УДК 004.056

БЕЗОПАСНОСТЬ БОЛЬШИХ ИНФОРМАЦИОННЫХ СИСТЕМ: ЦЕЛЕПОЛАГАНИЕ АВТОМАТИЗАЦИИ БОРЬБЫ С КИБЕРАТАКАМИ

А.А. Остапенко
Воронежский государственный технический университет
Россия, 394049, Воронеж, ул. Ватутина, 1
E-mail: alexostap123@gmail.com

А.П. Васильченко
Финансовый университет при Правительстве Российской Федерации
Россия, 117997, Москва, Профсоюзная ул., 45
E-mail: rainicheck@yandex.ru

Ключевые слова: система, безопасность, риск, ущерб, вероятность, регламент, база знаний и данных.

Аннотация: В порядке развития инструментария риск-анализа в работе предложены оригинальные подходы к оценке рисков, учитывающие нарушение качеств информации и работоспособности защищенных систем и сетей под воздействием разнообразных векторов атак используемых ими уязвимостей, предложена автоматизация разработанных методик в виде калькуляторов риска частичной, либо полной утраты ценности, конфиденциальности и доступности информации с учетом специфики защищаемого объекта и множества атакуемых ею уязвимостей. Кроме того, предлагается создание банка знаний кибератак и уязвимостей в виде агрегированных регламентов различных стадий противодействия вторжениям, включая текущее реагирование и ликвидацию последствий в отношении зарегистрированных инцидентов, где пользователь может в диалоговом режиме получить из банка практические рекомендации по борьбе с многообразием сценариев атак и брешей, используемых злоумышленниками.

1. Введение

Излишне упоминать о стремительном росте количества компьютерных вторжений в большие информационные системы (БИС), акцентирующем внимание исследователей киберпространства на нарушениях его безопасности [1], в основе которых лежат сочетания векторов (сценариев) реализации атак и уязвимостей БИС, используемых злоумышленниками [2-7]. В этом контексте научно-техническому персоналу, защищающему БИС, сейчас приходится иметь дело с сотнями известных злоумышленных сценариев и тысячами выявленных уязвимостей, порождающими десятки тысяч их сочетаний, каждое из которых имеет свою специфику реагирования средств и органов защиты. Очевидная мультиразмерность вышеуказанной проблемной ситуации обуславливает необходимость автоматизации агрегирования данных и знаний о киберинцидентах, а также – выработки на их основе адекватных проектных решений по методологии и технике противоборства с ними.

2. Целеполагание

С учетом изложенного выше представляется возможным сформулировать:

- объект исследования, как проектное пространство регистрируемых инцидентов, атакуемых БИС, включающее базы данных и знаний о компьютерных атаках и уязвимостях различного профиля;
- предмет исследования в качестве оценки рисков возникновения киберинцидентов, формирования мер реагирования на них и ликвидации их последствий в условиях реализации компьютерных атак и уязвимостей БИС;
- цель исследования, состоящую в повышении защищенности атакуемых БИС за счет разработки и применения методического, алгоритмического и программного обеспечения автоматизации риск-анализа и регламентации противодействия кибератакам.

Отсюда вытекает научно-техническая задача настоящей работы, заключающаяся в создании автоматизированного инструментария для управления защищенностью БИС посредством риск-калькуляции и регламентации реагирования на инциденты, создаваемые успешной реализацией кибератак.

Исследование аналогов [2-7] позволяет констатировать наличие следующих противоречий между:

- методическим несовершенством используемых риск-калькуляторов (а именно: некорректное объединение ущербов различных по своей сущности нарушений конфиденциальности, целостности и доступности информации; для конкретной защищаемой системы отсутствие в оценках возможности учета ценности информации в вышеперечисленных нарушаемых ее качествах; ошибочное неразделение авторами калькуляций факторов частичной и полной утраты работоспособности атакуемой системы, которые требуют принципиально различные показатели в оценке возможных ущербов; необоснованное алгебраическое перемножение значений множества метрик; введение, видимо, эмпирически полученных констант в виде коэффициентов и слагаемых, которые очевидно должны меняться по ходу развития арсенала кибер-вторжений и по мере совершенствования подсистем защиты от них; некорректное введение аналогий с теорией вероятности в отношении совместного и раздельного учета факторов нарушения качеств доступности, целостности и конфиденциальности информации) и объективной необходимостью исправления вышеперечисленных недостатков в инструментах современного адекватного анализа рисков;
- затрудняющей противодействие атакам разобщенностью (структурной, терминологической, методической и др.) ресурсов CAPEC, NIST, MITRE ATT&CK, БДУ, CISA KEV (предлагающих меры, тактики, техники и калькуляцию в отношении ожидаемых инцидентов кибербезопасности) и практической потребность агрегирования и редактирования вышеуказанных баз знаний и данных в формате регламентов реагирования на инциденты и ликвидации их последствий (причем, реализация вышеизложенного, ввиду мультиразмерности множества обрабатываемых сведений, требует автоматизации процесса как на стадии формирования, так и при актуализации создаваемого информационного базиса).

Представленные выше противоречия обуславливают необходимость решения следующих задач:

- разработка методического, алгебраического и программного обеспечения оценки рисков успешной реализации кибератак, предусматривающего (с использованием данных полей CVSS) среднестатистическое раздельное измерение ущербов нарушения целостности, доступности и конфиденциальности информации доя различных CAPEC-

векторов и актуальных уязвимостей (CISE KEV), включая адаптацию метрик риска к специфике защищаемой системы (в многообразии наличиствующих в ней уязвимостей, ее защищенных объектов, стоимости информационных ресурсов атакуемых компонентов);

- в триединстве методического, алгоритмического и программного обеспечения создание автоматизированного инструментария агрегирования знаний и данных, относящихся к парам вектор атак-уязвимость БИС, имея ввиду предоставление пользователю возможности автоматического получения возможности автоматического получения регламентов противодействия в отношении всяких пар, поименованных в ресурсах CAPEC и CISA KEV.

3. Результаты

Решение перечисленных задач достигнуто в форме следующих **результатов**:

- калькулятор риска, обеспечивающий автоматизированный расчет ущербов и вероятностей их наступления для различных нарушений качеств информации и работоспособности БИС в результате реализации всевозможных компьютерных атак и с использованием ими зарегистрированных уязвимостей, а также – способствующий построению риск-ландшафтов для исследуемых сочетаний векторов кибератак и программных ошибок;
- банк знаний об инцидентах компьютерных вторжений в БИС, которые автоматизировано агрегированы в специально разработанном формате регламентов различных стадий противодействия кибератакам (реагирование и ликвидации последствий в отношении зарегистрированных инцидентов).

Новизна результатов заключается в том, что:

- предложенный калькулятор риска обеспечивает комплексный подход к оценке ущербов и вероятностей их наступления, в отличие от аналогов учитывающий различные сущность нарушения качеств информации, частичную либо полную утрату работоспособности и особенности защищаемой системы;
- впервые автоматизировано предлагается сформировать банк знаний, в диалоговом режиме предлагающий пользователю регламенты реагирования на компьютерные инциденты и ликвидации их последствий для существующего многообразия кибератак и уязвимостей, используемых ими.

Практическая ценность достигнутых результатов состоит в том, что:

- разрабатываемый калькулятор рисков открывает перспективу формирования риск-ландшафтов защищаемых БИС во всем многообразии известных векторов атак и уязвимостей при адекватном пользовании их показателей в отношении различных нарушений работоспособности и с учетом специфики атакуемого объекта;
- в широком множестве БИС различного назначения (при соответствующей адаптации к специфике заданного объекта) создаваемый банк знаний позволит весьма оперативно выдавать регламенты для борьбы с конкретными вариантами кибервторжений, что в дальнейшем даст возможность незамедлительно организовать эффективную защиту объекта.

Теоретическая значимость результатов работы является существенной в следующих аспектах:

- аналитика рисканализа, реализуемая в предложенном в работе калькуляторе, объективно имеет потенциал к совершенствованию и реально может быть развита, особенно в плане учета множества одновременно используемых уязвимостей и расширения учитываемых показателей защищаемой системы;

- в контексте современной практики применения искусственного интеллекта создаваемый банк знаний имеет перспективу своего теоретического развития в плане реализации машинного обучения и внедрения нейросетевых технологий для противодействия компьютерным атакам.

4. Заключение

Пожалуй, впервые удалость столь глубоко и масштабно рассмотреть довольно актуальную научно-техническую задачу создания инструментария, интегрирующего пестрое и мало согласованное пространство данных, техник и мер противодействия кибератакам, включая целеполагание, рисканализ и формирование знаний о регламентации борьбы с компьютерными инцидентами.

Разумеется, не все удалось учесть и точно сформулировать в настоящем исследовании, требует своей доработки и программный продукт. Однако сам факт обращения к столь масштабной проблематике и получения заслуживающих внимания теоретических и практических результатов ее хотя бы частичного разрешения достоин позитивной оценки научно-технической общественности, для которой далее предлагаются развернутые характеристики достижений настоящей работы.

Список литературы

1. Остапенко Г.А., Щербакова Д.В., Калашников А.О. и др. Организационно-правовая защита сетей / Под ред. Академика РАН Д.А. Новикова. Горячая линия – Телеком, 2023. 228 с.
2. The Common Attack Pattern Enumeration and Classification (CAPEC). Электрон. дан. Режим доступа: https://capec.mitre.org/.
3. NIST Information Technology Laboratory National Vulnerability Database. Электрон. дан. Режим доступа: https://nvd.nist.gov/vuln.
4. MITRE ATT&CK. Электрон. дан. Режим доступа: https://attack.mitre.org/matrices/enterprise/.
5. NIST Common Vulnerability Scoring System Calculator. Электрон. дан. Режим доступа: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.
6. База данных угроз безопасности информации. Электрон. дан. Режим доступа: https://bdu.fstec.ru/threat.
7. Каталог известных эксплуатируемых уязвимостей (CISA KEV). Электрон. дан. Режим доступа: https://www.cisa.gov/known-vulnerabilities-catalog.