DOI 10.36622/1682-7813.2025.28.1.003
УДК 349:004.056

МЕТОДИКА АНАЛИЗА РИСКОВ КОМПЛЕКСНЫХ КИБЕРАТАК НА УСТРОЙСТВА СО ВСТРАИВАЕМОЙ ОПЕРАЦИОННОЙ СИСТЕМОЙ ПУТЕМ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ ДЕЙСТВИЙ НАРУШИТЕЛЯ

А.Л. Сердечный, М.В. Чесноков, П.Н. Поваляев, Л.В. Паринова, В.М. Питолин

В данной статье рассматривается методика анализа рисков комплексных кибератак на системное программное обеспечение компьютерных систем, построенных на базе встраиваемых операционных систем. Применяется метод моделирования сценариев действий нарушителя для оценки вероятности ущерба и выработки стратегий по его снижению. Представлены принципы использования сетей Петри и метода Монте-Карло для построения моделей атак. Описаны основные риски, связанные с уязвимостями программного обеспечения, и предложены меры по их минимизации.

Ключевые слова: кибератака, анализ рисков, моделирование атак, сети Петри, метод Монте-Карло, встраиваемые операционные системы, системное программное обеспечение.

Введение

Современные компьютерные системы, основанные на встраиваемых операционных системах, являются объектами постоянных атак злоумышленников. Эти системы широко используются в промышленности, автомобилестроении, медицинских устройствах и других критически важных отраслях, что делает их потенциальной мишенью для атак. Нарушение их работы может привести к серьезным последствиям, включая утечку конфиденциальных данных, нарушение функционирования инфраструктуры и значительные финансовые потери [1-6].

Злоумышленники используют различные методы атак, такие как эксплуатация уязвимостей программного обеспечения, атаки на доверенные цепочки поставок, вредоносные обновления и эскалация привилегий. Анализ возможных сценариев атак и оценка их рисков становятся важными аспектами обеспечения безопасности таких систем. Рост количества атак отображён на рис. 1.

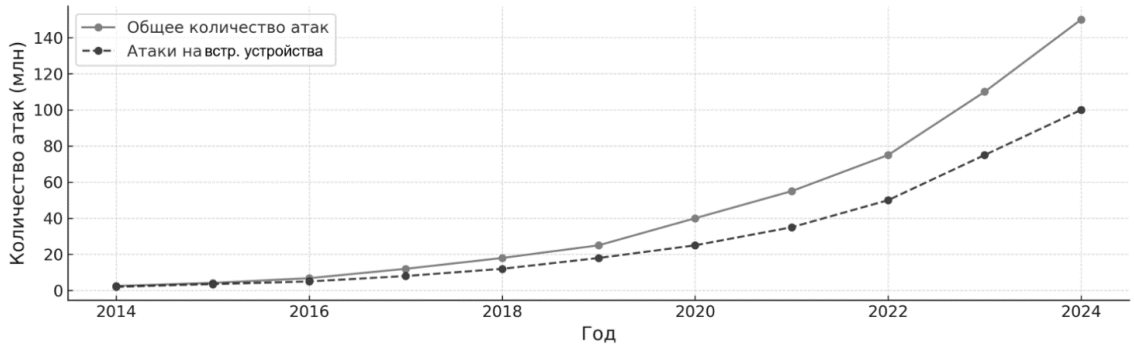

Рис. 1. Количество атак за год

Одним из наиболее эффективных способов выявления слабых мест и прогнозирования последствий атак является моделирование действий нарушителя. Данный подход позволяет не только определить вероятные векторы атак, но и оценить их влияние на систему, а также предложить меры по снижению рисков.

В данной статье представлена методика анализа рисков, основанная на моделировании сценариев атак с использованием сетей Петри и метода Монте-Карло [7-8]. Сети

Петри позволяют визуализировать возможные этапы атаки, в то время как метод Монте-Карло дает возможность провести количественный анализ вероятностей различных исходов атак. Основная цель исследования – риск-анализ успешных атак и разработка механизмов снижения рисков, что способствует повышению защищенности встраиваемых компьютерных систем.

Формирование сценариев кибератак на программное обеспечение компьютерных систем, построенных на базе встраиваемых операционных систем

Одним из первых шагов в анализе рисков является выявление слабых мест рассматриваемых устройств. В этом исследовании был использован инструмент EMB3D, который позволил связать различные идентификаторы угроз и уязвимостей, включая TID (Threat ID), CWE (Common Weakness Enumeration) и CVE (Common Vulnerabilities and Exposures). Это позволило провести детальный анализ известных уязвимостей и оценить потенциальные сценарии атак.

На этом этапе анализируются известные уязвимости (CVE), связанные с используемым программным обеспечением, а также применяемые злоумышленниками техники атак (по классификации MITRE ATT&CK). В рамках исследования использовался инструмент EMB3D для связи между идентификаторами угроз (TID), уязвимостями (CWE) и конкретными эксплойтами (CVE), что позволило построить более точную картину возможных атак и их последствий [9-10]. На рис. 2 представлена связь между идентификаторами угроз, техниками для их реализации и эксплуатируемыми уязвимостями, направленными на программное обеспечение.

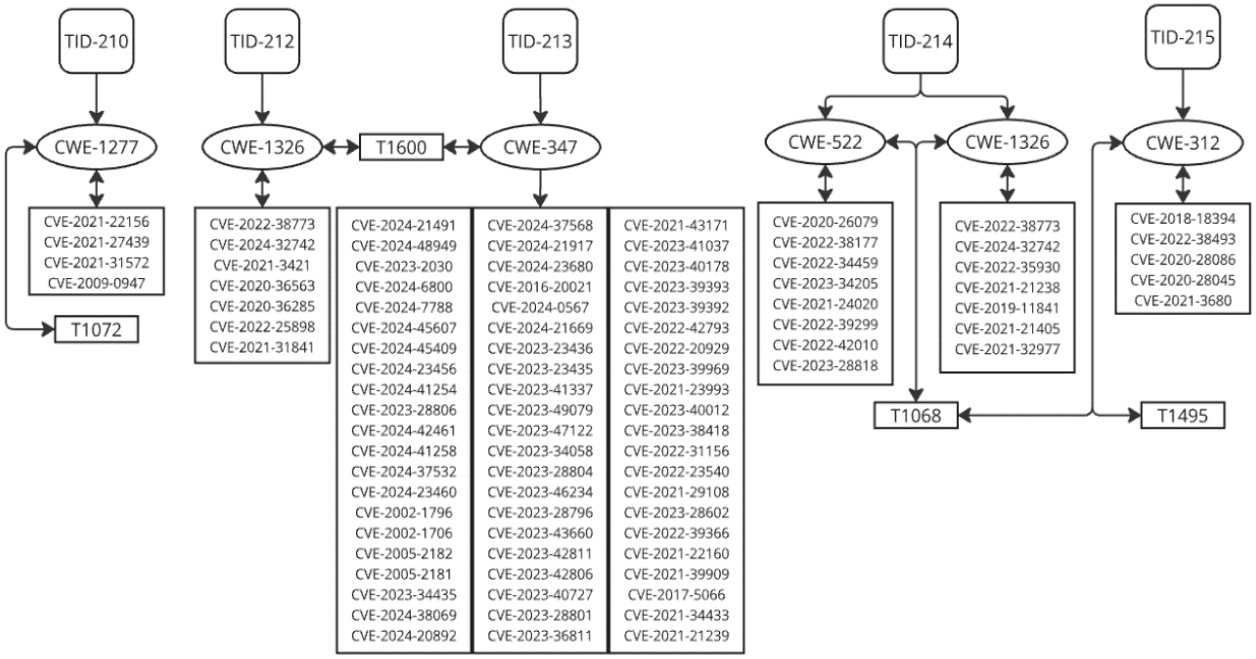

Рис. 2. Взаимосвязь между угрозами, техниками и уязвимостями

На рис. 2 представлены следующие взаимосвязи:

– TID-210: Device Vulnerabilities Unpatchable, позволяющая использовать уже известные уязвимости. Однажды обнаруженная уязвимость будет доступна для использования на всех устройствах, на которых установлено это встроенное ПО, в течение всего срока его службы;

– TID-212: FW/SW Update Integrity Shared Secrets Extraction, позволяющая внедрить вредоносное программное обеспечение на устройство. Предварительно требуется получить ключ для проверки обновлений с другого устройства;

– TID-213: Faulty FW/SW Update Integrity Verification, позволяющая внедрить вредоносное программное обеспечение на

устройство. Устройство имеет некорректную проверку цифровой подписи;

– TID-214: Secrets Extracted from Device Root of Trust, позволяющая подписать вредоносную версию программного обеспечения. Злоумышленнику необходимо получить доступ к неизменяемым корневым сертификатам;

– TID-215: Unencrypted SW/FW Updates, позволяющая провести обратное проектирование обновление программного обеспечения.

Формирование моделей кибератаки в виде последовательности реализации MITRE-техник

Визуализация действий злоумышленника в виде последовательности техник, описанных в базе MITRE ATT&CK, позволяет получить структурированное и понятное представление о сценариях атак. Это особенно важно для сложных атак, где последовательность действий и их взаимосвязи играют ключевую роль.

Граф на основе сетей Петри представляет собой математический инструмент для моделирования дискретных событий в системах с параллельными процессами. Основными элементами графа являются позиции (узлы), переходы (действия) и дуги, связывающие их. Позиции описывают состояния системы, переходы — события, которые изменяют эти состояния, а дуги задают направления переходов [11]. Маркировка сети, представленная цветными маркерами, определяет текущие уязвимости системы.

Сети Петри являются мощным инструментом для моделирования, анализа и верификации дискретных событийных систем.

Они предоставляют формальный математический аппарат для описания процессов, состоящих из множества взаимодействующих компонентов, что делает их особенно подходящими для представления сценариев кибератак.

В рамках данного пункта рассматривается методология построения графических моделей сценариев атак, где каждое действие злоумышленника представлено как узел, связанный с техникой из базы MITRE ATT&CK. Такой подход не только упрощает анализ угроз, но и способствует разработке микромоделей, описывающих отдельные этапы атак.

Графическое представление позволяет:

– формализовать сложные сценарии атак;

– сравнить различные сценарии для оценки их эффективности;

– создать основу для дальнейшего анализа.

На рис. 3 представлена микромодель угроз на системное программное обеспечение, а в табл. 1 представлено описание структурных элементов микромодели.

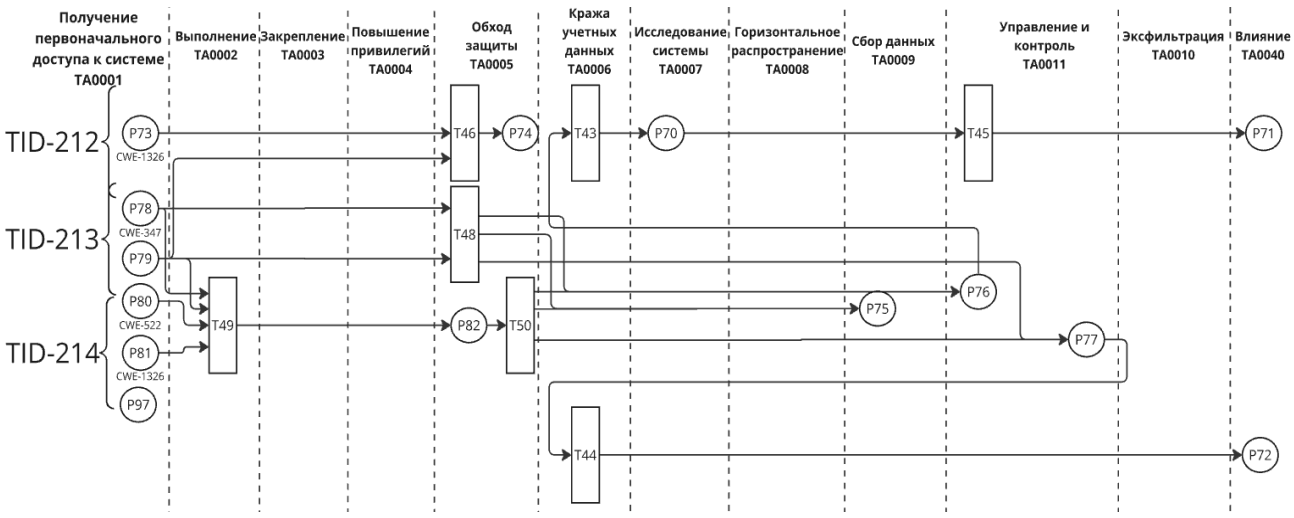

Рис. 3. Микромодель угроз, использующих механизмы проверки обновления программного обеспечения

Таблица 1

Описание элементов микромодели

Идентификатор	Описание
P70	Сброс устройства до заводских настроек невозможен
P71	Устройство выведено из строя
P72	DoS: Устройство работает некорректно
P73	Устройство использует общий ключ для проверки целостности прошивки CWE-1326: Отсутствует неизменяемый корень доверия в оборудовании
P74	Злоумышленник извлекает общий секретный ключ с устройства, делая его доступным для дальнейшего использования
P75	Получен доступ к конфиденциальным данным
P76	Устройство потеряло соединение с остальной системой
P77	Устройство работает под воздействием вредоносной логики
P78	Устройство использует прошивку с цифровой подписью CWE-347: Неправильная проверка криптографической подписи
P79	Устройство поддерживает обновления прошивки
P80	Устройство имеет корень доверия CWE-522: Недостаточная защита конфиденциальных данных
P81	Корень доверия физически доступен или не является неизменяемым CWE-1326: Отсутствует неизменяемый корень доверия в оборудовании
P82	Получен доступ к материалам аутентификации корня доверия
P97	Удалённое управление устройством через изменение конфигурации сервиса
T43	Отключение возможности перезаписи обновления T1074
T44	Манипуляция работой устройства T1074
T45	Устройство теряет функциональность T1068
T46	Извлечение общего секретного ключа из устройства T1600
T48	Обход механизмов проверки подписи прошивки T1600
T49	Эксплуатация уязвимости безопасности корня доверия для извлечения конфиденциальных данных T1068
T50	Злоумышленник подписывает вредоносную прошивку T1495
T65	Деструктивное воздействие на ОС T1495
GT2	Запушено вредоносное ПО

Формирование сценариев атак на основе последовательности MITRE-техник и построение микромоделей для их реализации позволило детализировать возможные действия злоумышленников на каждом этапе атаки. Подход позволяет не только анализировать возможные пути атак, но и определять наиболее уязвимые точки для защиты.

Расчет вероятностей успешности реализации различных вариантов сформированных сценариев кибератак

Первым шагом для расчёта является определение частоты использования конкретного типа ошибки. Для CWE, представленных на рис. 3 рассчитаны частоты в табл. 2.

Таблица 2

Частота наличия CWE

Идентификатор CWE	Частота использования
347	0,4875
522	0,0294
1326	0,2857

Используя частоту успешной эксплуатации ошибок, можно применить метод численного анализа сложных моделей. Метод Монте-Карло является мощным инструментом для численного анализа сложных систем, основанным на статистическом моделировании случайных процессов. Широко используемый метод в различных областях науки и техники, включая физику, экономику и, всё чаще, информационную безопасность. Его ключевая идея заключается в многократном проведении экспериментов или симуляций с использованием случайных входных данных, что позволяет оценить вероятности различных событий или найти приближённые решения задач, для которых точное аналитическое решение недоступно [126].

Суть метода Монте-Карло заключается в имитации поведения модели на основе случайно сгенерированных чисел, а также последующей статистической оценке данных. Для оценки вероятности события проводится серия независимых экспериментов, в ходе которых фиксируется количество раз, когда событие E произошло. Оценка вероятности рассчитывается как отношение количества достижений i позиции к общему количеству проводимых экспериментов.

Основной целью использования метода является – оценка вероятности успешности реализации атак на системное программное обеспечение. Одна итерация метода представляет собой моделирование сценария атаки на основе входных данных, полученных случайно. Такие данные отражают возможность использования злоумышленником определенного набора уязвимостей. Погрешность данного метода < 0,8%. Для автоматизации процесса получения эмпирических результатов эксперимента было реализовано программное решение. Данное решение позволяет многократно моделировать сформированный сценарий атаки. Рассмотрим основные этапы работы программы:

– первым этапов является формирование таблицы связей исходной модели;

– второй этап заключается в определении параметров начальных модели;

– определение начальных позиций, добавление их в список для обработки. Позиция является начальной если она не имеет входящих связей;

– добавление маркера в каждую начальную позицию на основе рассчитанной частоты появления, с помощью генератора случайных чисел от 0 до 1. Маркер будет добавлен в позицию если полученное случайное число будет от 0 до заданной частоты появления;

– для каждой позиции проверяются следующие после нее переходы. Для каждого перехода, связанного с рассматриваемой позицией, проверяется следующее условие: каждая приводящая к переходу позиция была достигнута и в каждой из позиций присутствует маркер. Если данное условие выполняется то все последующие позиции после перехода отмечаются как достигнутые, обновляется текущий список для обработки;

– возвращается список достигнутых позиций в формате позиция и количество её достижений.

Для позиций на рис. 3 получены следующие результаты: P71 достигается с частотой 0,1361, а P72 с частотой 0,1799.

Полученные ранее эмпирические вероятности позволяют оценить частоту наступления определенного события, основываясь на взаимосвязи используемых злоумышленником техник. Однако, данный подход позволяет сформировать лишь базовое понимание. Чтобы перейти к более детальному анализу, необходимо провести сравнение между полученными эмпирическими значениями и теоретическими распределениями.

При осуществлении проверки используется критерий Пирсона. Данный статистический метод позволяет оценить согласованность между имеющимися частотами успешности реализации атак и их теоритическими значениями. Критерий Пирсона основан на вычислении суммы квадратов отклонений между наблюдаемыми и ожидаемыми значениями.

В роли теоретической модели выступит распределение Пуассона, хорошо описывающее происходящие редко события при определенной средней интенсивности за исследуемый промежуток времени. В рамках данной работы событие – успешно реализованная атака.

Вышеперечисленные методы позволят подтвердить правильность выбранной методологии, а также выявят влияние скрытых факторов. В рамках данного пункта будет получено более глубокое понимание распределения вероятностей успешности проведения атаки, что позволит точнее определить уровень риска.

Таким образом, для P71 и P72 получаем следующее распределение на рис. 4 и рис. 5 соответственно.

Реальная интенсивность атак постоянно растёт. Таким образом, для более детального понимания реальной ситуации существует необходимость перейти к нестационарному потоку. Аппроксимируя данные о количестве зафиксированных атак, получаем прирост приблизительно 4% в месяц или 12,5% за квартал. С учетом прироста получаем следующие распределения вероятностей на рис. 4-5.

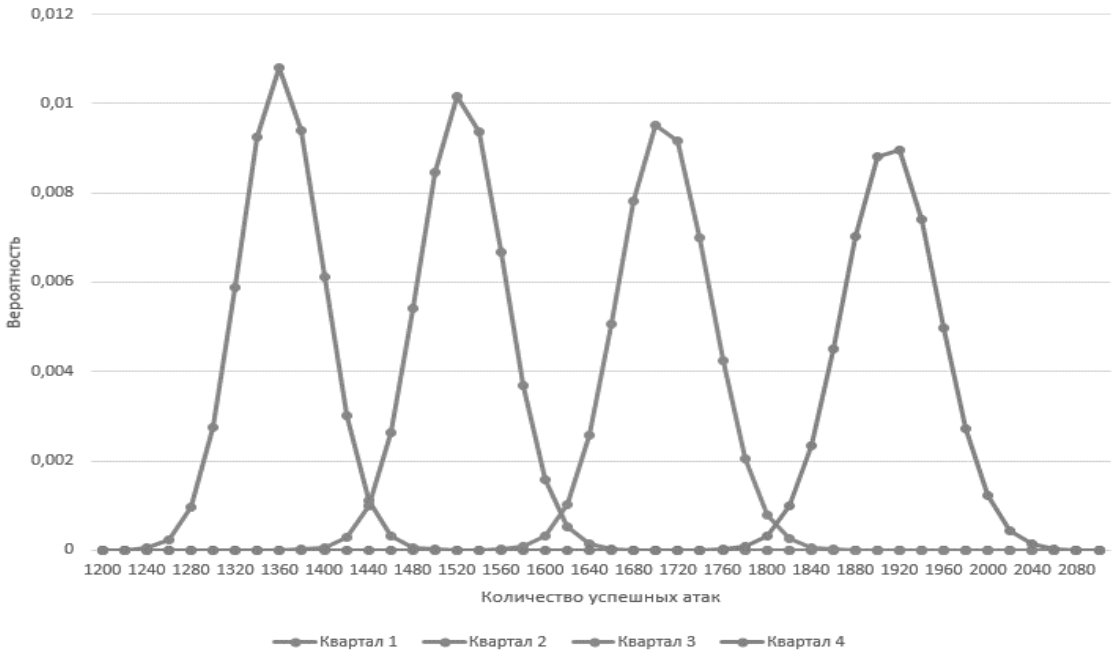

Рис. 4. Распределение вероятности P71

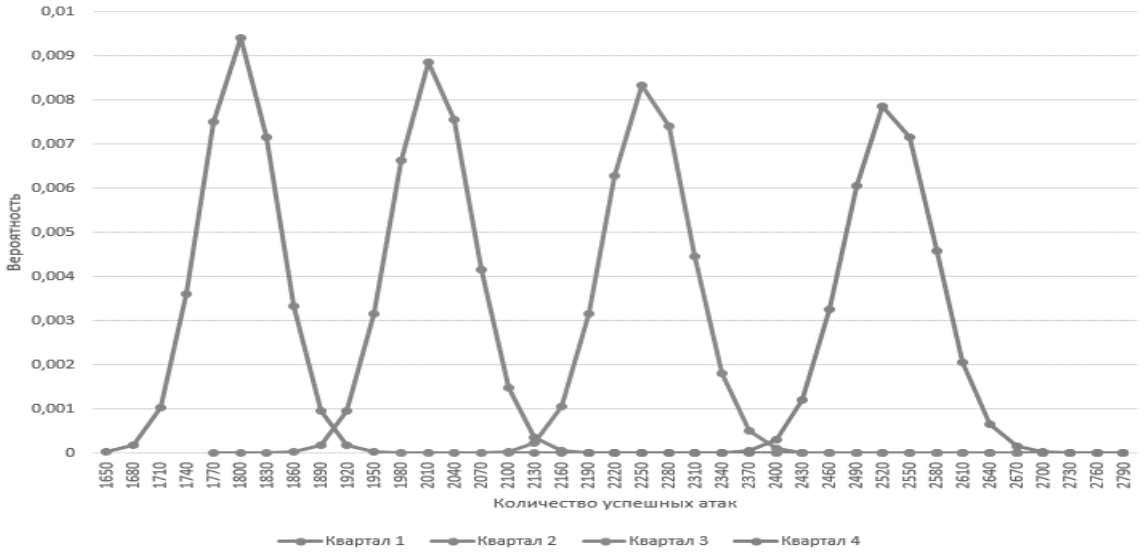

Рис. 5. Распределение вероятности P72

В данном разделе проводился анализ, направленный на определение количественной величины вероятности успешности реализации атак на системное программное обеспечение. Были вычислены исходные параметры модели, включающие в себя частоту использования определенного набора уязвимостей. На основе полученных данных вычислены значения эмпирических вероятностей успешности реализации атак.

В результате моделирования было подтверждено, что метод Монте-Карло позволяет эффективно анализировать сложные модели кибератак, учитывая множественную связь различных путей злоумышленника.

Для полученных в результате вероятностей успешности атаки был проведен анализ на соответствие распределению Пуассона. Данное сравнение позволило говорить о том, что эмпирические значения согласуются с теоретическим распределением.

Риск-анализ реализации различных вариантов сформированных сценариев атак на программное обеспечение компьютерных систем, построенных на базе встраиваемых операционных систем

Расчёт рисков кибератаки является ключевым этапом анализа угроз, направленным на количественную оценку потенциального ущерба и вероятности наступления нежелательных событий. В основе данного подхода лежит представление о том, что риск — это функция вероятности реализации атаки и её последствий. На следующем этапе свяжем результаты расчётов вероятностей атак с соответствующими уровнями ущерба, создавая графики, где ось ординат будет отражать риск, а ось абсцисс — величину ущерба. Эти графики не только визуализируют риски, но и позволяют лучше понять, какие сценарии атак оказывают наибольшее влияние на систему. На рис. 6 представлена зависимость риска от потенциального ущерба для P71: устройство выведено из строя. На рис. 7 представлена зависимость риска от потенциального ущерба для P72: устройство работает некорректно.

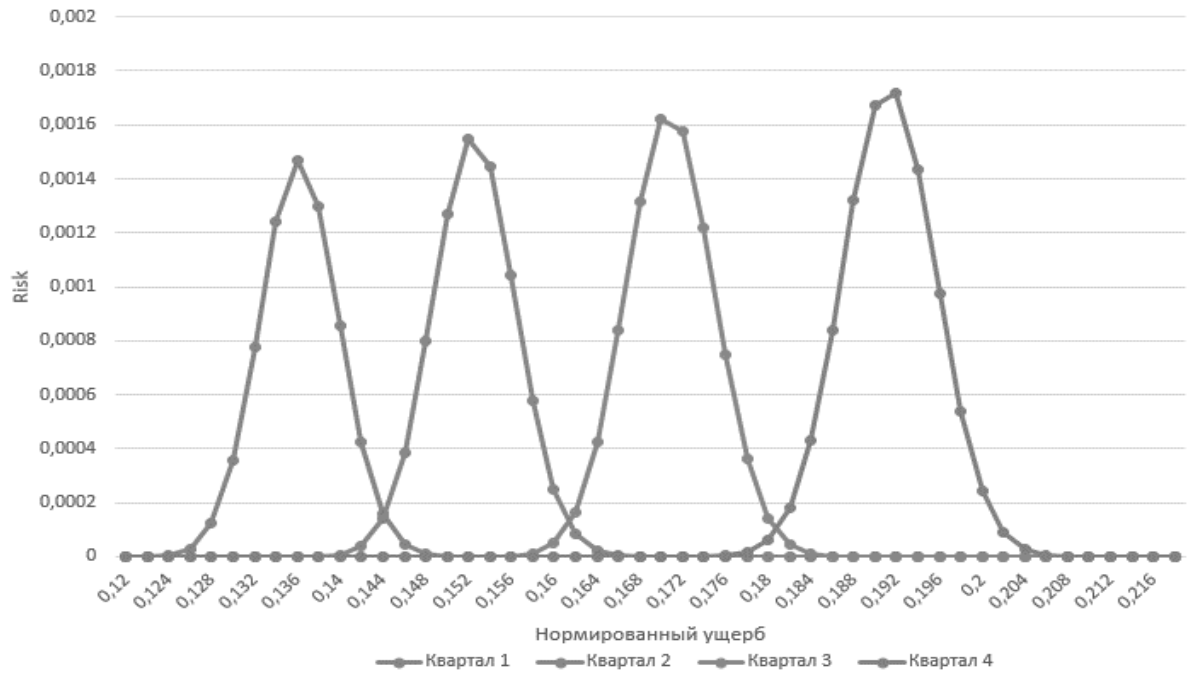

Рис. 6. Риск выведения устройства из строя

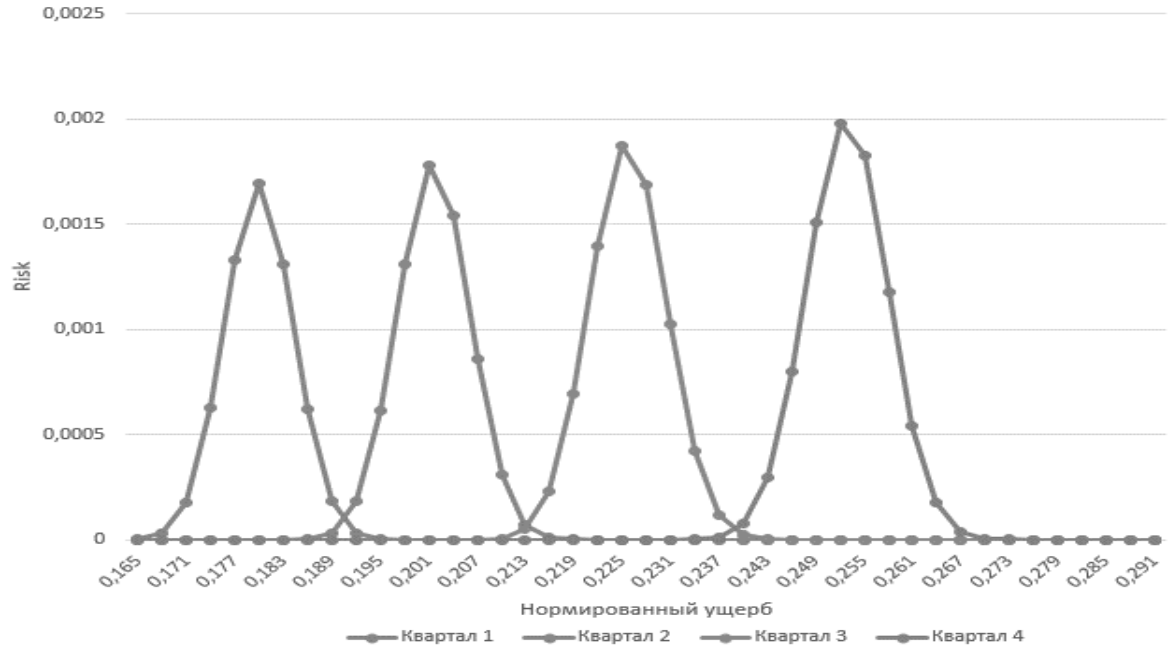

Рис. 7. Риск нарушения работоспособности устройства

Анализ графиков распределения рисков для различных сценариев атак позволяет выявить наиболее критичные угрозы, которые требуют особого внимания. Высокие значения рисков были отмечены для следующих ситуаций:

- отказ в обслуживании, связанный с нагрузкой ключевых функций устройства;
- нарушения функциональности среды виртуализации;
- нарушения работоспособности устройства в ходе злоупотреблением функций диагностики;
- выведения устройства из строя в ходе постоянно инициализируемого обновления;
- компрометации устройства посредством внедрения руткита.

Высокие риски в указанных случаях обусловлены сочетанием нескольких факторов, включая сложность обнаружения атак, критичность затрагиваемых функций и потенциальные последствия для устройства и всей инфраструктуры. Например, компрометация руткитом предоставляет злоумышленникам полный контроль над устройством, что может привести к цепным атакам, охватывающим другие элемен тысистемы. Отказ в обслуживании и нарушения в виртуализации могут существенно затруднить функционирование критически важных систем, влияя на доступность сервисов и данных. Атаки, связанные с диагностикой или обновлением, используют встроенные механизмы управления, что делает их особенно опасными при недостаточном уровне защиты.

Эти наблюдения указывают на необходимость разработки дополнительных мер защиты, направленных на снижение вероятности реализации атак и минимизацию их последствий.

Для снижения риска отказа в обслуживании, связанного с механизмами обновления прошивки, необходимо обеспечить безопасность всех этапов процесса, начиная с проверки аутентичности и целостности обновлений. Устройство должно гарантировать, что загружаемая прошивка не подверглась изменениям, что достигается использованием цифровых подписей. Производитель подписывает прошивку с помощью защищенного закрытого ключа, а устройство, обладая соответствующим открытым ключом, проверяет подлинность подписи. Этот процесс обеспечивает защиту от подделки и вмешательства в содержимое обновлений. На рис. 8 представлены внедренные меры защиты D1: проверка целостности прошивки, D2: шифрование данных в прошивке.

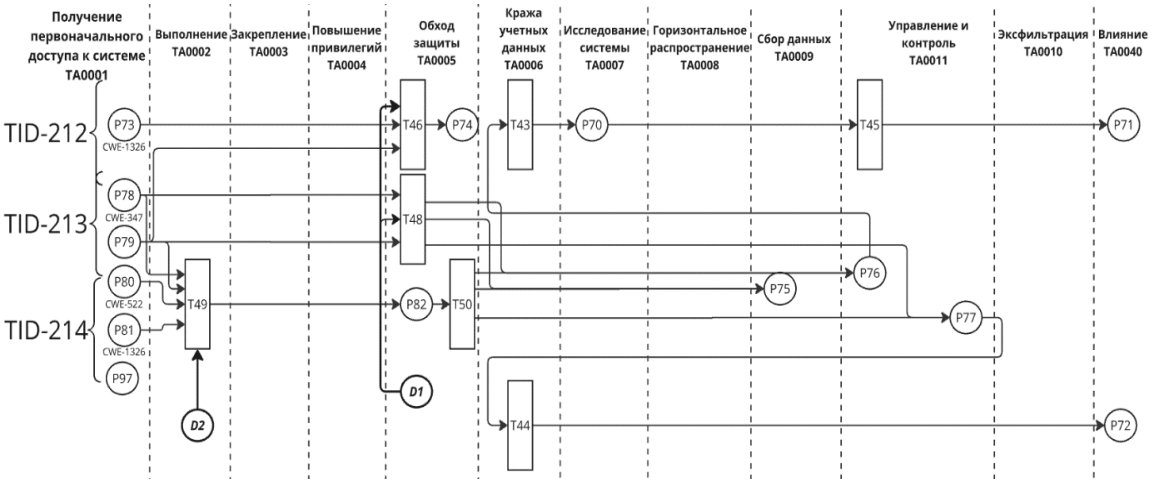

Рис. 8. Внедрение мер защиты

Заключение

В ходе выполнения работы была проведена комплексная оценка рисков реализации кибератак на системное программное обеспечение компьютерных систем, построенных на базе встраиваемых операционных систем, на основе статистики реальных инцидентов, что позволяет предложить эффективные меры защиты устройств.

Таким образом, работа достигла своей цели — повышения защищенности компьютерных систем, построенных на базе встраиваемых операционных систем, через детализированный анализ рисков кибератак, их вероятности и последствий, а также выработку эффективных мер для управления этими рисками.

Список литературы

1. Эпидемии в телекоммуникационных сетях / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. Сер. Теория сетевых войн. Вып. 1. М: Горячая линия – Телеком, 2017. 284 с.

2. Атакуемые взвешенные сети / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. Сер. Теория сетевых войн. Вып. 2. М: Горячая линия – Телеком, 2017. 284 с.

3. MITRE ATT&CK. / URL: https://attack.mitre.org/matrices/enterprise/.(дата обращения: 5.01.2025).

4. MITRE EMB3D. URL: https://emb3d.mitre.org/ (дата обращения: 5.01.2025).

5. CVE. / URL: https://cve.mitre.org/ (дата обращения: 5.01.2025).

6. Банк данных угроз безопасности информации ФСТЭК России. / URL: https://bdu.fstec.ru/threat. (дата обращения: 5.01.2025).

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. Остапенко Г.А. Автоматизированный банк знаний и калькулятор рисков реализации кибератак и уязвимостей (часть II) / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Д.С. Нестеров, А.С. Дубов, В.А. Старцев // Информация и безопасность. 2024. Т. 27. Вып. 1. С. 31-54.

9. Остапенко А.А. Методики и алгоритмы риск-анализа успешности реализации массированных кибератак / А.А. Остапенко // Информация и безопасность. 2024. Т. 27. Вып. 3. С. 401-420.

10. Остапенко А.Г. Картографирование киберпространства и обеспечение информационной безопасности / А.Г. Остапенко, А.Л. Сердечный, С.Д. Трубицын, Д.А. Нархов, В.Ю. Остапенко // Информация и безопасность. 2022. Т. 25. Вып. 1. С. 115-128.

11. Сердечный А.Л. Риск-анализ и прогнозирование частоты и ущербности компьютерных атак / А.Л. Сердечный, А.С. Маликова, А.Г. Остапенко, М.Е. Волкова, Д.А. Нархов, А.Н. Бартенев. // Информация и безопасность. 2021. Т. 24. Вып. 2. С. 159-178.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection problem of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 20.01.25

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, зам. начальника отдела, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России; доцент, Воронежский государственный технический университет, e-mail: alex-voronezh@mail.ru
Чесноков Михаил Васильевич – студент, Воронежский государственный технический университет, e-mail: mixail.chesnokov.01@mail.ru
Поваляев Павел Николаевич – студент, Воронежский государственный технический университет, e-mail: povalyev.pavel6@mail.ru
Паринова Лариса Владимировна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: lv_parinova@mail.ru
Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: pitol@mail.ru

METHODOLOGY FOR ANALYZING THE RISKS OF COMPLEX CYBER-ATTACKS BY MODELING SCENARIOS OF VIOLATOR'S ACTIONS

A.G. Ostapenko, A.L. Serdeshny, M.V. Chesnokov, P.N. Povalyaev, L.V. Parinova, V.M. Pitolin

This article discusses a methodology for analyzing the risks of complex cyber attacks on the system software of computer systems based on embedded operating systems. The method of modeling scenarios of violator's actions is used to assess the likelihood of damage and develop strategies to reduce it. The principles of using Petri nets and the Monte Carlo method for building attack models are presented. The main risks associated with software vulnerabilities are described and measures to minimize them are proposed.

Keywords: cyberattack, risk analysis, attack modeling, Petri nets, Monte Carlo method, embedded operating systems, system software.

Submitted 20.01.25

Information about the authors

Alexey L. Serdechnyi – Cand. Sc. (Technical), Deputy Head of Department, State science research experimental institute of technical information protection problem of Federal service of technical an export control; Associated Professor, Voronezh State Technical University, e-mail: alex-voronezh@mail.ru
Mikhail V. Chesnokov – student, Voronezh State Technical University, e-mail: mixail.chesnokov.01@mail.ru
Pavel N. Povalyaev – student, Voronezh State Technical University, e-mail: povalyev.pavel6@mail.ru
Larisa V. Parinova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: lv_parinova@mail.ru
Vladimir M. Pitolin – Dr. Sc. (Technical), professor, Voronezh State Technical University, e-mail: pitol@mail.ru