DOI 10.36622/1682-7813.2024.27.3.006
УДК 349:004.056

МЕТОДИКИ И АЛГОРИТМЫ РИСК-АНАЛИЗА УСПЕШНОСТИ РЕАЛИЗАЦИИ МАССИРОВАННЫХ КИБЕРАТАК

А.А. Остапенко

Обосновывается актуальность исследования массированных кибератак через оценку вероятности их успеха и возникающих в данном случае ущербов. Предполагается использование различных видов дискретных распределений вероятности, где успешность единичной атаки рекомендуется оценивать с использованием CVSS-калькуляторов, учитывающих как разновидность реализуемого вида атаки, так и особенности эксплуатируемой ей уязвимости. Оценку вероятности успеха множества атак заданного вектора на комплексе уязвимостей защищаемой системы предлагается осуществлять с помощью мультиномиального распределения, которое (в случае атак на единственную уязвимость) выражается в биномиальное распределение. Наиболее ожидаемые ситуации определяются через частоты успешной реализации сочетания вектор-уязвимость. В свою очередь ущерб может быть оценен через критичности эксплуатируемых уязвимостей. В итоге с помощью соответствующих полей CVSS-калькулятора возможно связать величину ущерба с его разновидностями (нарушения доступности, целостности, конфиденциальности). Ситуацию с «ливнем» разноплановых атак предлагается описывать с помощью временной оценки риска приближения суммы ущербов к уровню потери работоспособности защищаемой системы, где ущерб будет оцениваться произведением значения интервала простоя на стоимость единицы времени простоя атакуемого объекта. Вышеизложенное проиллюстрировано в виде блок-схем соответствующих алгоритмов риск-анализа. Для регулирования рисков предложено использовать функции чувствительности. Использование функций чувствительности открывает перспективу аналитического управления риском. В работе также присутствуют таблицы, наглядно демонстрирующие процессы: формирования пар «вид атаки – эксплуатируемая уязвимость; выбора экспертных оценок для определения вероятности и ущерба единичной атаки «атака-уязвимость», а также – формулировки задач, необходимые для адекватного целеполагания исследования.

Ключевые слова: кибератака, вероятность, ущерб, уязвимость, распределение, частота, критичность, простой, алгоритм, чувствительность.

Введение

Как вербальные, так и структурные модели процессов нарушения и обеспечения безопасности киберпространства во многом ориентированы на установление наличия и интенсивности связей между его компонентами [1]. Однако, аналитика, и, тем более, пользователя этого пространства, в первую очередь, интересует не взаимная обусловленность процессов и их авторов, которую описывают вышеупомянутые двумерные модели, а банальный вопрос о том, чем и насколько они рискуют на данном театре противоборствующих сил и тенденций. То есть, по большому счету, им хотелось бы иметь надежный прогноз динамических рисков ущербности их бизнеса. Именно в этом контексте ими рассматривается безопасность и перспективность своего функционирования во всепоглощающем киберпространстве. И даже киберстратегам развития крайне важны как текущие, так и ожидаемые значения риска. В отсутствии этого (третьего) измерения любая иная формализация будет рассматриваться авторами всего лишь как более удобная (в тех или иных проектных ситуациях) визуализация, к сожалению, почти полностью возлагающая численную аналитику происходящего на пользователя данного инструмента. Ему же объективно требуется гораздо более емкая и оцифрованная картина, подчеркнуть которую из созерцаемых текстов и графов довольно затруднительно.

При этом, гиперпроизводительность и ультраемкость современных вычислительных комплексов в сочетании с алгоритмами искусственного интеллекта ежедневно творят чудеса, предоставляя

необычные сервисные возможности киберпользователям. Все это, вероятно, можно и объективно нужно поставить на службу теории и практики информационной безопасности, методология обеспечения которой (в свете разрешения вышеупомянутых модельных противоречий) нуждается в модернизации.

Отсюда, введение в модели безопасности дополнительных метрик риска, имеющих перспективу цифрового их представления, видится абсолютно необходимым и вычислительно реализуемым, особенно с применением искусственных нейронных сетей.

Уходят времена, когда красочные картинки и философские размышления относительно безопасности казались весьма актуальными и увлекательными без какой-либо оцифровки возможностей наступления негативных последствий. Сейчас этот пробел объективно необходимо и вполне достижимо восполнить, благодаря корректной алгоритмизации обработки больших данных, в первую очередь, для оценки успешности реализации кибератак на защищаемую систему.

При этом, понятийный аппарат рассматриваемой проблематики выглядит следующим образом:

- безопасность – состояние защищенности системы от определенного множества угроз, риск реализации которых не превышает допустимых значений;

- риск – возможность наступления ущерба, который представляет собой совокупность негативных последствий реализации рассматриваемых угроз;

- мера риска – как правило, произведение величины ущерба на вероятность ее (величины) наступления;

- функция риска – решетчатая совокупность мер риска, выстроенная в зависимости от величины ущерба;

- кибератака – момент решительных, координированных и преднамеренных действий злоумышленника по нанесению ущерба атакуемой кибернетической системе;

- вид атаки – классифицированная разновидность атакующих действий злоумышленника, которую зачастую, отождествляют с терминами «шаблон» или «вектор»;

- класс атак – совокупность видов атак, имеющих общие свойства реализации, например, «инъекции», «социальная инженерия» и др.;

- множественные атаки – совокупность атакующих действий злоумышленника, неоднократно реализуемые в отношении защищаемой системы;

- уязвимость – слабое (в отношении некоторых видов атаки) место в программном обеспечении, оборудовании или протоколах безопасности защищаемой системы;

- единичная атака – действия злоумышленника, реализуемые с помощью одного вида атак в отношении единственной уязвимости защищаемой системы;

- массированные атаки – скоординированные множественные атаки различных видов на комплекс уязвимостей защищаемой системы;

- частота атаки – параметр, показывающий насколько часто в единицу времени используется тот или иной вид атаки при эксплуатации заданной уязвимости;

- критичность уязвимости – интегральный параметр, характеризующий степень сложности эксплуатации уязвимости.

Опираясь на сформулированные выше определения, рассмотрим процессы реализации множественных кибератак.

Практика реализации единичных кибератак [1] уходит в прошлое, и мы вступаем в эпоху массированных компьютерных вторжений в защищаемые автоматизированные информационные системы и сети. Уже сейчас даже эпизодические угрозы реализации сотен разновидностей атак, эксплуатирующих десятки тысяч уязвимостей [2-6], представляют собой мультиразмерную задачу вероятностного моделирования [7-8]. При этом, данная проблема усугубляется ещё и тем, что специалистам по защите информации все чаще приходится иметь дело с множественными атаками (в том числе, генерируемыми ботами) на комплексы уязвимостей в отсутствии инструментария, необходимого и

достаточного для адекватного анализа и парирования подобных вторжений. В порядке разрешения вышеуказанного противоречия вполне актуальна и уместна разработка методик и алгоритмов оценки и регулирования рисков реализации массированных кибератак, чему, собственно, и посвящено настоящее исследование, ориентированное на:

- объект автоматизированные информационные системы, подвергающиеся массированным кибератакам;

- предмет риск-анализ успешности реализации множественных компьютерных атак на комплексы эксплуатируемых уязвимостей объекта.

В данному случае очевидной целью выступает повышение киберзащищенности объекта в следующих направлениях:

- риск-анализ множественных атак представляется возможным осуществить через вероятность успеха единичных атак того или иного вида на определенную уязвимость, которую предстоит выявить с использованием открытой статистики кибератак [2-8];

- по известной вероятности успеха единичной атаки возможно смоделировать ситуацию, когда злоумышленник потоком атак заданного вида осуществляет попытку как можно большее количество раз проэксплуатировать соответствующую уязвимость защищаемой системы;

- не меньший практический интерес представляет случай, когда множеством атак заданного вектора злоумышленник стремится проэксплуатировать целую серию уязвимостей, и объективно необходимо осуществить многовероятностный риск-анализ такой ситуации, включая построения множества риск-гистограмм [1];

- в свою очередь, весьма необходимо рассмотреть вариант, условно названный «ливнем атак», когда без какой-либо хронологии атаки различными векторами по всему множеству выявленных уязвимостей (фактически система попадает в стресс-испытания с точки зрения обеспечения кибербезопасность, а задача риск-анализа серьезно осложняется и требует построения риск-ландшафта в трех измерениях вектор-уязвимость-риск, который очень необходим для наглядности регулирования защищенности системы);

- наконец, кроме оценки риска, требуется его регулирование, имея ввиду параметрическую настройку и структурную модификацию средств защиты информации, реализуемую в соответствии с результатами риск-анализа, проведенного в соответствии с предлагаемыми методиками.

Вытекающие из вышеизложенного задачи, представлены в табл. 1, где указаны их формулировки и условия для их решения, которым будет посвящено дальнейшее изложение результатов настоящего исследования.

Таблица 1

Задачи риск-анализа массированных кибератак

Номер задачи	Формулировка решаемых задач	Условия задачи
Единичная атака на единственную уязвимость системы		
1	Рассматривается ситуация, когда i-ый вид кибератаки пытается проэксплуатировать j- ую уязвимость. При этом, известны CVSS- параметры уязвимости и CAPEC (MITRE) - данные атаки. Необходимо вычислить вероятность p_{ij} и ущерб u_{ij} успешной реализации данного единичного вторжения.	В соответствии с классификациями CAPEC, MITRE и идентифицированы i-ый вид атаки и эксплуатируемая j-ая уязвимость.

Продолжение табл. 1

Номер задачи	Формулировка решаемых задач	Условия задачи
Множественные атаки одного вида на единственную уязвимость системы		
2	Рассматривается ситуация, когда n атак осуществляется i-ым вектором на j-ую уязвимость. При этом, известно значение вероятности успеха единичной атаки p_{ij}. Необходимо вычислить вероятность $P(k, n, p_{ij})$ и ущерб $U(k, n, p_{ij})$ того, что из вышеуказанных n атак k раз удастся проэксплуатировать данную уязвимость. Для злоумышленника представляет интерес частная задача, когда необходимо определить вероятность того, что потребуется k атак i-го вида прежде, чем наступит первая успешная эксплуатация j-ой уязвимости. Вторая подзадача сводится к вычислению вероятности $P(k, n, p_{ij})$ того, что злоумышленнику потребуется осуществить n атак i-го вида на j-ую уязвимость, чтобы k раз была проэксплуатирована заданная уязвимость.	$k < n$ $p_{ij} < 1$
Множественные атаки одного вида на комплекс уязвимостей системы		
3	Рассматривается ситуация, когда на m уязвимостей осуществляется n атак i-го вида. При этом, известны значения вероятностей успеха единичных атак p_{is} для всех рассматриваемых уязвимостей (полная группа) $s = 1(1)m$. Необходимо аналитически определить значения вероятностей $P(k_{is}, n, p_{is})$ и ущербов $U(k_{is}, n, p_{is})$ для k_{is} всевозможных $s = 1(1)m$ вариантов эксплуатации атакуемых уязвимостей при осуществлении заданного количества атак.	Для всех $s = 1(1)m$: $\sum_{s=1}^{m} p_{is} = 1$ $\sum_{s=1}^{m} k_{is} = n$ $m < n$
Множественные атаки различных видов на комплекс уязвимостей системы		
4	Рассматривается ситуация, когда на m уязвимостей осуществляются множественные атаки посредством r векторов. При этом известны вероятности и ущербы, определенные при решении предыдущей задачи. Необходимо аналитически определить риск-ландшафт подобного «ливня атак» и обобщенно оценить риск достижения защищаемой системы неработоспособности в условиях данного стресс-теста, осуществляемого злоумышленниками	Предполагается, что атаки различных видов независимы друг от друга.

Окончание табл. 1

Номер задачи	Формулировка решаемых задач	Условия задачи
Управление риском в условиях реализации массированных кибератак		
5	Рассматривается ситуация, когда под «ливнем атак» объективно необходимо рациональное управление рисками их успешности. При этом обеспечивается мониторинг ущербов, возникающих в защищаемой системе по мере осуществления кибер-противоборства, а также известны все параметры частных рисков, определённые в ходе решения предыдущих задач. Необходимо организовать алгоритмизацию процедур регулирования риска в параметрическом и структурном контекстах.	Предполагается, что имеется доступ Регулированию базовых параметров риска, а также к процессам устранения уязвимостей.

Риск-анализ единичных кибератак

Прежде всего необходимо установить взаимно однозначное соответствие между вектором атаки и эксплуатируемой им уязвимостью. Это представляется возможным с использованием [1-8] ресурсов CAPEC, CWE, CVE, CISA KEV и перечня уязвимостей, выявленных в защищаемой системе. Поэтапно, как это показано в табл. 2, сортируя данные вышеуказанных источников, можно получить искомое соответствие:

- первоначально нужно идентифицировать (избрать) рассматриваемый далее *i*-ый вид атаки, для чего используется ресурс CAPEC;
- на следующем этапе следует подобрать множество программных ошибок CWE, которые использует *i*-ый вид атаки;
- далее из CWE вытекает множество уязвимостей CVE, которые может проэксплуатировать *i*-ый вид атаки;
- в последствии уместно использовать ресурс CISA KEV, который позволит отобрать из формированного ранее множества уязвимостей наиболее актуальные из них;
- на заключительном этапе следует оставить в рассмотрении лишь те актуальные уязвимости, которые свойственны защищаемой системе.

Так обеспечивается соответствие *i*-го вида атаки и *j*-ой уязвимости (табл. 2).

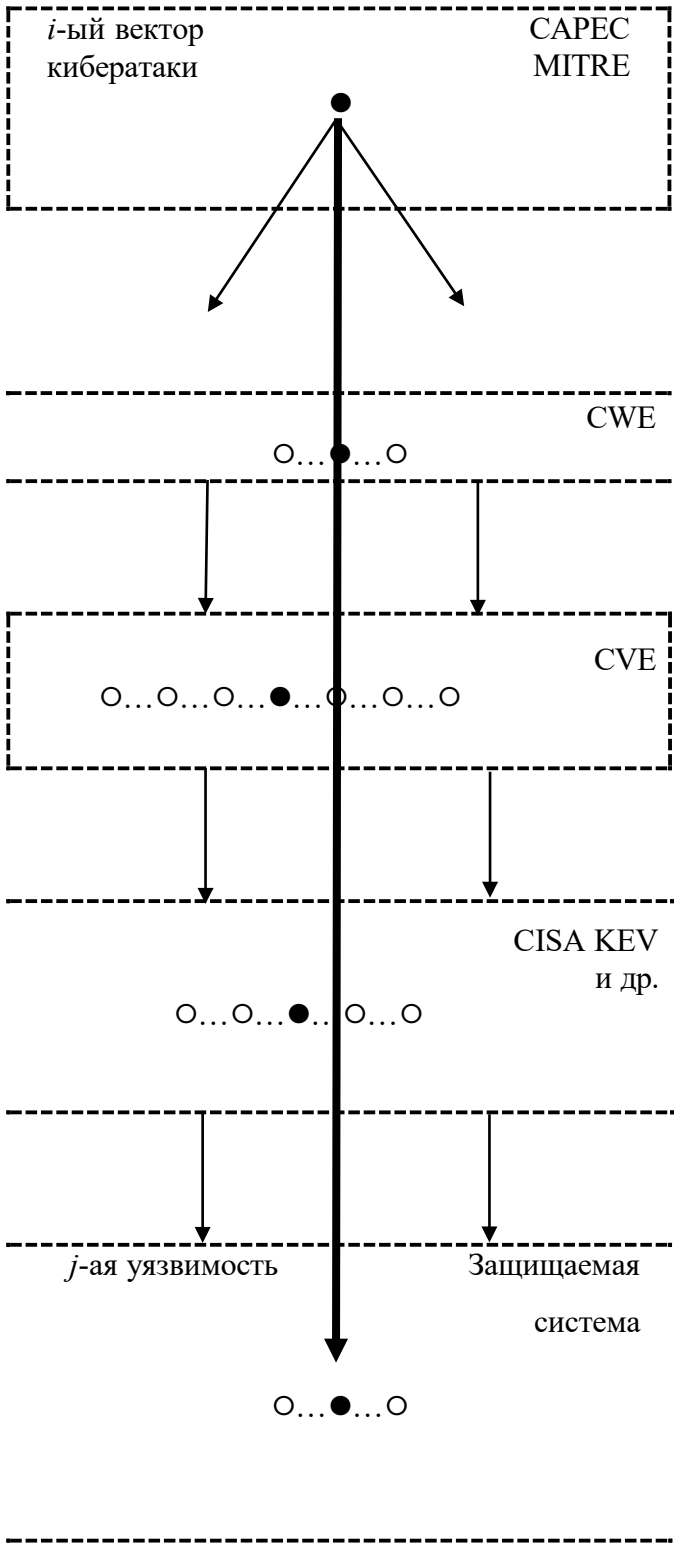
Схема, проиллюстрированная в табл. 2, не является абсолютной. Так, далеко не все уязвимости CVE опираются на программные ошибки CWE. Например, «бреши», связанные с аппаратным обеспечением, не требуют исполнения этапа 2. Использование ресурса CISA KEV также должно учитывать национальный характер представляемых данных, что в свою очередь может исключить этап 4 из предлагаемой схемы

Когда вышеуказанная пара установлена можно приступать к оценке вероятности ее реализации. В качестве варианта можно воспользоваться данными, сконцентрированными в полях CVSS-калькулятора, третья версия которого иллюстрируется в табл. 3. Задача состоит в том, чтобы выбрать количественную оценку параметра по его качественной характеристике. С использованием CAPEC и CVSS формируются значения следующих параметров:

1. *PA* – возможность осуществления заданного вида атак;
2. *AV* – уровень удаленности злоумышленника, реализующего вторжение в уязвимость;
3. *AC* – сложность эксплуатации соответствующей уязвимости;
4. *PR* – уровень привилегий необходимый для осуществления вторжения в уязвимость;

Таблица 2

Формирование пар «вид атаки – эксплуатируемая уязвимость»

Номер этапа	Графовая иллюстрация процедуры установления соответствия	Сущность осуществляемых этапов
1		*i*-ый вид атаки идентифицированный по CAPEC или MITRE-классификации
2		По классификации CWE определяются ошибки, которые могут быть проэксплуатированы идентифицированным видом атаки
3		С использованием CVE-ресурса определяются уязвимости, соответствующие избранным программным ошибкам
4		С помощью ресурса CISA KEV и др. осуществляется отбор наиболее актуальных (на текущий момент) уязвимостей
5		Выбираются уязвимости, характерные для защищаемой системы

5. UI – необходимость взаимодействия с пользователем в ходе вторжения в уязвимость;

6. КЦД – разновидность ожидаемого ущерба (нарушения конфиденциальности, целостности или доступности информации).

Таблица 3

Вариант оценки значений параметров для риск-анализа единичных атак «атака- уязвимость»

Обозначение параметров	Назначение параметров	Качественная оценка параметров	Количественная оценка параметров	Источник данных
Экспертные оценки параметров вида атаки				
PA	Оценивает возможность появления атаки заданного вида	очень низкая	0,1	CAPEC
		низкая	0,3	
		средняя	0,5	
		высокая	0,7	
		очень высокая	0,9	
Экспертные оценки параметров уязвимости				
AV	Задает уровень удаленности вторжения атакующего	Локальный	0,5	CVSS
		Соседняя сеть	0,7	
		Сетевой	0,9	
		Физический	0,3	
AC	Учитывает сложность эксплуатации уязвимости	Высокая	0,3	CVSS
PR	Определяет требуемый уровень привилегий	Высокий	0,3	CVSS
UI	Оценивает необходимость взаимодействия с пользователем	Требуется	0,3	CVSS
		Не требуется	0,8	
Экспертные оценки параметров ущерба				
КЦД	Оценивает возможности нарушения	Конфиденциальности	0; 0,2; 0,5	CVSS
		Целостности		
		Доступности		

Первый параметр непосредственно относится к виду атаки, а второй-пятый – к эксплуатируемой уязвимости. Шестой параметр связан с уязвимостью и видом ущерба, который она несет.

Следует заметить, что выше рассмотрен один из вариантов учета факторов, влияющих на вероятность и ущербность единичных атак. Отсюда вытекает подзадача конструирования соответствующего калькулятора, в том числе с использование недавно обнародованной четвертной версии CVSS.

Если параметры табл. 3 определены в своих значениях, представляется возможным приступить к расчету вероятности единичной атаки, которая выражается следующим образом:

$$p_{ij} = PA * AV * AC * PR * UI, \qquad (1)$$

Поправку в выражение (1) вносит коэффициент КЦД, задающий вид ожидаемого ущерба. В этом случае мы имеем три варианта результата (1), соответственно для нарушения конфиденциальности, целостности и доступности информации в результате

эксплуатации *j*-ой уязвимости посредством реализации *i*-го вида атаки. Следует заметить, что такую процедуру в отношении p_{ij} необходимо осуществлять для всякого последующего расчета множественных кибератак.

При этом, величина ущерба будет равна:

$$u_{ij} = \text{КЦД} * C, \quad (2)$$

где *C* – ценность защищаемого ресурса.

В свою очередь, из выражений (1) и (2) риск может быть определен следующим образом:

$$Risk_{ij} = p_{ij}\, u_{ij} = PA * AV * AC * PR * UI * \text{КЦД} * C, \quad (3)$$

откуда следует нормированный риск:

$$\overline{Risk_{ij}} = \frac{Risk_{ij}}{C} = PA * AV * AC * PR * UI * \text{КЦД}. \quad (4)$$

Выражение (4) позволяет в последующих выкладках риск-анализа абстрагироваться от экономики защищаемой системы и проводить сравнительный анализ между парами «атака-уязвимость».

Риск-анализ множественных кибератак заданного вида на единственную уязвимость защищаемой системы

Теперь, когда решена первая задача и с помощью методик предыдущего раздела удалось рассчитать вероятность единичной атаки *i*-го вида на *j*-ую уязвимость, представляется возможность приступить и к вероятностному моделированию множественных кибератак. В частности, согласно второй задаче, рассмотрим ситуацию, когда в отношении *j*-ой уязвимости реализуется *n* атак *i*-го вида. При этом необходимо определить вероятность и ущерб k успешных атак из *n*. В этом случае уместно использовать биномиальное распределение [9], откуда искомая вероятность будет равна:

$$P(k, n, p_{ij}) = C_n^k {p_{ij}}^k (1 - p_{ij})^{n-k}, \quad (5)$$

а ущерб составит:

$$U(k, n, p_{ij}) = k u_{ij}. \quad (6)$$

Наибольший риск просматривается в районе мат.ожидания np_{ij}, где из (5) и (6) получаем его нормированное (4) значение в следующем виде:

$$\overline{Risk_{ij}}(k, n, p_{ij}) = C_n^{k_m} {p_{ij}}^{k_m} (1 - p_{ij})^{n-k_m} * k_m * \text{КЦД}, \quad (7)$$

где $k_m = [np_{ij}]$ и $[*]$ – операция округления,

$C_n^{k_m} = \frac{n!}{k_m!(n-k_m)!}$ и надо искать оптимум риска в динамике параметра *n*.

Выражения (5)-(7) позволяют построить блок-схему алгоритма риск-анализа, представленную на рис. 1.

Похожий алгоритм имеет подзадача (поиска количества атак *n* до появления первого успеха), где количество сочетаний равно единице и мы имеем вероятность:

$$P(n, p_{ij}) = p_{ij}\,(1 - p_{ij})^n \quad (8)$$

и ущерб

$$U(n, p_{ij}) = u_{ij}. \quad (9)$$

Соответственно максимальный риск просматривается в районе мат.ожидания $(1 - p_{ij})/p_{ij}$. Здесь наглядно видно, что при $n \to \infty$ $p_{ij} \to 0$, т. е. для малой вероятности успеха единичной атаки придется значительно наращивать количество

осуществляемых атак.

Алгоритм второй подзадачи (поиск количества атак n для появления k их успехов) почти идентичен рис. 2, с разницей в вычислении количества сочетаний:

$$P(n,k,p_{ij}) = C_{n+k-1}^{k-1} {p_{ij}}^{k} (1-p_{ij})^{n},$$
$$U(n,k,p_{ij}) = k u_{ij}. \tag{10}$$

Максимум нормированного риска очевидно надо искать в районе мат. ожидания $k(1-p_{ij})/p_{ij}$, откуда видно, что для больших k и малых p_{ij} потребуется наращивать количество осуществляемых атак.

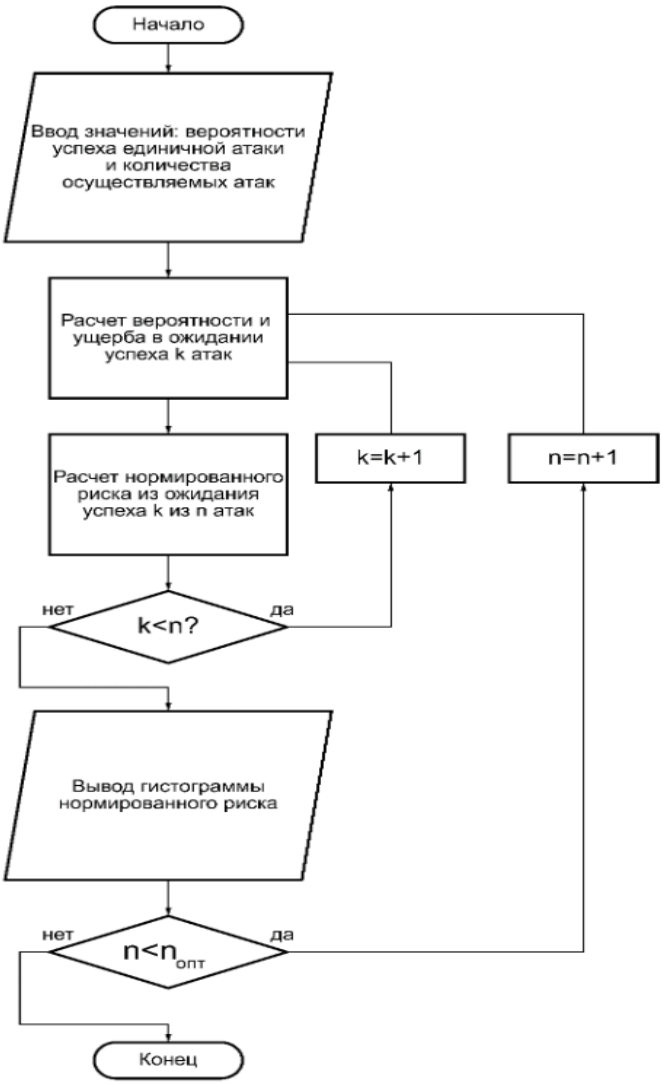


Рис. 1. Блок-схема алгоритма риск-анализа множественных атак заданного вида на единственную уязвимость

Крайний оператор (рис. 1) имеет непосредственное отношение к действиям злоумышленника, когда он стремится к достижению оптимального значения количества атак, которое представляется возможным определить решением относительно n следующего уравнения:

$$\frac{\partial \overline{Risk}}{\partial n} = 0. \tag{11}$$

Несмотря на то, что самостоятельная подзадача, специалисту по защите информации объективно необходимо

представлять значение $n_{\text{опт}}$, за пределами которого повышать уровень риска злоумышленнику не удастся. Однако решение уравнения (11) довольно затруднительно и здесь видимо придется прибегать к приближенным способам вычисления факториалов [10], либо использовать рекуррентные соотношения нахождения числа комбинаторных сочетаний [9].

В результате получается иметь границы риска для различных видов ущерба, нарушающих конфиденциальность, целостность и доступность информации множественными атаками *i*-го вида на *j*-ую уязвимость в зависимости от количества осуществляемых атак.

Риск-анализ множественных кибератак заданного вида на комплекс уязвимостей защищаемой системы

Пожалуй, наибольший практический интерес представляет случай противоборства, когда множественные атаки осуществляются на комплекс уязвимостей, имеющихся в защищаемой системе. Для моделирования такой ситуации уместно применить мультиномиальное распределение [9], где *i*-ый вид атаки пытается проэксплуатировать *m* уязвимостей, т. е.

$$j = 1(1)m$$

и тогда возможно аналитически выразить вероятность успеха злоумышленника

$$P(k_{is}, k, p_{is}) = n! \prod_{s=1}^{m} \frac{{p_{is}}^{k_{is}}}{(k_{is})!}, \qquad (12)$$

и ожидаемого ущерба

$$U(k_{is}, k, p_{is}) = \sum_{s=1}^{m} k_{is} u_{is}, \qquad (13)$$

где: p_{is} – нормированная вероятность успеха единичной атаки *i*-го вида на *s*-ю уязвимость;

k_{is} – количество успешных атак *i*-го вида на *s*-ю уязвимость;

$\sum_{s=1}^{m} \overline{p_{ıs}} = 1$, $\overline{p_{ıs}} = \frac{p_{is}}{\sum_{s=1}^{m} p_{is}}$ (полная группа событий [9]);

$$\sum_{s=1}^{m} k_{is} = n.$$

Представленные выражения (12) и (13) свидетельствуют о том, что задача носит многовариантный характер, затрудняющий всеобъемлющий риск-анализ. Здесь уместно прибегнуть к использованию математических ожиданий $n\overline{p_{ıs}}$ [9], откуда можно задать математически ожидаемое количество успешных атак на *s*-ю уязвимость:

$$k_{is} = [n\overline{p_{ıs}}] \text{ для всех } s = 1(1)m, \qquad (14)$$

где: [*] – операция округления;

$\sum_{s=1}^{m} np_{is} = n$ (полная группа событий.

В свою очередь для оценки ущерба возможно воспользоваться [2-4] данными критичности уязвимостей k_{is}, $s = 1(1)m$. Здесь для соблюдения условия полной группы событий уместно осуществить следующее нормирование:

$$\frac{k_{is}}{\sum_{s=1}^{m} k_{is}} = \overline{k_j}, \qquad (15)$$

где $\sum_{s=1}^{m} \frac{k_{is}}{\sum_{s=1}^{m} k_{is}} = 1$;

k_{ij} – критичность *j*-ой уязвимости при реализации *i*-го вида атаки

Из выражения (15) единичный ущерб при эксплуатации *s*-ой уязвимости будет равен:

$$u_{is} = \text{КЦД} * \overline{k_s} C. \qquad (16)$$

Выражения (12)-(16) позволяют оценить риск (нормированный по ценности защищаемого ресурса) в следующем виде:

$$\overline{Rısk} = n! \prod_{s=1}^{m} \frac{{p_{is}}^{k_{ms}}}{(k_{ms})!} * \sum_{s=1}^{m} \overline{k_s} * \text{КЦД}, \qquad (17)$$

где удельный ущерб u_{is} при эксплуатации каждой из m отдельно взятой уязвимости составит:

$$u_{is} = k_s * \text{КЦД}, s = 1(1)m. \qquad (18)$$

Отсюда представляется возможным построить гистограммы (для вариантов

КЦД) риска по каждому ущербу (18) с вероятностью (12)

$$\overline{Risk}(s) = P * (k_{ms}, n, \overline{p_{is}}) * \overline{u_{ij}}. \quad (19)$$

В выражении (19) наличествует параметр *n*, при вариации значений которого может быть получено семейство гистограмм.

В целях автоматизации этого процесса на рис. 2 предложен алгоритм риск-анализа, где в качестве входных данных (рис. 3) используется гистограмма успешности единичных атак, а выходными данными выступает (рис. 2) гистограмма нормированного риска.

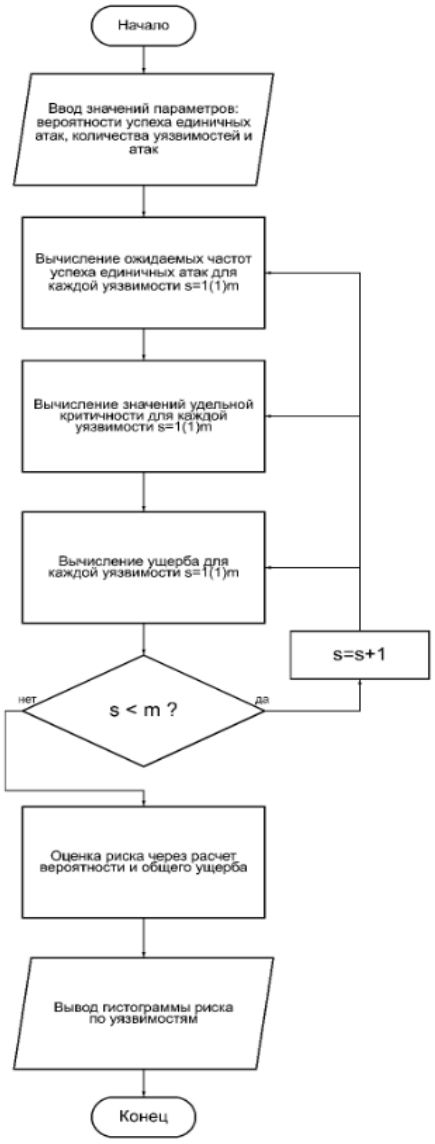


Рис. 2. Блок-схема алгоритма риск-анализа множественных кибератак заданного вида на комплекс уязвимостей защищаемой системы

Разумеется, с учетом коэффициента КЦД (17) пример (рис. 3 и 4) утроится в контексте основных видов нарушения безопасности (конфиденциальности, целостности и доступности) информации.

Кроме того, следует заметить, что вариант определения количества успешных атак через матожидание (14) не является единственно возможным. В этой связи представляется также целесообразной попытка вычисления этого параметра через частоты F_{ij} атак [1-4] в следующем выражении:

$$k_{is} = [\mathrm{n}\overline{F_{is}}], s = 1(1)m], \quad (20)$$

где: [*] – операция округления;

$\overline{F_{ij}} = \frac{F_{ij}}{\sum_{s=1}^{m} F_{is}}$.

Выражение (20) следует рассматривать как еще одну частную задачу риск-анализа (19), решение которой, ввиду ее многопараметричности, уместно искать по пути численной оптимизации.

Множественные атаки различного вида на комплекс уязвимостей защищаемой системы

Конечно, стресс-тестом для защищаемой системы следует считать «ливень атак», когда в краткосрочной перспективе осуществляется массированное вторжение с помощью различных видов атак на комплекс выявленных уязвимостей. В определенной степени все рассмотренные выше разновидности атак можно считать частным случаем «ливневого вторжения», поэтому его рассмотрение представляется вполне актуальным.

Если исходить из того, что по разновидностям атаки реализуется независимо друг от друга, то аналитически ситуацию можно описать совокупностью уравнений, подобных (19):

$$\overline{Risk}(i, s) = P * (k_{ms}, n, \overline{p_{is}}) * \overline{u_{is}}, \quad (21)$$

где $s = 1(1)m$ – множество m атакуемых уязвимостей;

$i = 1(1)r$ – множество r атакующих векторов.

Отсюда, согласно рис. 4, можно получить

набор гистограмм риска, который естественно образует ландшафт (рис. 5), ибо на плоскости осей уязвимостей и видов атак «произрастают» столбики нормированного риска (21). Наглядное представление множества рисков, идентифицированных с парами «атака-уязвимость», открывает перспективу организации эффективного кибер-противоборства.

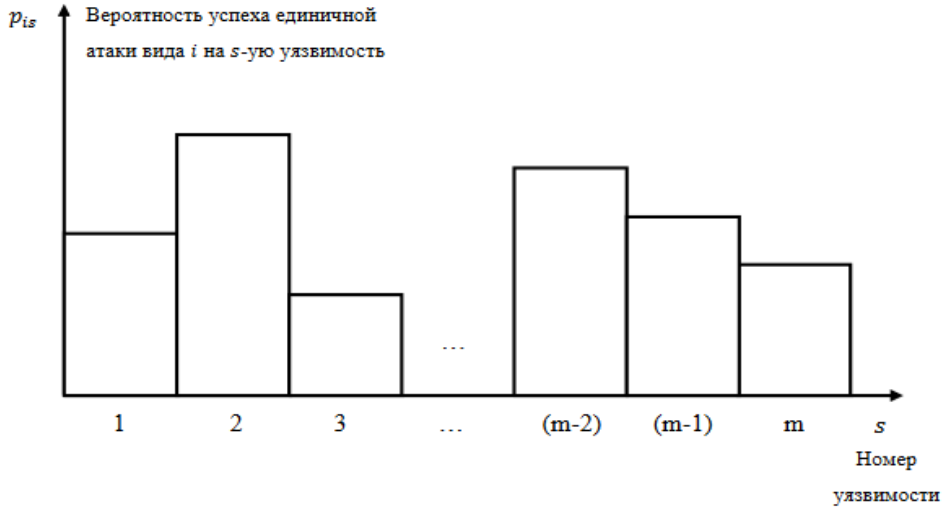


Рис. 3. Входные данные алгоритма (рис. 2) в качестве гистограммы вероятности единичной атаки вида i на m уязвимостей защищаемой системы

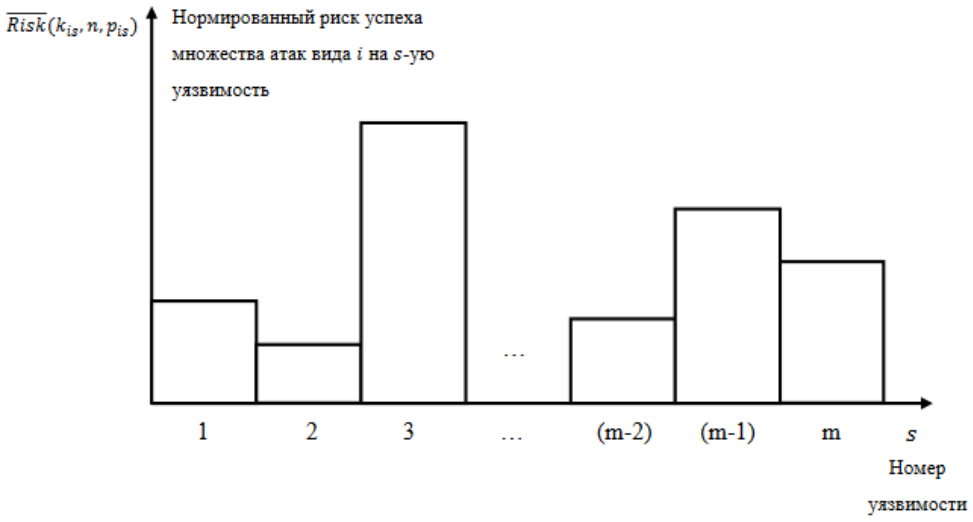


Рис. 4. Выходные данные алгоритма (рис. 2) в качестве гистограммы рисков успешности атак вида i на m уязвимостей защищаемой системы

Формирование риск-ландшафта (рис. 5) определяется двумя множествами: уязвимостей и видов атаки. Первое множество (табл. 2) задается условиями актуальности избранных уязвимостей [8] и их назначением в защищаемой системе, которое, в свою очередь, определяют используемые ею программные обеспечение и архитектура (ответ на этот вопрос, как правило, дает соответствующее тестирование).

Второе множество формируется в соответствии с возможностями осуществления атаки на первое (табл. 2). Именно в этом контексте появляются уравнения (21), которые фактически формируют сечения риск-ландшафта по параллелям оси уязвимостей (рис. 5). Анализ этих сечений по пику риска позволяет выявить уязвимости, наиболее подверженные данному вектору атаки. Второе сечение, по параллелям оси векторов

атаки дает информацию об уязвимостях, наиболее подверженных целой серии видов атаки.

Вариации с количеством осуществляемых атак n демонстрируют динамику стресс-теста защищаемой системы и могут указать пороги полной утраты её работоспособности. В таком моделировании риск-ландшафт весьма полезен для определения кибер-устойчивости исследуемого объекта.

В том случае, когда представляется возможным оперировать экспериментальными данными текущего ущерба, наносимого в ходе множественных атак, администраторам защищаемой системы уместно воспользоваться методикой, проиллюстрированной на рис. 6.

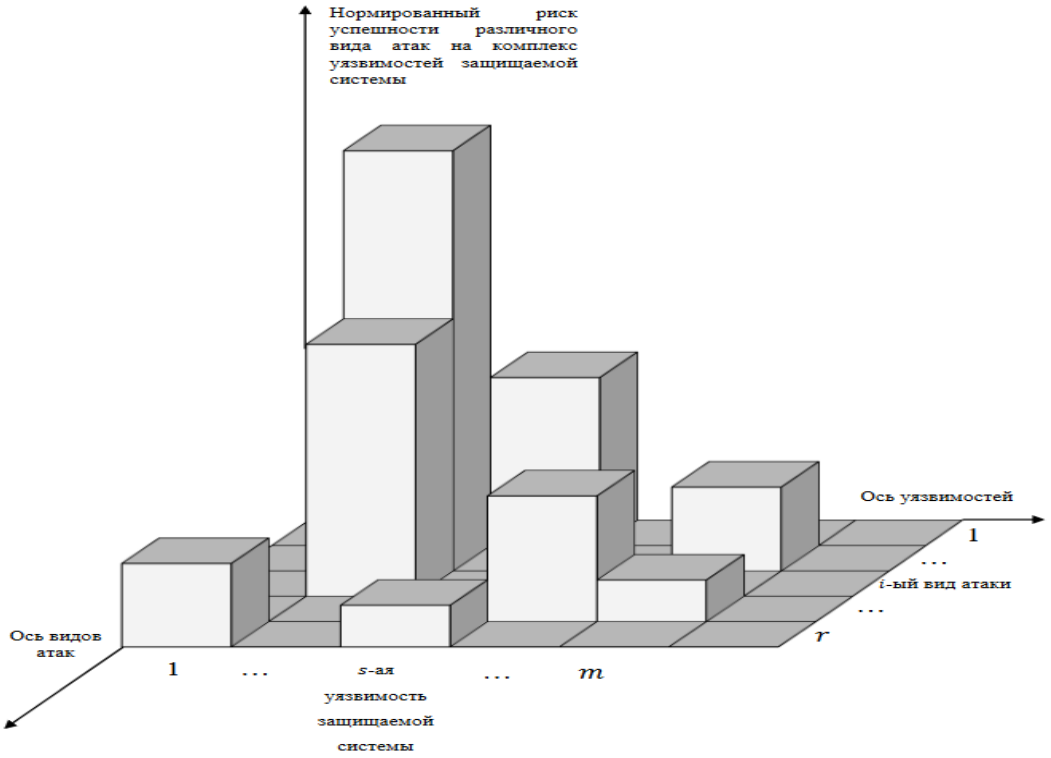


Рис. 5. Пример, иллюстрирующий выходные данные анализа в качестве риск- ландшафта «ливня атак» (21)

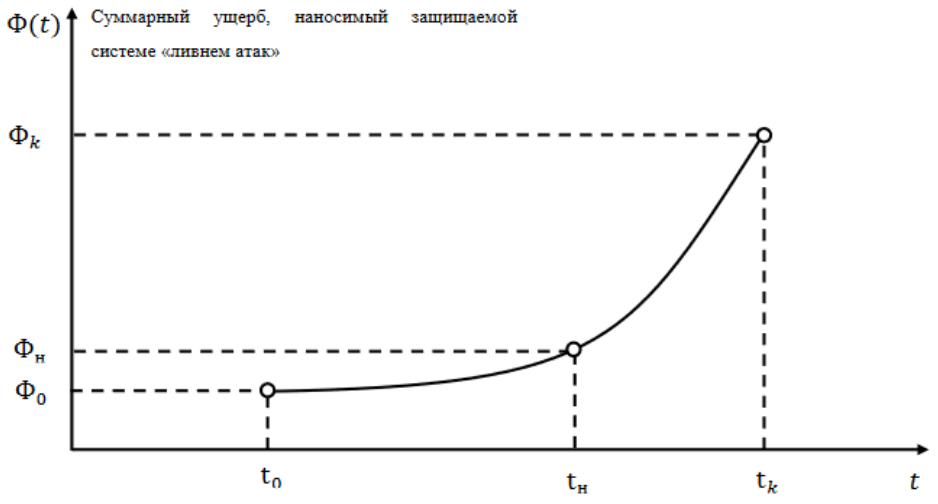


Рис. 6. График зависимости от текущего времени суммарного ущерба, наносимого защищаемой системе «ливнем атак»

На рис. 6 обозначено:

t – текущее время;

t_0 –момент времени, в который было зарегистрировано вторжение в защищаемую систему «ливня атак»;

$t_н$ – момент времени, в который осуществляется оценка риска успеха «ливня атак»;

t_k –момент времени, в котором защищаемая система утрачивает работоспособность под «ливнем атак»;

$Ф_0$ – значение суммарного ущерба при обнаружении вторжения «ливня атак»;

$Ф_н$ – значение суммарного ущерба в момент оценки риска успеха «ливня атак»;

$Ф_k$ – критическое значение суммарного ущерба, при котором защищаемая система теряет работоспособность.

Здесь (рис. 6) данные ущерба, отслеживаемые от момента регистрации массированного вторжения t_0 по настоящее время $t_Н$, позволяет спрогнозировать (в т. ч. автоматизировано) момент полной утраты работоспособности t_k атакуемой системы, для которой задан порог $Ф_k$ ее устойчивости. В этом случае риск возникновения такой ситуации можно приближенно оценить следующим выражением:

$$Risk(Ф_k) \cong P(t_k) * U(Ф_k), \qquad (22)$$

где $P(t_k)$ – вероятность достижения критического уровня ущерба $Ф_k$;

$U(Ф_k)$ – ущерб защищаемой системы, последующий при достижении $Ф_k$.

Раскрывая выражение (22), получаем приближенно:

$$Risk(Ф_k) \cong \frac{(t_н - t_0)}{(t_k - t_0)} * (\Delta t_п * C_0), \qquad (23)$$

где $\Delta t_п$ – время простоя потерявшей свою работоспособность защищаемой системы;

C_0 – стоимость единицы времени простоя для защищаемой системы.

Из выражения (23) определяется нормированный по C_0 риск:

$$\overline{Risk}(Ф_k) \cong \frac{(t_н - t_0)}{(t_k - t_0)} * (\Delta t_п), \qquad (24)$$

При наличии необходимых исходных данных [2-4] просто (по отдельным видам атак и уязвимостям) подобной методикой с успехом можно воспользоваться в инженерных расчетах риск-анализа.

Управление рисками множественных кибератак

Такая задача всегда стоит перед специалистами по защите информации и неизменно является особенно затруднительной для них [1] из-за ее многофакторности и мультиразмерности. Поэтому дойти до необходимой конкретики в ее аналитическом решении, как правило, не удается. Достаточно обратиться к набору уравнений (21), который обычно насчитывает десятки параметров и тысячи их вариаций. Даже при современных вычислительных возможностях формализация и оптимизация такой модели весьма затруднительны. Отсюда обычно приходится прибегать к вышеописанным процедурам, когда сечения риск-ландшафта указывают на элементы защищаемой системы, в которых, в первую очередь, необходимо осуществлять параметрические (чаще всего, изменяя p_{is}) или структурные (скажем, закрытие уязвимостей) регулировки. Конкретная алгоритмизация подобных действий, учитывающая специфику защищаемой системы, представляет собой отдельную и довольно затруднительную подзадачу.

В тех случаях, когда осуществляется мониторинг ущербов, наносимых защищаемой системе множественными атаками, и известны пределы ее устойчивости, представляется возможным обратиться к методике, проиллюстрированной на рисунке 6, адаптировав ее под задачи управления риском. На первый взгляд, данный полуэмпирический подход сулит достаточно простое решение по критерию (24). Однако алгоритм регулировки Ф(t) явно не очевиден, ибо требует управления частными ущербами риск-ландшафта в количестве m * r. Этот вопрос остается пока открытым и является предметом еще одной подзадачи настоящего исследования.

В обобщенном виде алгоритм

управления риск-ландшафтами защищаемой системы представлен на рис. 7. Он фактически состоит из двух циклов:

– коррекция вероятности успеха единичной атаки для наиболее опасных сочетаний вектор-уязвимость, что можно сделать по табл. 3, изменяя, скажем, удаленность AV или уровень привилегий PR;

– структурно-функциональная модернизация системы, скажем, путем снижения критичности наиболее опасных уязвимостей.

Повторы этих циклов на уровне параметрическом и структурном способны привести локальные показатели риск-ландшафта в допустимые границы, адекватное задание которых также является дополнительной подзадачей настоящего исследования.

В целях организации управления риском упростим выражение мультиноминального распределения вероятности [9] с помощью формулы Стерлинга [10]:

$$n! \approx (\frac{n}{e})^n\sqrt{2\pi n}, \qquad (25)$$

Учитывая, что из сотен вариантов сочетаний успешности атак на имеющиеся уязвимости нас интересуют, прежде всего наиболее ожидаемые

$$k_{is} = \mathrm{n}\overline{p_{ıs}},$$

где $\overline{p_{ıs}} = p_{is} / \sum_{s=1}^{m} p_{is}$.

Для всех s = 1(1)m, можно записать второй факториал в выражении (12) следующим образом:

$$k_{is}! \approx (\frac{k_{is}}{e})^{k_{is}}\sqrt{2\pi k_{is}} = (\frac{n\overline{p_{ıs}}}{e})^{k_{is}}\sqrt{2\pi n\overline{p_{ıs}}} = (\frac{n}{e})^{k_{is}}\overline{p_{ıs}}^{kis}\sqrt{2\pi n\overline{p_{ıs}}}$$
$$= (\frac{n}{e})^{k_{is}}\overline{p_{ıs}}^{kis}\sqrt{2\pi n}\sqrt{\overline{p_{ıs}}}. \qquad (26)$$

Подставляя (25) и (26) в выражение (12), получаем:

$$P = (\frac{n}{e})^n\sqrt{2\pi n}\prod_{s=1}^{m}\frac{\overline{p_{ıs}}}{(\frac{n}{e})^{k_{is}}\overline{p_{ıs}}^{kis}\sqrt{2\pi n}\sqrt{\overline{p_{ıs}}}} =$$
$$= \frac{(\frac{n}{e})^n\sqrt{2\pi n}}{\prod_{s=1}^{m}(\frac{n}{e})^{k_{is}}\sqrt{2\pi n}\sqrt{\overline{p_{is}}}} = \frac{(\frac{n}{e})^n\sqrt{2\pi n}}{(\frac{n}{e})^{\sum_{i=1}^{m}k_{is}} * m\sqrt{2\pi n}\prod_{s=1}^{m}\sqrt{\overline{p_{is}}}}, \qquad (27)$$

Памятуя, что, $\sum_{i=1}^{m} k_{is} = n$ упрощаем выражение (27):

$$P = \frac{(\sqrt{2\pi n})^{1-m}}{\prod_{s=1}^{m}\sqrt{\overline{p_{ıs}}}}, \qquad (28)$$

В свою очередь для ущерба (13) имеем:

$$U = \sum_{s=1}^{m}(n\overline{p_{ıs}})u_{is}, \qquad (29)$$

Далее рассмотрим регулирование риска и обратимся к функциям чувствительности, зарекомендовавших себя в решении многих практических задач управления [11, 12]. Имея в виду множество регулируемых параметров m, n и p_{iq} для всех q = 1(1)m, в первом приближении относительное отклонение риска можно описать [12] следующим выражением:

$$\frac{\Delta\overline{Rısk}}{\overline{Rısk}} \approx \frac{\partial(\ln\overline{Rısk})}{\partial(\ln n)}\left(\frac{\Delta n}{n}\right) + \frac{\partial(\ln\overline{Rısk})}{\partial(\ln m)}\left(\frac{\Delta m}{m}\right) + \sum_{s=1}^{m}\frac{\partial(\ln\overline{Rısk})}{\partial(\ln p_{is})}\left(\frac{\Delta p_{is}}{p_{is}}\right), \qquad (30)$$

Исходя из равенства $\ln\overline{Rısk} = \ln P + \ln U$, согласно выражениям (28) и (29) имеем:

$$\ln\overline{Rısk} = (1-m)(\ln\sqrt{2\pi} + \frac{1}{2}\ln n) - \frac{1}{2}\sum_{s=1}^{m}\ln\overline{p_{ıs}} + \ln n + \ln\sum_{s=1}^{m}\overline{p_{ıs}}u_{is}, \qquad (31)$$

Отсюда (31) могут быть найдены функции относительной чувствительности риска:

$$S^{\ln \overline{Risk}}_{\ln m} = m\frac{\partial\,(\ln \overline{Risk})}{\partial m} = -m\,(\ln\sqrt{2\pi} + \frac{1}{2}\ln n); \quad (32)$$

$$S^{\ln \overline{Risk}}_{\ln n} = n\frac{\partial\,(\ln \overline{Risk})}{\partial n} = (1-m)\,\frac{1}{2}\frac{1}{n}n + n\frac{1}{n} = \frac{3-m}{2}; \quad (33)$$

$$S^{\ln \overline{Risk}}_{\ln \overline{p_{is}}} = \overline{p_{is}}\frac{\partial\,(\ln \overline{Risk})}{\partial \overline{p_{is}}} = -\frac{\overline{p_{is}}}{2}\frac{1}{\overline{p_{is}}} + \overline{p_{is}}\frac{1}{\overline{p_{is}}u_{is}}u_{is} = \frac{1}{2}; \quad (34)$$

Следует заметить, что регулировка риска изменением $\overline{p_{is}}$ возможна только в рамках *s*-ой уязвимости, ибо сумма этих нормированных вероятностей по определению равна единице. Поэтому для (34) необходимо найти частные производные по первичным p_{iq} вероятностям единичного успеха *i*-го вида на *q*-ю уязвимость:

$$\frac{\partial \overline{p_{is}}}{\partial p_{qs}} = \frac{\sum_{s=1}^{m} p_{is} - p_{iq}}{(\sum_{s=1}^{m} p_{is})^2} = \frac{\sum_{s=1, s\neq q}^{m} p_{is}}{(\sum_{s=1}^{m} p_{is})^2} = \frac{1-\overline{p_{iq}}}{\sum_{s=1}^{m} p_{is}}, \quad (35)$$

Отсюда с учетом выражений (34) и (35) имеем:

$$S^{\ln \overline{Risk}}_{\ln p_{iq}} = \frac{p_{iq}}{2}\frac{\sum_{s=1, s\neq q}^{m} p_{is}}{(\sum_{s=1}^{m} p_{is})^2}, \quad (36)$$

При этом выражение (36) требует своей конкретизации с учетом факторов, определяющих успех единичной атаки. В таблице 3 приведен пример вычисления этой вероятности по совокупности факторов с помощью калькулятора CVSS 3 в виде произведения их экспертных значений (1). То есть потребуется еще одна частная производная:

$$\frac{\partial \ln p_{iq}}{\partial \varphi} = \frac{\partial}{\partial \varphi}(\ln \varphi + \sum \varphi_s), \quad (37)$$

где: φ_i – значение фактора вида атаки;

φ_s – значения факторов уязвимости.

Однако это отдельная подзадача, которая в отношении ущербов требует использовать также калькулятор CVSS 4.

Попытаемся привести пример численного расчета. Согласно выражению (28), при равновеликих частых вероятностях ($\overline{p_{is}} = 1/m$, s = 1(1)m) имеем:

$$P = \frac{(\sqrt{m})^{m-1}}{(\sqrt{2\pi})^{m-1}(\sqrt{n})^{m-1}} = (\frac{m}{n})^{\frac{m-1}{2}}\frac{1}{(2\pi)^{\frac{m-1}{2}}}, \quad (38)$$

где, задавая m = 5 и n = 10, для примера численно получаем:

$$P = (\frac{1}{2})^2\frac{1}{(6{,}28)^2} = \frac{1}{4}\frac{1}{39{,}44} = \frac{1}{157{,}75} = 0{,}0064. \quad (39)$$

В свою очередь, полагая равновеликими ущербы по всем уязвимостям ($u_{is} = u_0,\ s = 1(1)m$), для общего ущерба имеем:

$$U = \sum_{s=1}^{5} = n(\frac{1}{m})u_0 = m * n\frac{1}{m}u_0 = nu_0, \quad (40)$$

тогда получаем выражение риска:

$$Risk = u_0\frac{(m)^{\frac{m-1}{2}}}{(n)^{\frac{m-3}{2}}(2\pi)^{\frac{m-1}{2}}}, \quad (41)$$

а нормированный риск будет равен:

$$\overline{Risk} = \frac{Risk}{u_0} = \frac{(m)^{\frac{m-1}{2}}}{(n)^{\frac{m-3}{2}}(2\pi)^{\frac{m-1}{2}}} = \frac{25}{10*39{,}44} = 0{,}0644. \quad (42)$$

Точность описания движения риска при вариации управляющих параметров может быть повышена с использованием функций чувствительности высших порядков [12], что является предметом отдельной подзадачи настоящего исследования.

Точность модели можно также повысить, училив приближение к факториалам [11]:

$$n! = (\frac{n}{e})^n\sqrt{2\pi n}(1 + \frac{1}{12n}), \quad (43)$$

Тогда поправка составит:

$$\delta = \frac{(1+\frac{1}{12n})}{\prod_{s=1}^{m}(1+\frac{1}{12n\overline{p_{is}}})}, \quad (44)$$

Уместен также пересчет под первичные (еще не нормированные) вероятности p_{is}. В этом случае имеем риск, равный:

$$Risk = \left(\frac{\sum_{s=1}^{m} p_{is}}{2\pi n}\right)^{\frac{m-1}{2}} * \frac{n\sum_{s=1}^{m}(p_{is}u_{is})}{\prod_{s=1}^{m}\sqrt{(p_{is}}} * \delta, \quad (45)$$

Соответственно логарифм риска составит:

$$\ln Risk = \frac{m-1}{2}\left[ln\left(\sum_{s=1}^{m} p_{is}\right) - \ln n - \ln(2\pi)\right] + \ln n - \ln\sum_{s=1}^{m}(p_{is}u_{is}) - \frac{1}{2}\sum_{s=1}^{m} ln(p_{is}) + \ln\delta, \quad (46)$$

для которого функции чувствительности, без учета δ, будут равны:

$$S_{\ln n}^{\ln Risk} = \frac{3-m}{2}; \quad (47)$$

$$S_{\ln m}^{\ln Risk} = \frac{m}{2}[\ln(\sum_{s=1}^{m} p_{is}) - \ln n - \ln(2\pi)]; \quad (48)$$

$$S_{\ln p_{is}}^{\ln Risk} = \frac{(m-1)}{2}\frac{p_{is}}{\sum_{s=1}^{m} p_{is}} + \frac{p_{is}u_{is}}{\sum_{s=1}^{m}(p_{is}u_{is})} - \frac{1}{2}; \quad (49)$$

Предложенные выражения (46)-(49) уместно использовать при уточненной алгоритмизации процесса управления риском (рис.7).

Управление рисками успешности кибератак представляется возможным за счет:

– отсечения части атак, например, с помощью «песочниц» (средство проверки ПО на потенциальную вероятность в изолированной среде, защищающее от целевых и массированных атак на внутренний периметр компании), интегрированных с межсетевыми экранами и др. средствами защиты информации;

– регулирования влияния факторов (вектор и сложность атаки, уровень привилегий, взаимодействие с пользователями, доступность средств эксплуатации, доступность средств устранения и др.) определяющих величины вероятности и ущерба единичной атаки на уязвимость;

– устранения ряда уязвимостей защищаемой системы.

Все это должно учитываться с использованием функций чувствительности (47)-(49) в ходе управляемого движения риска к области его допустимых значений.

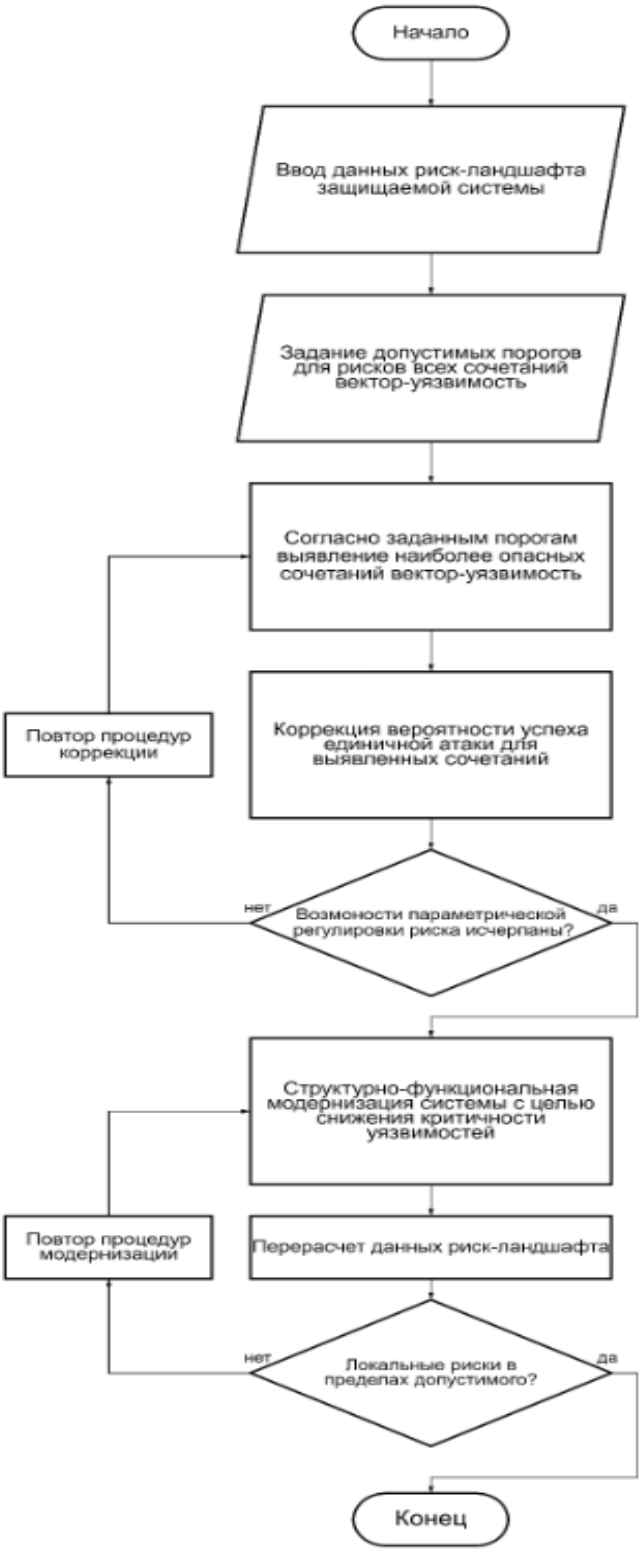


Рис. 7. Блок-схема обобщенного алгоритма управления риск-ландшафтом

Заключение

Резюмируя вышеизложенное, необходимо обозначить пути практической реализации полученных результатов и актуальных направлений их развития:

1. В рамках студенческого и аспирантского исследовательских интересов представляет реальный интерес применение предложенных методик для обеспечения безопасности самых разнообразных компьютерных, автоматизированных и телекоммуникационных систем и сетей, подвергающихся массированным вторжениям посредством реализации

многочисленных кибератак, включая оценку и регулирование рисков нарушения конфиденциальности, целостности и доступности информации с использованием открытых баз знаний и данных, а также рекомендуемого методического обеспечения. Спектр таких объектов довольно широк (от интернета вещей до средств критической информационной инфраструктуры и др.), как и многообразие классов компьютерных атак (инъекция, социальная инженерия и др.), реализуемых в отношении перечисленных объектов.

2. Предложенная аналитика открыта для своего совершенствования и обозначенные подзадачи требуют своего решения в плане развития методологии обеспечения информационной безопасности, базирующейся на объективной необходимости риск-анализа процессов деструктивных кибервоздействий, включая моделирование таковых не только в терминах «вид атаки – эксплуатируемая уязвимость», но и при более глубоком проникновении в сущность происходящего по линии «субъектов-сценариев-объектов атак», требующей повышенной детализации рассмотрения структурно-функциональных отношений всех фигурантов противоборства (этапы MITRE ATT&K и т. п.). Некоторое подобие механизмов реализации информационно-кибернетических и информационно-психологических деструктивных воздействий открывает перспективу успешного использования рассматриваемого аппарата в отношении консциентальных атак и операций, которые в рамках гибридной войны все чаще сочетаются с массированными компьютерными вторжениями.

3. Разумеется, мультиразмерность задач риск-анализа множественных кибератак объективно требует автоматизации их решения для всех обозначенных проектных ситуаций, включая оценку и особенно регулирование информационных рисков с использованием средств искусственного интеллекта, обеспечивающих для специалиста по защите информации нейро-аналитику в ходе реализуемого им киберпространства. Последнее, при адекватной организации машинного обучения специализированной нейросети, выглядит довольно перспективным в условиях революционного развития технологий искусственного интеллекта и экономики данных, которые также все чаще становятся сегодня объектами атак злоумышленников.

Перечисленные направления представляются достаточно актуальными в контексте осуществления проектной деятельности средствами риск-анализа (по обеспечению информационной безопасности компьютерных, автоматизированных информационных и телекоммуникационных систем и сетей), а решение сформулированных в настоящей работе подзадач будет способствовать успеху настоящего исследования.

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.: ил. – Серия «Теория сетевых войн»; Вып. 8.

2. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения: 05.07.2024).

3. UNSW_NB15. URL: https://www.kaggle.com/datasets/ (дата обращения: 07.07.2024)..

4. Методический документ от 28.10.2022г. ФСТЭК России. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. URL: https:// fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/ metodicheskij-dokument-ot-28-oktyabrya -2022-g-2 (дата обращения: 10.07.2024).

5. The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org/ (дата обращения: 11.07.2024).

6. NIST Common Vulnerability Scoring System Calculator. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата обращения: 11.07.2024).

7. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 12.07.2024).

8. Каталог известных эксплуатируемых уязвимостей (CISA KEV). URL: https://www.cisa.gov/known-vulnerabilities-catalog (дата обращения: 12.07.2024).

9. Сигорский В. П. Математический аппарат инженера. – К: Техника, 1977-768с.

10. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся ВТУЗов. –М: ОГИЗ, 1648-556с.

11. Атакуемые взвешенные сети / А. Г. Остапенко, Д. Г. Плотников, А. О. Калашников и др.; Под ред. академика РАН Д. А. Новикова. –М: Горячая линия – Телеком, 2017-284с. Серия «Теория сетевых войн»; вып. 2.

12. Розенвассер Е. Н., Р. М. Юсунов. Чувствительность систем управления. –М: Наука, главная редакция физико-математической литературы. 1981-464с.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 17.07.2024

Информация об авторе

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

METHODS AND ALGORITHMS FOR RISK ANALYSIS OF THE SUCCESS OF IMPLEMENTING MASSIVE CYBER ATTACKS

A.A. Ostapenko

The relevance of the study of massive cyberattacks is substantiated through an assessment of the probability of their success and the damages that arise in this case. It is assumed to use various types of discrete probability distributions, where it is recommended to evaluate the success of a single attack using CVSS calculators, taking into account both the variety of the type of attack being implemented and the features of the vulnerability exploited by it. It is proposed to evaluate the probability of success of a set of attacks of a given vector on a complex of vulnerabilities of the protected system using a multinomial distribution, which (in the case of attacks on a single vulnerability) is expressed in a binomial distribution. The most expected situations are determined through the frequency of successful implementation of the vector-vulnerability combination. In turn, the damage can be assessed through the criticality of exploited vulnerabilities. As a result, using the appropriate fields of the CVSS calculator, it is possible to associate the amount of damage with its varieties (violations of accessibility, integrity, confidentiality). It is proposed to describe the situation with a "downpour" of diverse attacks using a temporary risk assessment of the amount of damage approaching the level of loss of operability of the protected system, where the damage will be estimated by the product of the value of the downtime interval by the cost of a unit of downtime of the attacked object. The above is illustrated in the form of flowcharts of the corresponding risk analysis algorithms. It is proposed to use sensitivity functions to manage risks. The use of sensitivity functions opens up the prospect of analytical risk management. The work also contains tables that clearly demonstrate the processes: the formation of pairs "type of attack – exploited vulnerability; the selection of expert assessments to determine the probability and damage of a single attack "attack-vulnerability", as well as the formulation of tasks necessary for adequate goal–setting of the study.

Keywords: cyberattack, probability, damage, vulnerability, distribution, frequency, criticality, simplicity, algorithm, sensitivity.

Submitted 17.07.2024

Information about the author

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