DOI 10.36622/1682-7813.2025.28.2.014
УДК 004.056

РИСКИ РЕАЛИЗАЦИИ КИБЕРАТАК: МОДЕЛИРОВАНИЕ МНОЖЕСТВЕННЫХ ВТОРЖЕНИЙ

Г.А. Остапенко, А.А. Остапенко, Д.Н. Герасимова, К.С. Кудинов, Ю.М. Малежик

Работа посвящена исследованию множественных кибератак. Рассмотрены общие сценарии действий злоумышленников, последовательность процедур риск-анализа кибератак. Предложены модели единичной и многовекторной атаки, позволяющие оценивать риски их реализации. Предложена классификация кибератак по количеству вторжений, шаблонов и целей. Получены выражения для расчёта общего риска систем при одновременной реализации нескольких векторов атаки. Эти результаты могут использоваться для разработки эффективных стратегий защиты автоматизированных информационных систем и управления их рисками.

Ключевые слова: кибератака, уязвимость, риск, ущерб, вторжение, сценарий, вероятность.

Введение

Благодаря интенсивному развитию арсенала компьютерных атак и эксплуатирующих ими уязвимостей [1], за последнее десятилетие киберпространство фактически превратилось в поле битвы [2], где спецслужбы враждующих государств и криминальные структуры неустанно противоборствуют за достижение информационного превосходства. В целях отслеживания динамики этого процесса созданы и успешно функционируют интернет-ресурсы [3-10], без которых сегодня уже немыслима работа любого специалиста по защите информации.

Вместе с тем, по прежнему актуальной остаётся цель создания аналитических инструментов [1,2], позволяющих моделировать кибератаки и предсказывать их последствия. В этом отношении представляется перспективным использование и развитие аппарата оценки и регулирования рисков [1], внедрение которого особенно актуально в отношении множественных атак, отличающихся повышенной сложностью как в описании, так и в части противодействия им.

Именно поэтому авторы настоящей статьи обратились к этому множеству вредоносных воздействий, имея ввиду прежде всего их классификацию и методическое обеспечение оценки и регулирования рисков.

Особенности формализации описания кибератак

Представляется целесообразным предложить следующую классификацию кибератак (рис.1)

Рис. 1. Обобщенная классификация кибератак

Простейшим вариантом следует считать одиночные атаки, где реализуется одноразовая попытка вторжения в атакуемую систему с помощью единственного шаблона. Такие атаки зачастую используются на начальных этапах разведки. При множественных атаках такая попытка осуществляется избранным шаблоном несколько раз, что повышает шанс на успех, но также увеличивает вероятность обнаружения. Характерным примером в данном случае является многократная атака, когда последовательно реализуется серия попыток вторжения одним и тем же шаблоном.

Многовекторные атаки, в отличии от рассмотренных разновидностей, нацелены на множество объектов, атакуемых в любой последовательности или синхронно. Это делает их более сложными для отражения, поскольку специалистам приходится реагировать на угрозы одновременно по нескольким направлениям. Если злоумышленник при попытке вторжения использует различные шаблоны, то такую атаку можно назвать комбинированной, комбинирующей разнообразные средства для достижения большого ущерба. Подобные комбинированные удары дезориентируют силы защиты и являются особенно опасными.

Наиболее изощрёнными следует считать комплексные атаки, где применение средств вторжения может быть рассредоточено как в пространстве, так и во времени. Фактически это целая информационная операция, которая включает этапы разведки, внедрения, закрепления в системе и выполнения конечных целей. Зачастую такие атаки координируются группами злоумышленников могут длится месяцами, оставаясь незамеченными.

Представленная (рис.1) классификация с успехом может быть развита с учетом спецификации защищаемых систем и целей, преследуемых злоумышленниками. С переходом в детализации от шаблонов атаки к реализующим её тактикам классификация станет ещё более емкой и возможно даже многомерной. Однако это не отменяет необходимости моделирования всех необходимых для рассмотрения разновидностей вторжения, что принципиально необходимо для развития теории обеспечения кибербезопасности.

Проиллюстрированная (рис.1) классификация фактически рассматривает наивысший уровень формализации кибератак, который можно назвать общесценарным (рис.2). С него начинается процесс риск-анализа, характеризующего опасность рассматриваемых вторжений.

Чисто методически за ним следует уровень, на котором идентифицируются шаблоны атаки. Как правило это происходит с помощью ресурса CAPEC, и эти шаблоны задают каркас множественных кибератак (рис.1). CAPEC структурирует знания о методиках атак, что облегчает их анализ и прогнозирование [4].

Дальнейшая детализация осуществляется при помощи MITRE ATT&K, где для всякого шаблона атаки может быть предложена последовательность реализующих её техник [5].

Затем представляется возможным установить программные ошибки, которые могут использовать шаблоны и техники. Это осуществляется с помощью ресурса CWE [6].

В свою очередь эксплуатируемые уязвимости можно определить из заданных ресурсов CVE и БДУ [7,9].

Вычисление вероятностей возможно с помощью данных ресурсов CVSS и EPSS, а величины ущерба с помощью CVSS и CISA KEV [8-11].

Расчёт рисков компонентов и в целом атакуемой системы завершает процесс риск-анализа. На этом этапе определяются критические точки инфраструктуры, разрабатываются планы реагирования и меры для минимизации потенциального ущерба.

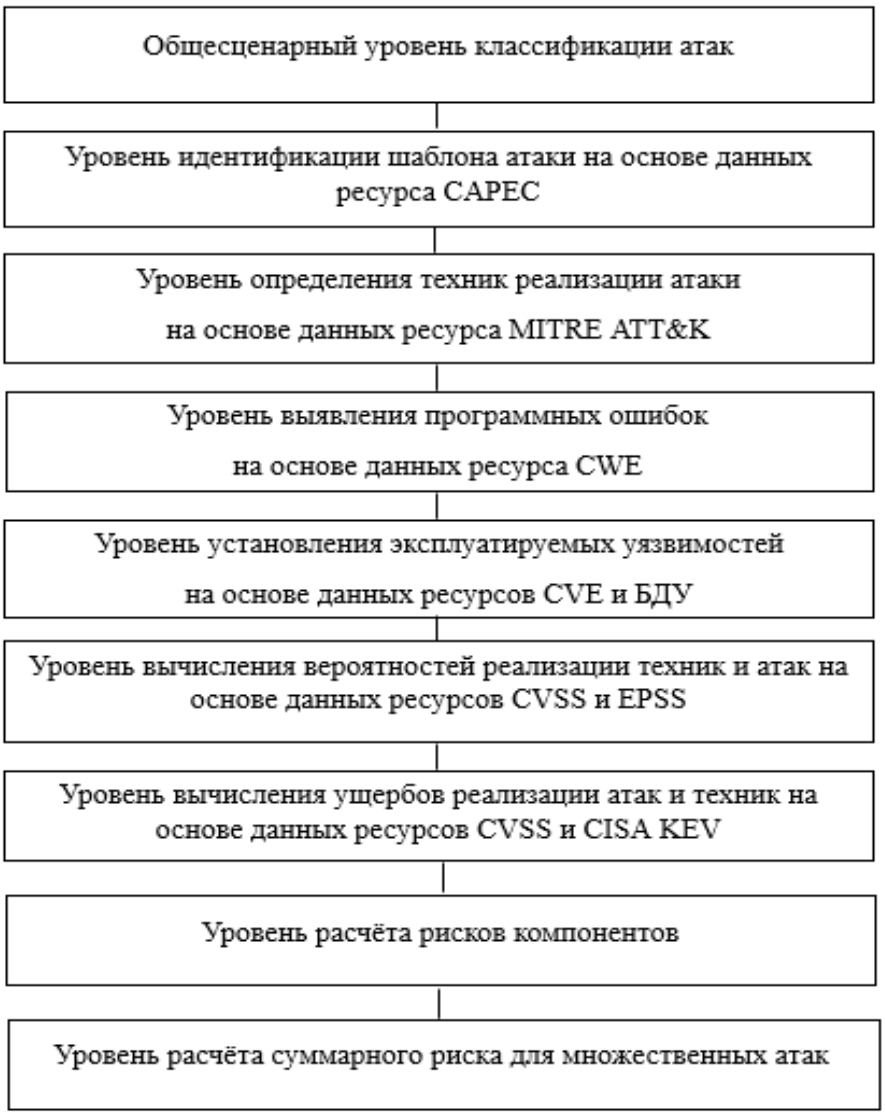


Рис. 2. Последовательность процедур риск-анализа кибератак

Методическое обеспечение процесса риск-моделирования многовекторных, единичных и многократных кибератак

Одной из важнейших составляющих методического обеспечения является разработка методик оценки рисков для различных типов атак, таких как единичные, многовекторные и многократные кибератаки атаки. Однако эпоха единичных атак постепенно подходит к концу, тем самым открывается новая эпоха массированных компьютерных вторжений, направленных на автоматизированные системы. Сегодняшняя угроза представлена огромным числом различных типов атак. Такая ситуация и создает сложную многомерную проблему для специалистов по защите информации, которым необходимо одновременно бороться с множеством угроз. Каждый тип атак имеет свои особенности, которые влияют на выбор методов и оценку последствий потенциальных угроз. Здесь задача осложняется тем, что отсутствуют эффективные инструменты и методы для полного анализа возникающих рисков и своевременного реагирования на массовые киберугрозы. Настоящая разработка нацелена на создание современной методологии, позволяющей моделировать многовекторные кибератаки, что позволит специалистам по защите информации вовремя регулировать риски реализации многовекторых кибератак.

Особенностью многовекторных атак являются тот факт, что они реализуются одновременно по нескольким объектом с использованием различных шаблонов атак (рис. 3).

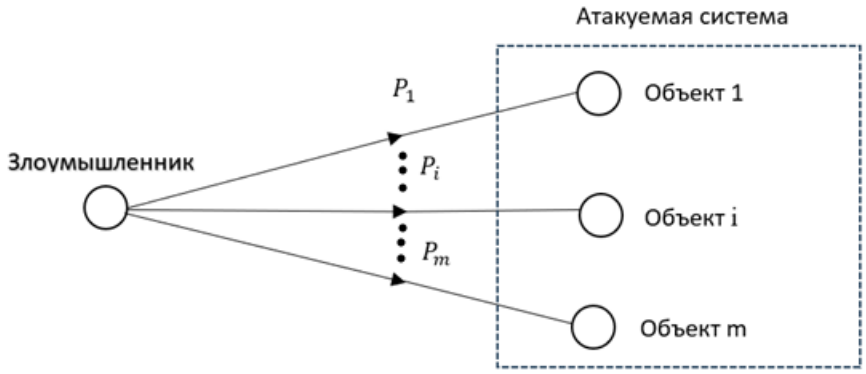


Рис. 3. Схема многовекторной атаки системы

Если предположить, что удалось вычислить вероятности успешной реализации каждого из использованных векторов $P_1 \dots \dots \dots P_m$, то вероятность удачной атаки хотя бы одним из них будет равна

$$P = 1 - \prod_{i=1}^{m}(1 - P_i)\,, \qquad (1)$$

В этой формуле (1) учтены все возможные сочетания успешности векторов (одиночные, попарные и даже одновременно всех векторов атаки).

Отсюда риск возникновения подобной ситуации представляется оценить следующим выражением:

$$Risk_{\Sigma} = \sum_{i=1}^{m} P_i U_i + \sum_{i=1}^{m} P_i P_j \left(U_i + U_j\right) + \dots + \prod_{i=1}^{m} P_i \sum_{i=1}^{m} u_i\,, \qquad (2)$$

где $\sum_{i=1}^{m} P_i U_i$ - риск успешности единичных атак с ущербами, i=1(1)*m,*

$\sum_{i=1}^{m} P_i P_j (U_i + U_j)$ – риск успешности всевозможных попарных сочетаний векторов с ущербами U_i и U_j, i, j = 1(1)m и $i \neq j$,

$\prod_{i=1}^{m} P_i \sum_{i=1}^{m} u_i$ – риск успешной реализации всех рассматриваемых векторов атаки.

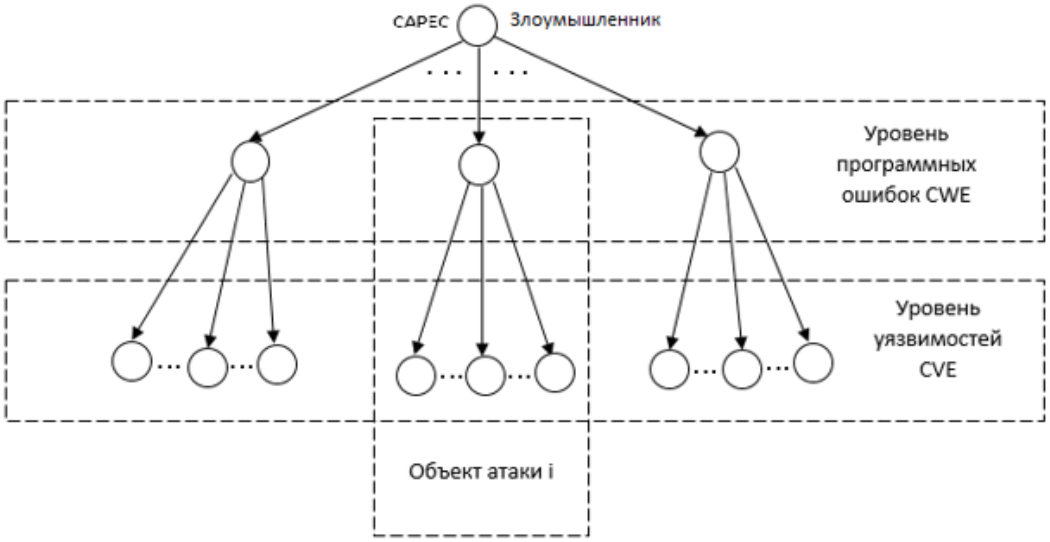
Разумеется, потребуется также оценка ожидаемых ущербов, наносимых каждому объекту атаки, $u_1, \dots, u_i \dots, u_j \dots, u_m$.

Следуя выражению (2), представляется возможным измерить риск для любого сочетания рассматриваемых векторов атак. В этом случае многовекторная атака становится комбинированной.

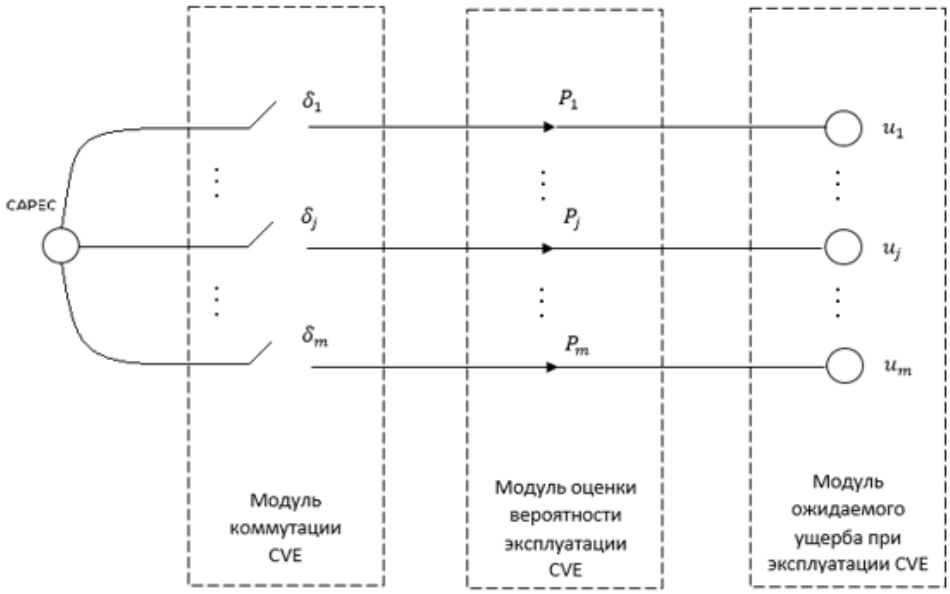
Разумеется, реализованные раньше алгоритмы и программы автоматизированного риск анализа [1] обретут второе дыхание в комплексе вышеописанного (1) и (2) моделирования кибератак (масштабно и относительно оригинально).

На следующем уровне детализации возникает необходимость в использовании моделей единичной атаки. Обобщенно они представлены на рисунке 3, где рисунок 3а иллюстрирует действия злоумышленника по выбору на объекте атаки множества программных ошибок CVE. В свою очередь, рисунок 3б отражает поиск злоумышленником тех уязвимостей, которые обладают необходимой критичностью в случае их эксплуатации избранным шаблоном атаки CAPEC. Модули процесса обеспечивают злоумышленнику отбор требуемой CAPEC уязвимости CVE (модуль коммутации), а также оценку P_j вероятности успешной её эксплуатации и получения ожидаемого ущерба u_j, исходя из возможностей ресурсов калькуляции CVSS и EPSS.

На следующем уровне детализации в модуль включаются техники (MITRE), которые реализуют соответствующие этапы вторжения уже для собственного набора уязвимостей.



а)



б)

Рис. 3. Сценарий действий злоумышленника

Предложенные модели значительно повышают эффективность анализа и проектирования систем, тем самым обеспечивая универсальность подхода к управлению рисками в условиях постоянно меняющегося ландшафта угроз.

Рассмотрим систему, подвергающуюся множественным атакам многовекторно, по её компонентам. Здесь обычно применяется биноминальное распределение вероятности [3]:

$$P(k,n,p) = C_n^k p^k (1-p)^{n-k}, \qquad (3)$$

где k – ожидаемое количество успешных атак в отношении рассматриваемого компонента защищаемой системы;

n – реализуемое количество атак заданным злоумышленником шаблоном;

p – вероятность успеха единичной атаки компонента заданным шаблоном.

Пример вычисления вероятностей, согласно выражению (3), имеется в [3] для случая n=10, n различных значений p. Считая k величиной ущерба, здесь можно оценить риск:

$$Risk(k,n,p) = kC_n^k p^k (1-p)^{n-k}, \qquad (4)$$

где k = 1(1)10.

Для установленных в примере значений p = 0,25;0,5;0,75, согласно выражению (4), были рассчитаны величины риска (рис. 4). Как видно из рис. 4, они значительно разнятся. Это говорит о том, что в рамках многокомпонентной системы (с различными вероятностями успеха единичной атаки её элементов) разброс значений рисков довольно значителен.

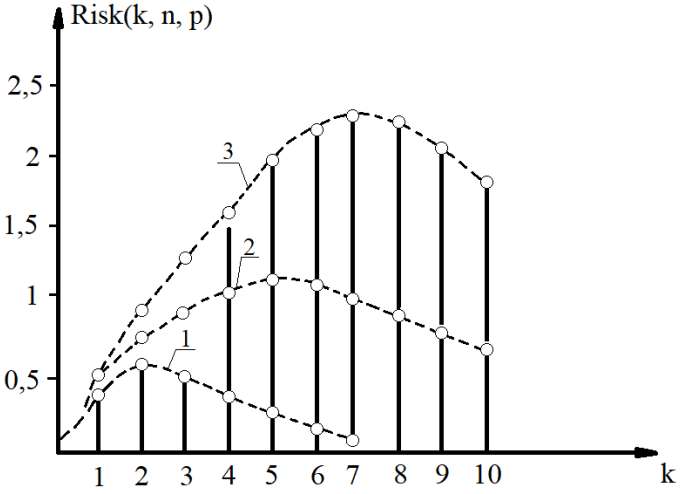


Рис. 4. Графики зависимости рисков компонентов атакуемой системы (огибающей риска первой 1, второй 2 и третьей 3 компоненты) от ущерба в виде количества успешных атак

Вместе с тем, возможно реализовать управление с целью уравнивания этих рисков хотя бы по их максимальным величинам. Дело в том, что считать параметр k ущербом возможно только в том случае, если ценности информационного ресурса всякого компонента защищаемой системы равновелики. Однако такая ситуация, не учитывающая p, создает перекос в системы обеспечения безопасности (рис. 4). Отсюда ущерб в действительности равен kC_i, где C_i - ценность защищаемого ресурса i-ой компоненты. Следуя этому свойству, представляется возможным перераспределить ценность ресурса системы с учетом максимумов риска компонентов, найденных без учёта этих ресурсов. К примеру, для рассматриваемого примера следует добиваться равенства:

$$max\{P_1 k_1 C_1\} = max\{P_2 k_2 C_2\} = max\{P_3 k_3 C_3\}\,, \qquad (5)$$

В результате графики огибающих риска примут вид, представленный на рисунке 5. Отсюда суммарный риск, равный:

$$Risk_{\sum} = Risk_1 + Risk_2 + Risk_3, \qquad (6)$$

дает соответствующий график огибающей (рис. 5). Он (с некоторой неравномерностью) имеет относительно неизменное значение, причем данная неравномерность, может быть, оптимизационно отрегулирована под нужный уровень вариаций параметров p_1, p_2 и p_3.

Приведенный пример для трех компонентов легко может быть обобщен для произвольного количества таковых, а суммарный риск в заданном диапазоне ущербов будет равномерен с необходимой неравномерностью.

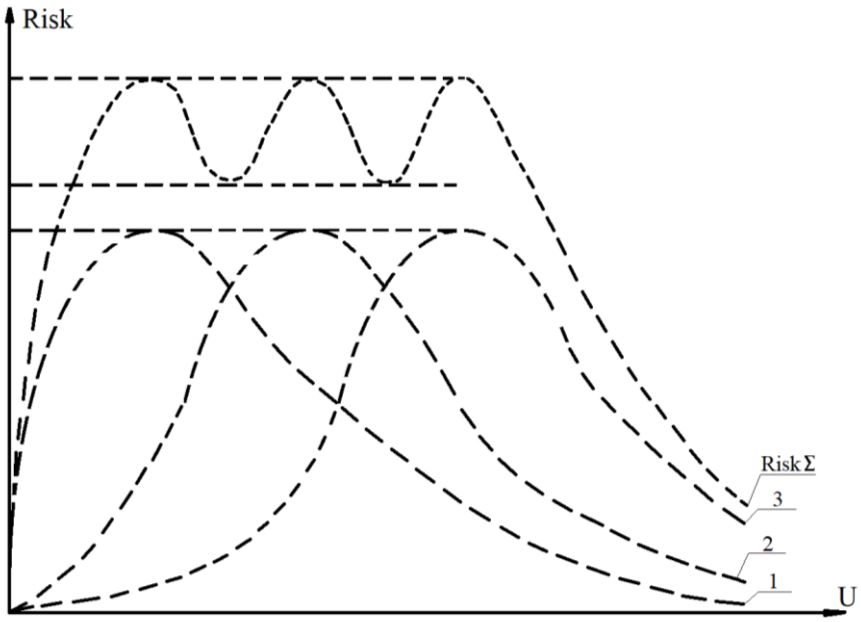


Рис.5. Формирование функции суммарного риска из огибающих трех компонент системы и ущерба с учетом ценности охраняемого ресурса компонента

Возможна также проектная ситуация, когда система имеющая m уязвимостей, подвергается потоком из n атак (рис.6), одного шаблона.

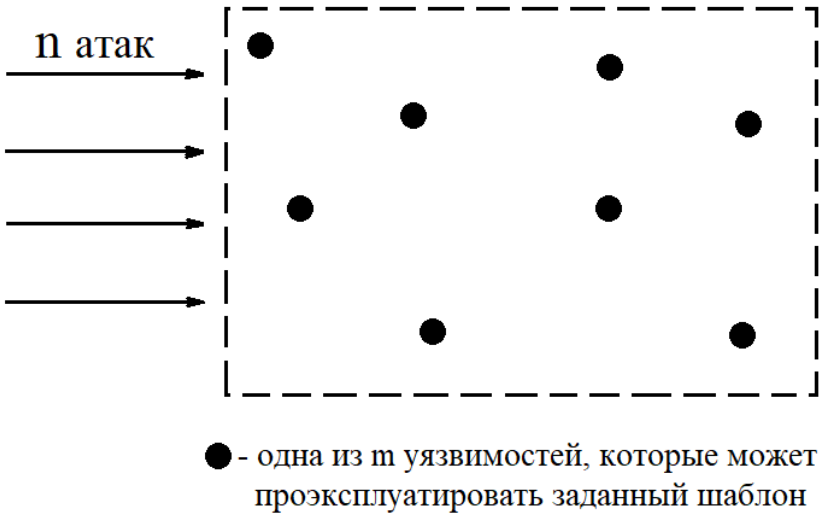


Рис. 6. Система из m уязвимостей, атакуемая потоком из n атак

В этом случае уместно применить мильтиномиальное распределение [3] вероятности:

$$P(x_1, \dots, x_m, n, p_1, \dots, p_m) = \frac{n!}{x_1! \ \dots \ x_m!} p_1^{x_1} \dots \ p_m^{x_m}, \quad (7)$$

где x_i= 0,1,2… и i = 1(1)m;

$\sum_{i=1}^{m} x_i = n$; p_i – вероятность успешной эксплуатации i-ой уязвимости;

$\sum_{i=1}^{m} p_i = 1$; np_i – матожидание количества успешных атак на i-ую уязвимость.

Для выражения (7) суммарный ущерб от рассматриваемой атаки составит:

$$U_{\Sigma} = \sum_{i=1}^{m} x_i u_i \,, \qquad (8)$$

где u_i - ущерб от единичной успешной атаки i-ой уязвимости.

С учетом вышеизложенного наиболее ожидаемый итог атаки имеет следующий риск (9):

$$Risk_{\Sigma}([np_1], \dots, [np_m], n, p_1, \dots, p_m) = \left(\sum_{i=1}^{m} x_i u_i\right) \times P([np_1], \dots, [np_m], n, p_1, \dots, p_m), \qquad (9)$$

где $[np_1]$ – целая часть при i=1(1) m.

Если предположить, что ущербы уязвимостей равновероятны, т.е. $u_i = u_0$ при i = 1(1)m, то выражение (9) примет вид:

$$Risk_{\Sigma} = nu_0 \times P([np_1], \dots, [np_m], n, p_1, \dots, p_m). \qquad (10)$$

Кроме того, вероятность в выражении (7) может быть существенно упрощена (избавлена от факториалов) с помощью приближения Стирлинга [3]:

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}\left(1 + \frac{1}{12n} + \cdots\right), \qquad (11)$$

что существенно сократит вычислительные затраты.

С точки зрения регулирования риска (9) представляется рациональным учесть ценность защищаемого ресурса C_i в каждом атакуемом компоненте системы i-ой уязвимостью:

$$u_i = \alpha_i C_i, \qquad (12)$$

где α_i – доля ценности, утрачиваемая при каждой успешной эксплуатации i-ой уязвимости.

Если нам удастся распределить общий ресурс атакуемых компонент обратно пропорционально произведению $[np_1]\alpha_i$, то суммарный риск будет минимизирован.

Возможны и иные оптимизации риска, учитывающие прочие особенности модели. Например, изменяемость α_i по мере роста x_i, т. е. частоты успеха единичных атак и т.п. Однако здесь, видимо, придется применять численную оптимизацию.

При этом надо понимать, что поток атак (рис.6) может также носить стохастический характер, который может быть расписан распределением Пуассона [3]:

$$P(n, \lambda) = \frac{\lambda t}{n!} e^{-\lambda t}, \qquad (13)$$

где n – ожидаемое за время наблюдения t количества атак;

λ - интенсивность атак, которую удалось оценить на предыдущих периодах наблюдения потока.

Из выражения (9) и (13) вероятность совмещенных событий (появления потока атак) и их реализации будет равна:

$$P_{\Sigma} = P(n, \lambda) \times P(x_1, \dots, x_m, n, p_1, \dots, p_m). \qquad (14)$$

Соответственно скорректируется и функция риска (10). Однако, следует понимать, что управление $P(n, \lambda)$ доступно лишь злоумышленнику через регулирование λ и для защитника атакуемой системы носит исключительно случайный характер. Поэтому лишь выражение $P(x_1, \dots, x_m, n, p_1, \dots, p_m)$ будет доступно ему для управления риском реализации атак.

Заключение

В работе представлена обобщенная классификация кибератак с акцентом на множественные вторжения, которая с успехом

может быть расширена путём детализации по реализуемым техникам и эксплуатируемым ими уязвимостям.

С учётом существующих данных сайтов атак и уязвимостей [4-10] предложена практически удобная последовательность процедур осуществления риск-анализа множественных вторжений.

Предложенные методические решения применены для исследования особенностей ряда множественных кибератак. Так, для многовекторного вторжения получены аналитические выражения для оценки вероятности успешной атаки и суммарного риска с учётом взаимодействия векторов р выравнивания рисков компонент через перераспределение ценности ресурсов.

Перспективой исследования множественных атак следует считать изучение комплексных кибервторжений. Сегодня криминальные группировки и спецслужбы враждующих государств всё чаще приобретают именно к этому инструменту информационной борьбы, где сценарные сюрпризы ожидают администраторов атакуемых систем и сетей по ходу реализации операции и за счёт гибридизации и варьирования набором средств атаки по ходу противоборства. Рваный тем вторжения, адаптируемого в зависимости от его промежуточных результатов, может демонстрировать как одиночные атаки, так и их «ливень». Искусство злоумышленника, а точнее группировки (время хакеров – одиночек давно прошло) будет проявляться именно в этом. Поэтому многотрудное моделирование комплексных атак все же необходимо осуществлять и результаты настоящей работы могут стать для него необходимым подспорьем, особенно с применением технологий искусственного интеллекта.

Список литературы

1. Автоматизированный атлас кибератак/ Г.А. Остапенко, А.П. Васильченко, А.О. Калашников и др.; под ред. Академика РАН Д.А. Новикова. М.: Горячая линия – Телеком, 2025. 188с.

2. Картография защищаемого киберпространства /А.Г Остапенко, А.Л. Сердечный, А.О. Калашников и др.; под ред. Академика РАН Д.А. Новикова. М: Горячая линия – Телеком, 2022. 372 с.

3. Математический аппарат инженера. Сигорский В.П. / М.: Техника, 1977. 768 с

4. CAPEC. URL: https://capec.mitre.org/ (дата обращения 05.05.2025).

5. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения 05.05.2025).

6. CWE. URL: https://cwe.mitre.org/index.html (дата обращения 05.05.2025).

7. CVE. – URL: https://cve.mitre.org/ (дата обращения 05.05.2025).

8. CISA KEV. URL: https://www.cisa.gov/known- exploited-vulnerabilities-catalog (дата обращения 05.05.2025).

9. Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru/threat (дата обращения 05.05.2025).

10. Exploit Prediction Scoring System (EPSS). – URL: https://www.first.org/epss/ (дата обращения 05.05.2025).

11. Общая система оценки уязвимостей (CVSS). URL: https://www.first.org/cvss/specificationdocument/ (дата обращения 05.05.2025).

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

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 17.05.2025

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

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

Герасимова Дарья Николаевна – студентка, Воронежский государственный технический университет, e-mail: dashka20.0615@gmail.com

Кудинов Кирилл Сергеевич – студент, Воронежский государственный технический университет, e-mail: kirillkudinov7777@gmail.com

Малежик Юлия Михайловна – студентка, Воронежский государственный технический университет, e-mail: juliamihailovna2003@mail.ru

RISKS OF IMPLEMENTING CYBER ATTACKS: SIMULATION OF MULTIPLE INTRUSIONS

G.A. Ostapenko, A.A. Ostapenko, D.N. Gerasimova, J.M. Malezik

The work is devoted to the study of multiple cyber attacks. The general scenarios of actions of intruders, the sequence of procedures of risk analysis of cyber attacks are considered. Single and multi-vector attack models are proposed to assess the risks of their implementation. A classification of cyber attacks by the number of intrusions, patterns, and targets is proposed. Expressions for calculating the total risk of systems with simultaneous implementation of several attack vectors are obtained. These results can be used to develop effective strategies for protecting automated information systems and managing their risks.

Keywords: cyber attack, vulnerability, risk, damage, intrusion, scenario, probability.

Submitted 17.05.2025

About the authors

Grigory A. Ostapenko – D.Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

Alexander A. Ostapenko – graduate Student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Daria N. Gerasimova– student, Voronezh State Technical University, e-mail: dashka20.0615@gmail.com

Kiril S. Kudinov– student, Voronezh State Technical University, e-mail: kirillkudinov7777@gmail.com

Julia M. Malezik – student, Voronezh State Technical University, e-mail: juliamihailovna2003@mail.ru