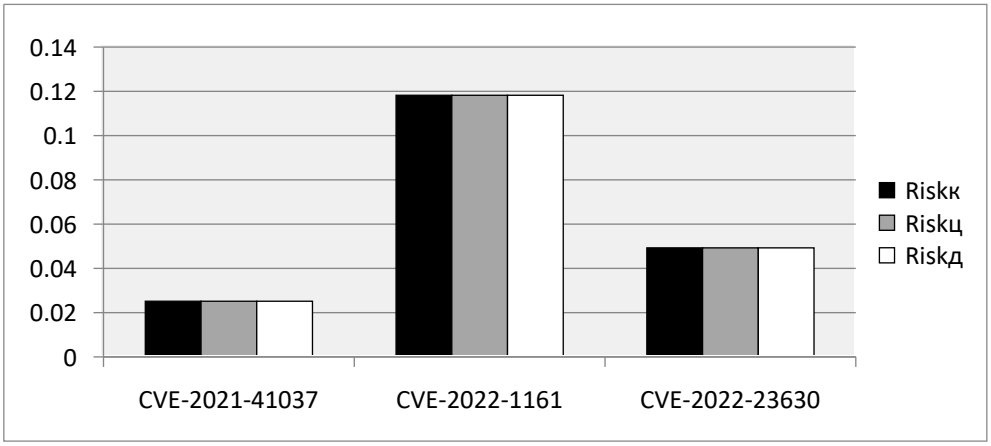

Рис. 8. Сечение риск-ландшафта для CAPEC 695

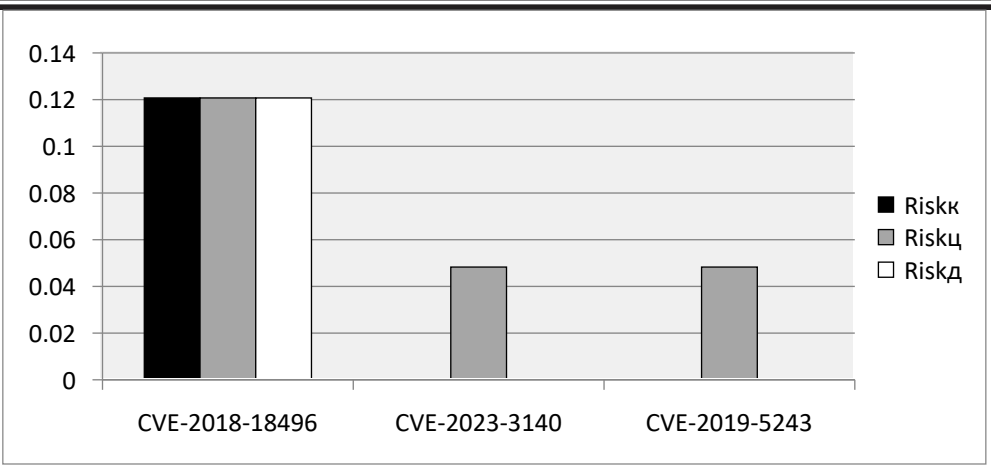

Рис. 9. Сечение риск-ландшафта для CAPEC 587

На основе рис. 1-9 и табл. 3 получены наиболее опасные сочетания уязвимостей и векторов атак класса «социальная инженерия» (табл. 4, 5).

Таблица 4

Наиболее опасные сочетания пар «вектор атаки – уязвимость»

Вектор атаки	Уязвимость	Тип ошибки
CAPEC-178	CVE-2022-31657 VMware Workspace ONE Access и Identity Manager содержат уязвимость для внедрения URL-адресов. Злоумышленник, имеющий доступ к сети, может перенаправить прошедшего проверку пользователя в произвольный домен. CVE-2023-23860 - SAP NetWeaver как для ABAP, так и для платформы ABAP позволяет злоумышленнику, не прошедшему проверку подлинности, создать ссылку, по которой ничего не подозревающий пользователь может перейти на вредоносный сайт, который может прочитать или изменить некоторую конфиденциальную информацию или подвергнуть жертву фишинговой атаке.	CWE-601 - Веб-приложение принимает управляемые пользователем входные данные, указывающие ссылку на внешний сайт, и использует эту ссылку при перенаправлении.
CAPEC-89	CVE-2023-3654 - cashIT! - решения для обслуживания. Устройства от "PoS / Dienstleistung, Entwicklung & Vertrieb GmbH" до 03.A06rks 2023.02.37 подвержены воздействию обхода источника через заголовок host в HTTP-запросе. Эта уязвимость может быть вызвана тем, что конечная точка HTTP подключена к сети.	CWE-346 - Продукт должным образом не проверяет достоверность источника данных или связи.
CAPEC-501	CVE-2022-4390 - Неправильная конфигурация сети в версиях маршрутизаторов серии NETGEAR RAX30 AX2400 до версии 1.0.9.90. IPv6 включен для интерфейса WAN по умолчанию на этих устройствах.	CWE-923 - Продукт устанавливает канал связи с конечной точкой (или от нее) для привилегированных или защищенных операций, но он должным образом не гарантирует, что он осуществляет связь с правильной конечной точкой.

Продолжение табл. 4

Вектор атаки	Уязвимость	Тип ошибки
CAPEC-185	CVE-2021-45027 - Уязвимость для загрузки произвольных файлов в сервере библиотеки Oliver v5 Версии <5.00.008.053 с помощью функции FileServlet позволяет злоумышленнику загружать произвольные файлы с использованием несанкционированных пользовательских данных.	CWE-494 - Продукт загружает исходный код или исполняемый файл из удаленного местоположения и выполняет код без достаточной проверки происхождения и целостности кода.
CAPEC-186	CVE-2023-40254 - Уязвимость при загрузке кода без проверки целостности в Genians Genian NAC V4.0, Genians Genian NAC V5.0, Genians Genian NAC Suite V5.0, Genians Genian ZTNA позволяет обновлять вредоносное программное обеспечение.	CWE-494 - Продукт загружает исходный код или исполняемый файл из удаленного местоположения и выполняет код без достаточной проверки происхождения и целостности кода.
CAPEC-103	CVE-2023-41897 - Сервер Home Assistant не устанавливает никаких заголовков безопасности HTTP, включая заголовок X-Frame-Options, который указывает, разрешено ли создавать рамки для веб-страницы. Отсутствие этого и соответствующих заголовков облегчает скрытые атаки с использованием кликджекинга и альтернативные возможности использования, такие как вектор, описанный в этом руководстве по безопасности	CWE-1021 - Веб-приложение не ограничивает или неправильно ограничивает объекты фрейма или слои пользовательского интерфейса, принадлежащие другому приложению или домену, что может привести пользователя к путанице в отношении того, с каким интерфейсом пользователь взаимодействует.
CAPEC-501	CVE-2022-4390 - Неправильная конфигурация сети в версиях маршрутизаторов серии NETGEAR RAX30 AX2400 до версии 1.0.9.90. IPv6 включен для интерфейса WAN по умолчанию на этих устройствах.	CWE-923 - Продукт устанавливает канал связи с конечной точкой (или от нее) для привилегированных или защищенных операций, но он должным образом не гарантирует, что он осуществляет связь с правильной конечной точкой.
CAPEC-695	CVE-2022-1161 - Злоумышленник, имеющий возможность изменять пользовательскую программу, может изменять программный код пользователя в некоторых системах управления ControlLogix, CompactLogix и GuardLogix.	CWE-829 - Продукт импортирует, требует или включает исполняемую функциональность (например, библиотеку) из источника, который находится за пределами предполагаемой сферы контроля.
CAPEC-587	CVE-2018-18496 - Когда страница предварительного просмотра RSS-канала about: feeds помещена в рамку другой страницы, ее можно использовать совместно со скриптовым содержимым для атаки с целью взлома кликов, которая заставляет пользователей загружать и запускать исполняемый файл из временного каталога.	CWE-1021 - Веб-приложение не ограничивает или неправильно ограничивает объекты фрейма или слои пользовательского интерфейса, принадлежащие другому приложению или домену, что может привести пользователя к путанице в отношении того, с каким интерфейсом пользователь взаимодействует.

Таблица 5

Риски для наиболее опасных пар

Идентификатор CAPEC	Идентификатор CVE	Risk U(к)	Risk U(ц)	Risk U(д)
CAPEC-178	CVE-2022-31657	0,118219	0,118219	0,118219
CAPEC-178	CVE-2023-23860	0,118219	0,118219	0
CAPEC-89	CVE-2023-3654	0,165507	0,165507	0,165507
CAPEC-501	CVE-2022-4390	0,118219	0,118219	0,118219
CAPEC-185	CVE-2021-45027	0,165507	0,165507	0,165507
CAPEC-186	CVE-2023-40254	0,165507	0,165507	0,165507
CAPEC-103	CVE-2023-41897	0,118219	0,118219	0,118219
CAPEC-501	CVE-2022-4390	0,118219	0,118219	0,118219
CAPEC-695	CVE-2022-1161	0,118219	0,118219	0,118219
CAPEC-587	CVE-2018-18496	0,120723	0,120723	0,120723

Из табл. 4, 5 можно сделать вывод, что наиболее опасные сочетания «вектор атаки – уязвимость» связаны с типами ошибки CWE-601, CWE-346, CWE-923, CWE-494, CWE-1021, CWE-923, CWE-829, что указывает на необходимость усиления мер защиты для снижения их рисков до приемлемого уровня.

Заключение

В результате работы удалось отобрать наиболее опасные пары «вектор атаки – уязвимость» на основе оценки рисков. Все это стало возможным при построении риск-ландшафта для векторов атак вида «социальная инженерия» в виде множества его сечений по каждому типу атак для использования различных уязвимостей.

Особенность рассматриваемого класса атак состоит, прежде всего, в том, что злоумышленник планирует навязать пользователю защищаемой системы действия, нарушающие ее безопасность. При всей прозаичности таких намерений, они довольно часто дают ожидаемый результат. Человеческий фактор при всей широте цифровой трансформации сегодняшнего бытия остается наиболее часто регистрируемой причиной сбоев, утечек и блокировок. Вот почему оценка и регулирование рисков представляется в данном слечае весьма эффективным инструментарием защиты. Особенно актуальна это задача для организаций, имеющих значительное количество пользователей, постоянное наблюдение за действиями которых весьма затруднительно. Здесь риск-ландшафт с учетом специфики защищаемой корпорации позволяет нацелить службу защиты информации на управление рисками в отношении наиболее опасных пар «вектор атаки - уязвимость» рассматриваемого класса кибератак, минимизируя при этом их успешность и ожидаемые ущербы нарушения целостности, доступности и конфиденциальности циркулирующих в организации сведений.

Новизна состоит в том, что впервые сформирован риск-ландшафт для кибератак класса «социальная инженерия» и выявлены наиболее опасные пары векторов данных кибератак и используемых ими уязвимостей.

Практическая ценность достигнутых результатов состоит в том, что построенный риск-ландшафт в силу его организации в виде совокупности вышеуказанных пар сечений, позволяет наглядно выявить наиболее опасные сочетания векторов и уязвимостей в отношении атак вида «социальная инженерия».

Теоретическая значимость результатов работы состоит в том, что использованные риск-метрики имеют перспективу своего теоретического развития в плане их адаптации к специфике защищаемых ТКС и анализа опасности векторов атак вида «социальная инженерия» на множество уязвимостей.

Здесь уместно будет рассмотреть несколько вполне практических случаев:

1. Когда реализуется единственный вектор атаки на группу уязвимостей, ему подверженных в защищаемой системе или сети. При этом атака носит одиночный характер и достаточно будет определить

отдельно вероятности успешной реализации для каждой пары «вектор-уязвимость» с подсчетом для нее соответствующего значения ущерба. Далее они очевидно будут суммироваться.

2. Когда единственный вектор атаки реализуется многократно с относительно постоянной интенсивностью. Пуассоновская модель наиболее удобна в данном случае и она даст вполне адекватные результаты.

3. Когда множество атак заданным вектором не носит поточный характер и нас интересуют лишь количества ее успехов во всех рассматриваемых уязвимостях. Ожидаемые значения поможет установить полиномиальное распределение.

4. Наконец, когда наблюдается «ливень» векторов атак на защищаемое множество уязвимостей, где закономерность успешных «попаданий» априори установить затруднительно. Здесь риск-анализ возможен через динамику накапливаемых ущербов с оценкой запаса устойчивости относительно удаленности от их критических значений по каждой уязвимости и по системе в целом.

Планируемая в дальнейшем программная реализация предлагаемых в настоящей работе методика позволит существенно повысить эффективность риск-анализа кибратак класса «социальная инженерия».

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. М: Горячая линия - Телеком, 2023. 228с.:

2. The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org/ (дата обращения 05.01.24).

3. NIST Information Technology Laboratory National Vulnerability Database. URL: https://nvd.nist.gov/vuln (дата обращения 05.01.24).

4. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения 05.01.24).

5. База данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения 05.01.24).

6. Каталог известных эксплуатируемых уязвимостей (CISA KEV). URL: https://www.cisa.gov/known-vulnerabilities-catalog (дата обращения 05.01.24).

7. Остапенко Г.А. Совершенствование организационно-правового обеспечения информационной безопасности предприятия: формирование риск-ландшафта сетевых атак / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Ю. Пекло // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 203-210.

8. С. Пекло А.Ю. Атаки типа «сетевая разведка»: риск-ландшафт и частная политика информационной безопасности предприятия / А.Ю. Пекло, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 235-246.

.

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 07.01.2024

Информация об авторах

Жидков Эдуард Иванович – студент, Воронежский государственный технический университет, e-mail: jidkov.eduard@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

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

Шварцкопф Евгения Андреевна – ассистент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

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

CYBERATTACKS OF THE TYPE “SOCIAL ENGINEERING”: THE RISK OF LANDSCAPE VECTORS OF ATTACKS AND VULNERABILITIES OF TELECOMMUNICATION NETWORKS

E.I. Zhidkov, A.P. Vasilchenko, A.A. Ostapenko
A.S. Koltsov, E.A. Schwarzkopf, A.S. Shchegolevatykh

It examines widespread attacks in cyberspace that focus on manipulating and exploiting people. The work established the correspondence of the CAPEC attack vectors and the CVE vulnerabilities used by them. For the resulting combinations of "attack vector – vulnerability", it is proposed to calculate the expected damages and the probabilities of their occurrence using CVSS calculation fields. In this way, it was possible to build a risk landscape of the considered variety of attacks in the form of a set of cross-sections of risk surfaces by vectors and vulnerabilities. The proposed approach provides an opportunity to identify the most dangerous sections that need to be regulated as a matter of priority in order to ensure the security of protected telecommunications networks.

Keywords: vulnerability, attack, security, risk, damage, probability, telecommunication networks, social engineering.

Submitted 07.01.2024

Information about the authors

Eduard I. Zhidkov – student, Voronezh State Technical University, e-mail: jidkov.eduard@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

Andrey S. Koltsov – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Evgeniya A. Schwarzkopf – assistant, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander S. Shchegolevatykh - Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com