DOI 10.36622/1682-7813.2025.28.1.006
УДК 349:004.056

РИСК-АНАЛИЗ КОМПЛЕКСНЫХ КИБЕРАТАК НА СЕТЕВЫЕ ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ, ПОСТРОЕННЫХ НА БАЗЕ ВСТРОЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

А.Л. Сердечный, К.Д. Гайсина, Д.С. Покудин, В.Г. Юрасов, Н.И. Баранников

В статье проводится анализ рисков кибератак на сетевые технологии компьютерных систем, использующих встроенные операционные системы. Рассматриваются современные угрозы информационной безопасности, выявленные на основе базы знаний EMB3D, с акцентом на уязвимости сетевых технологий. Проведен статистический анализ роста числа атак на встроенные устройства с 2014 по 2024 год, включая атаки на IoT-устройства с операционной системой Android. Авторами установлены взаимосвязи между уязвимостями, техниками, эксплуатирующими их, и возможными сценариями их реализации. Для моделирования сценариев атак применен аппарат сетей Петри-Маркова, а оценка вероятности успешных атак выполнена путем имитационного моделирования с помощью метода Монте-Карло. На основе полученных данных рассчитаны риски атак с учетом динамики роста их интенсивности.

Ключевые слова: встроенная операционная система, IoT, Android, EMB3D, MITRE, угрозы, риск, сценарий атаки, Монте-Карло, сети Петри-Маркова.

Введение

Встроенная операционная система (EOS) — это операционная система, разработанная специально для встроенных компьютерных систем. Эти системы предназначены для повышения функциональности и надёжности выполнения специализированных задач [1].

Анализ отчетов о киберинцидентах, направленных на компьютерные системы, построенные на базе встраиваемых операционных систем, показал развивающую тенденцию к многократному увеличению числа атак из года в год.

Так, в 2014 году число атак составило около 2 миллионов атак на IoT-устройства. Основными целями нарушителей были маршрутизаторы, IP-камеры, принтеры. Впервые зафиксированы крупные ботнет-сети из IoT-устройств, используемые для DDoS-атак [2].

В 2015 году число атак выросло до 3,5 миллионов. Основной тренд: рост атак на устройства умного дома и камер наблюдения. Также наблюдался рост числа атак на промышленные системы (+15%) [2, 3].

В 2016 году зафиксировано 5 миллионов атак на встраиваемые устройства. Всплеск атак связан с ботнетом Mirai, который заразил более 600 тысяч IoT-устройств. Основная угроза – массовые DDoS-атаки, мощность которых достигала рекордных значений [4].

В 2017 году нарушители атаковали компьютерные системы, построенные на базе встраиваемых ОС около 8 миллионов. Отмечается увеличение числа атак на промышленные системы SCADA и рост атак на устройства с открытыми портами Telnet и SSH [5].

В 2018 году число атак достигло 12 миллионов, а в 2019 году уже 18 миллионов. За этот период вредоносное ПО для IoT стало активнее применяться для осуществления атак. Нередки крупные DDoS-атаки на инфраструктуру телекоммуникаций [5].

В 2020 году рост атак связан с массовым переходом на удаленную работу в связи с пандемией COVID-19, что привело к показателю в 25 млн атак на встраиваемые устройства в год [2-6].

В 2021 и 2022 годах было по 35 млн и 50 млн атак на устройства со встраиваемой ОС соответственно. Отмечалась тенденция к массовому использованию IoT-устройств в ботнетах. Количество DDoS-атак выросло на 30% [6].

В 2023 году количество фиксируемых атак выходят на новый пик. За указанный период было зарегистрировано 75 млн инцидентов. Основным объектом стали

промышленные устройства, доля атак на них выросла на 40% [6].

В 2024 году отмечается очередной рост - более 100 миллионов атак. При этом 30 миллионов атак пришлись на Android-устройства (рост в 2,5 раза по сравнению с 2023 годом) [6].

Тренд роста атак связан с увеличением количества подключенных устройств и недостаточной их защищенностью.

Аналитиками также приводится статистика доли успешных атак. С 2014 года по 2024 год общий процент успешных атак вырос с 25% до 82%. За этот же период успешность DDoS-атак достигла 30%. Число атак, приводящих к нарушению работы устройства так же, возросло – 8% в 2014 году против 25% в 2024 году. По-прежнему одним из основных векторов остаются атаки, целью которых являются персональные данные и конфиденциальная информация. К 2024 году процент их успешности составил 27% от общего числа атак [5-6].

В рамках данной работы дальнейшее исследование и моделирование множества сценариев реализации кибератак происходило для встраиваемых устройств с операционной системой Android. Конкретизация объекта исследования с уточнением исследуемой операционной системы позволило детальнее подойти к требуемой выборке эксплуатируемых уязвимостей и применимых техник реализации атак.

Модель угроз информационной безопасности устройств со встраиваемой операционной системой MITRE EMB3D

Компания MITRE выпустила новую базу знаний о киберугрозах EMB3D нацеленную на структурирование имеющихся знаний об угрозах информационной безопасности для устройств, построенных на базе встраиваемых операционных систем, используемых в объектах критической информационной инфраструктуры.

Основная цель модели EMB3D – предоставить производителям устройств единое представление о различных уязвимостях в их технологиях, подверженных атакам, и механизмах безопасности для их устранения. Аналогично тому, как ATT&CK предлагает унифицированный механизм для отслеживания и передачи информации об угрозах, EMB3D стремится предложить центральную базу знаний об угрозах, нацеленных на встроенные устройства [7].

Матрица EMB3D содержит сведения об актуальных угрозах для устройств со встраиваемой операционной системой, которые классифицированы согласно атакуемым компонентам системы, в роли которых выступают аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение и сетевых технологии.

В данной работе подробно были рассмотрены угрозы, направленные на сетевые технологии компьютерных сетей, построенных на базе встраиваемых ОС, приведенные в базе знаний о киберугрозах EMB3D, а именно:

- TID-401: недокументированные функции протоколов

Некоторые устройства могут поддерживать проприетарные протоколы или добавлять проприетарные функции к открытым протоколам. Многие пользовательские функции или команды могут быть недостаточно хорошо документированы. Если пользователи не знают об этих функциях/командах, они не смогут правильно настроить устройство, чтобы удалить ненужные функции. Кроме того, они не смогут отслеживать потенциальное злонамеренное использование этих функций/команд для эксплуатации устройств [7].

- TID-404: удаленно запускаемая взаимоблокировка /DoS

Некоторые устройства имеют режимы работы, которые переводят их в нерабочее состояние. Устройства также могут иметь уязвимости в сетевом анализе или протоколе, которые могут привести к зависанию или иному состоянию, при котором устройство не отвечает на запросы. Таким образом, злоумышленник может отправить устройству сообщение, которое приведёт его в одно из этих состояний зависания или отсутствия реакции, сделав устройство неработоспособным или переведя его в другое состояние. Кроме того, если

устройство не имеет механизма сброса настроек или восстановления из этого состояния, оно может оставаться недоступным до тех пор, пока его не сбросят или не перезагружат, что может потребовать физического присутствия оператора [7].

- TID-405: исчерпание ресурсов сетевого стека

Удалённые подключения и коммуникации могут потреблять различные ресурсы устройства (например, буферы сетевого стека, обработку пакетов, сокетные подключения), которые при исчерпании могут привести к тому, что устройство перейдёт в состояние, при котором оно не будет отвечать на запросы. Злоумышленник может попытаться намеренно вызвать такое состояние, отправляя на устройство повторяющиеся или специально созданные сообщения, чтобы потреблять ресурсы и привести к тому, что устройство перестанет отвечать на запросы. Состояние, при котором устройство перестаёт отвечать на запросы, обычно сохраняется как минимум на время атаки. В некоторых случаях оно может сохраняться до тех пор, пока устройство не будет перезагружено, что может потребовать физического присутствия оператора [7].

- TID-406: несанкционированное подключение и управление

Некоторые устройства работают по протоколам, которые не поддерживают аутентификацию на сетевом уровне, подключение или создание сеансов на устройстве, что позволяет злоумышленникам устанавливать вредоносные соединения или отправлять вредоносные данные на устройство. Механизмы аутентификации включают пароли и криптографические ключи/сертификаты [7].

- TID-407: повторное воспроизведение управляющих команд

Злоумышленники могут повторно воспроизвести управляющие сообщения на устройстве, чтобы вызвать нежелательную функцию, отправить нежелательную команду или получить доступ к конфиденциальным данным. Воспроизведение сообщений может использоваться для обхода несуществующих или плохо спроектированных механизмов аутентификации, в которых отсутствуют надлежащие средства защиты, такие как одноразовый номер или временная метка [7].

- TID-408: передача конфиденциальных данных в незашифрованном виде

Некоторые устройства не обеспечивают надлежащее шифрование сообщений, содержащих операционную или управленческую информацию. Без надлежащего шифрования злоумышленник может прослушивать сообщения, чтобы получить доступ к операционной информации устройства, управленческой информации или данным для аутентификации, таким как учётные данные или ключи [7].

- TID-410: побочный канал криптографического протокола

Хотя шифрование данных может помешать злоумышленнику напрямую получить доступ к незашифрованному сообщению, злоумышленник может получить информацию об устройстве или передаваемых данных с помощью анализа побочных каналов и метаданных зашифрованных сеансов связи. Например, злоумышленник может использовать информацию о длине, последовательности и частоте сообщений, чтобы частично или полностью расшифровать их содержимое [7].

- TID-411: Слабый или небезопасный криптографический протокол

Устройство использует слабый или небезопасный криптографический протокол или алгоритм, который может быть взломан или скомпрометирован. Это может позволить злоумышленнику извлечь незашифрованную информацию из зашифрованных сообщений, извлечь криптографические ключи или обойти механизмы аутентификации [7].

Злоумышленники могут использовать различные методы для манипулирования этими протоколами, в том числе подбор ключей методом перебора или криптоанализ для расшифровки текста [7].

- TID-412: злоупотребление возможностями сетевой маршрутизации.

Некоторые устройства позволяют пересылать пакеты на другие подключенные устройства (например, маршрутизация, переадресация портов, туннелирование, VPN). Если устройство используется для переадресации или маршрутизации

сообщений, злоумышленник может изменить правила переадресации или маршруты.

Злоумышленник может использовать эту функцию, чтобы отключить необходимые правила переадресации для предотвращения разрешенных соединений или добавить новые правила, которые позволят получить несанкционированный доступ к другим устройствам. Злоумышленник может использовать это для получения доступа к устройствам, находящимся в защищенных сетях или зонах [7].

Установление взаимосвязей между уязвимостями и техниками MITRE ATT&CK, которые могут эксплуатироваться для реализации угроз EMB3D

Исходя из описаний актуальных угроз, представленных в матрице EMB3D, становится возможным осуществить выборку уязвимостей, которые может эксплуатировать нарушитель в ходе реализации кибератаки. Выборка должна осуществляться с учетом специфики выбранного объекта, а именно встраиваемого устройства с операционной системой Android.

Угроза TID-401 связана с недокументированными функциями, которые могут присутствовать на устройстве и которые позволяют вызвать нежелательное поведение системы. С данной угрозой можно связать следующие уязвимости (табл. 1), дополнительно классифицированные по типу ошибки CWE [8].

Таблица 1

Выборка уязвимостей для TID-401

Наименование и тип ошибки CWE	**Уязвимости CVE/BDU**
CWE-912 Скрытые функции	CVE-2023-6614 CVE-2021-43987 CVE-2021-24867
CWE-94 Неверное управление генерацией кода (Внедрение кода)	CVE-2017-7911 CVE-2021-43889 CVE-2024-2195
CWE-242 Использование по определению опасной функции	CVE-2021-40698 CVE-2021-42543
CWE-676 Использование потенциально опасных функций	CVE-2021-40698 CVE-2023-39495 CVE-2024-38434
CWE-475 Неопределенное поведение входных данных для API	CVE-2024-3099 CVE-2022-29207
CWE-749 Раскрытый опасный метод или функция	CVE-2023-50423 CVE-2023-50422 CVE-2023-49583 CVE-2023-50424 CVE-2024-1873 CVE-2024-35209 CVE-2023-40150 CVE-2023-36853

Аналогичным образом были сопоставлены оставшиеся TID и уязвимости, также отобранные с учетом описания слабостей системы, эксплуатируемые для реализации кибератак.

Для эксплуатации данных уязвимостей в ходе атак на сетевые технологии устройств со встраиваемой ОС стало возможным использование следующих техник (табл. 2), которые были отобраны с помощью матрицы MITRE ATT&CK. Также приведены техники из стандарта EMB3D, которые применимы исключительно к выбранному объекту исследования и позволяют отразить специфику моделируемой системы.

Таблица 2

Техники реализации TID для атак на сетевые технологии

Идентификатор техники	**Наименование**
T1203	Эксплуатация уязвимостей в клиентском ПО
T0867	Внедрение инструмента
T0886	Удаленные сервисы
T1498	Сетевой отказ в обслуживании
T1071.002	Протоколы передачи файлов
T1133	Внешние службы удаленного доступа
T0814	Перегрузка устройства большим количеством запросов
T1659	Внедрение контента
T1078	Существующие учетные записи
T0842	Прослушивание сетевого интерфейса
T0887	Прослушивание беспроводного канала связи
T1074	Промежуточное хранение данных
T1040	Прослушивание сети
T1212	Эксплуатация уязвимостей для получения учетных данных
T1110	Перебор пароля
T1078.001	Учетные записи по умолчанию
T0891	Закрепление сеанса с помощью «жестко-заданных» учетных данных
T0884	Изменение правил маршрутизации
T0836	Изменение параметров критических функций

Исходя из выбранных данных стало возможным установить следующую взаимосвязь между моделью TID, соответствующими уязвимостями с идентификаторов CVE или BDU, которые дополнительно классифицированы по типу ошибки CWE, и техниками MITRE ATT&CK, которые могут эксплуатировать данные слабости (рис. 1-4).

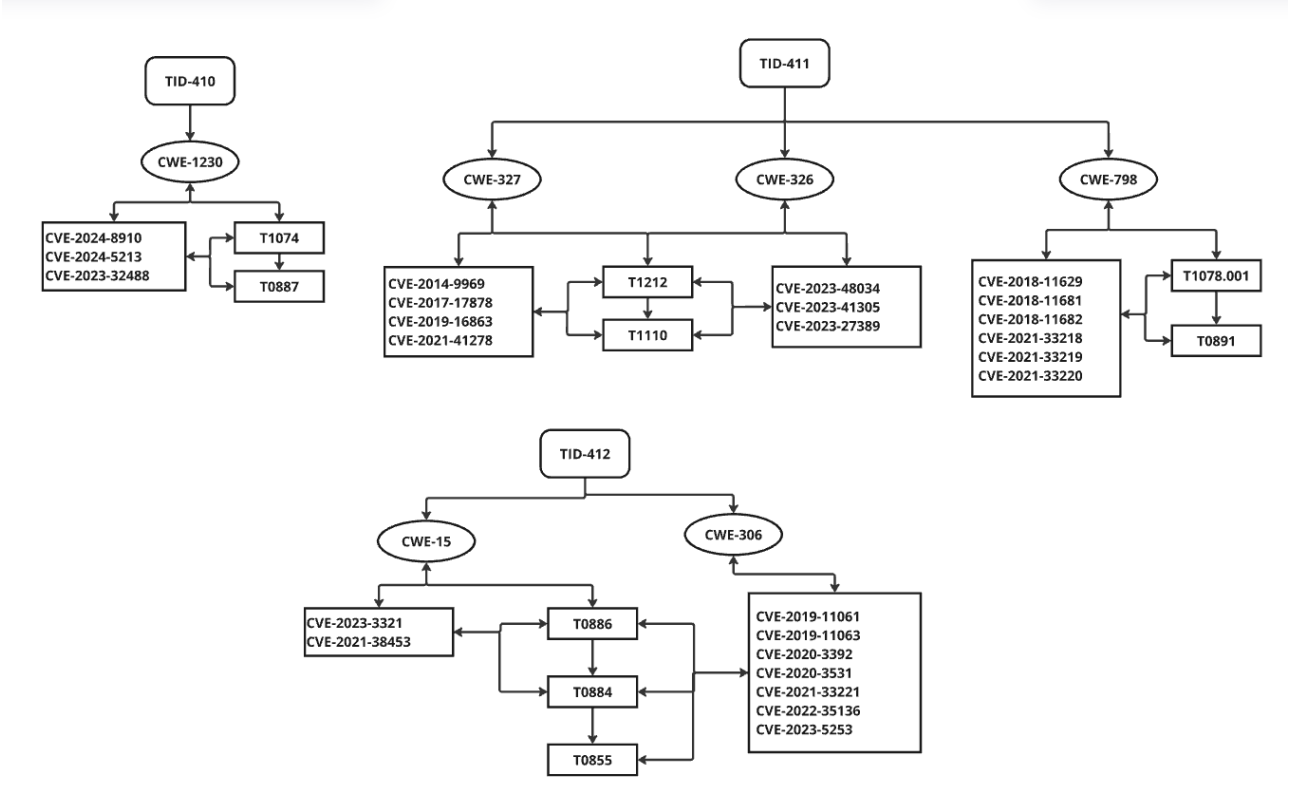

Рис. 1. Связь CWE, CVE, Техник и TID-410, 411, 412

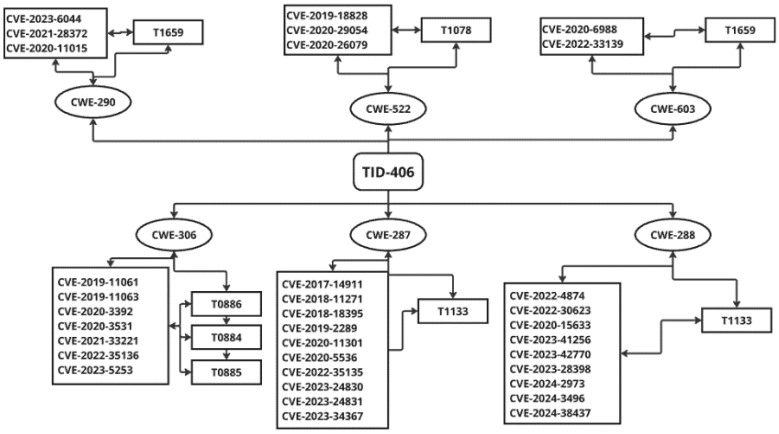

Рис. 2. Связь CWE, CVE, Техник и TID-406

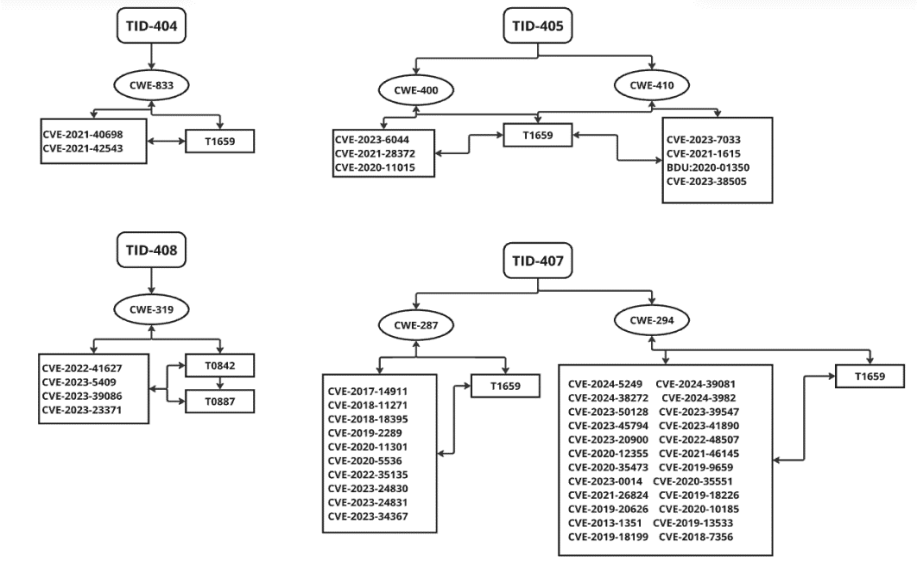

Рис. 3. Связь CWE, CVE, Техник и TID-404, 405, 407, 408

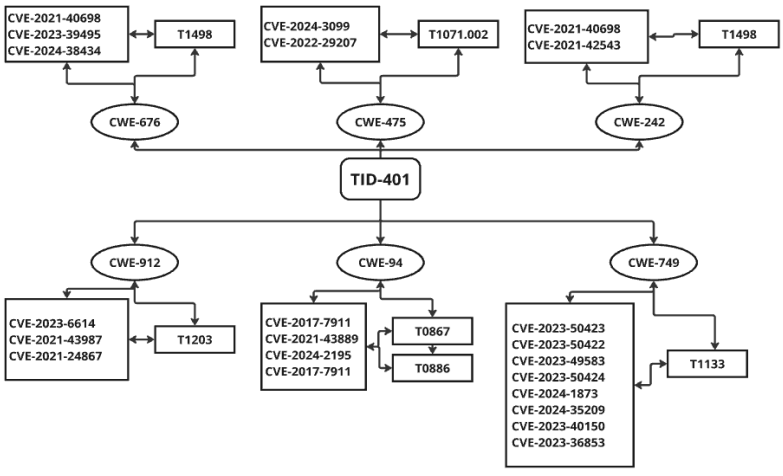

Рис. 4. Связь CWE, CVE, Техник и TID-401

Для осуществления дальнейшего моделирования множества сценариев действий нарушителя необходимо было построить графическую модель на основе выявление причинно-следственных связей между уязвимостями и техническими приемами их эксплуатации.

Формирование сценариев кибератак в виде последовательности реализации MITRE-техник

В рамках данного пункта были разработаны сценарии, основанные на последовательности MITRE-техник, что позволяет наглядно представить процесс атаки и определить критические точки защиты.

Сценарии представлены в виде графовой модели, которая представляет собой расширенную сеть Петри-Маркова и показывает причинно-следственны связи между применяемыми техническими приемами и состояниями, в которые переходит атакуемая система в результате их реализации [9-14].

Аппарат составных сетей Петри-Маркова (ССПМ) был предложен для моделирования динамики реализации угроз безопасности информации в информационных системах (ИС) и, в отличие от аппарата сетей Петри, позволяет оценивать вероятностно-временные характеристики процесса их реализации, а в отличие от традиционного аппарата сетей Петри-Маркова, учитывать не только параллельность выполняемых парциальных процессов, но и наличие различных логических условий их реализации [14-16].

Вводятся базовые понятия «условие» и «событие», которые могут быть связаны отношением типа «выполняется после» [16].

События выражают действия, реализация которых управляет состояниями системы. Состояния задаются в виде сложных условий, формулируемых как предикаты с переменными в виде простых условий. Только при достижении определенных состояний (в этом случае соответствующие предикаты принимают истинное значение) обеспечивается возможность действий (наступления событий). Условия, с фактами выполнения которых связана истинность предиката и, следовательно, возможность реализации события, называют «до-условиями» (предпосылками наступления события) [15].

В результате действия совершившегося при реализации события объявляют истинными все простые условия, непосредственно связанные с данным событием отношением «выполняется после». Эти условия рассматриваются как «пост-условия» (прямые следствия событий) [15].

Только после выполнения всех «до-условий» для некоторого события это событие может быть выполнено. После того как событие имело место, истинными становятся все «пост-условия» данного события, которые затем в свою очередь могут быть «до-условиями» каких-либо других событий, и т.д. Таким образом оформляется логическая взаимосвязь событий и условий, предопределяющих эти события, в виде логически обусловленных причинно-следственных цепочек условий и событий. Построение полной структуры таких отношений для моделируемой проблемной ситуации составляет цель и задачу формирования структуры модели [15].

В сетях Петри условия моделируются позициями, а события — переходами [14-16].

Позиция – вершина графа, которая моделирует условия выполнения перехода, осуществляемого посредством MITRE техник. Переход – вершина графа, которая моделирует события, в качестве которых рассматриваются действия нарушителя, осуществляемые в ходе реализации атаки, определяющиеся техниками MITRE ATT&CK.

Расширение сетей Петри заключается в добавлении специальных условий, определяющие правила для успешного срабатывания переходов. Действующие в сетях Петри соглашения о правилах выполнения переходов выражают логические взаимосвязи между условиями и событиями в моделируемой системе. Переход может сработать (срабатывание перехода), если выполнены все условия реализации соответствующего события. Последовательная реализация событий в системе отображается в сети в виде

последовательного срабатывания ее переходов [15].

Маркер – условия, определяющие успешность срабатывания перехода.

В рамках данной работы в качестве маркеров рассматриваются уязвимости, объединенные по типу ошибки. Маркеры помещаются в позиции и являются условиями для успешной реализации атак.

Рассмотрим участок графа, связанный с угрозами обхода процедуры аутентификации (рис. 5). Граф содержит следующие позиции, маркеры и переходы:

p1 Система предоставляет доступ к удаленным сетевым службам;

p2 Система имеет недостатки в механизмах аутентификации (CWE-287);

p3 Система содержит обходной путь, не требующий аутентификации (CWE-288);

p4 В системе отсутствует механизм аутентификации на стороне сервера (CWE-603);

p5 Система недостаточным образом защищает учетные данные (CWE-522);

p6 Устройство позволяет обойти процедуру аутентификации при повторной отправке сообщений (CWE-294);

p8 Устройство позволяет обойти процесс аутентификации путем подмены (CWE-290);

p9 Отсутствуют протоколы аутентификации;

p10 Устройство подключено по беспроводной сети;

T1 Установление соединения с помощью внешних служб удаленного доступа (T1133);

T2 Установление сеанса связи по обходному пути (T1133);

T3 Отправка вредоносного контента (T1659 (Внедрение контента);

T4 Подключение с помощью существующих учетных записей (T1078);

T5 Подключение к серверу с помощью модифицированного клиента (T1659);

T6 Подключение к системе по беспроводной сети путем компрометации беспроводного устройства (T0860);

T8 Подключение к системе по беспроводной сети путем компрометации беспроводного устройства (T0860);

T9 Подмена разрешенных IP-адресов (T1659);

GT1 Установлено соединение или сеанс связи с устройством;

T14 Закрепление в системе с помощью существующих учетных данных (T1078);

GT3 Нарушитель закрепился в компрометируемой системе;

T16 Повышение привилегий до уровня имеющихся аутентификационных данных (T1078);

GT4 Успешно повышены привилегии;

T20 Отправка поддельного отчетного сообщения (T0856);

T21 Передача управляющих сигналов в трафике (T1205);

T22 Использование неактивных учетных записей с целью предотвращения обнаружения (T1078);

GT5 Обход защиты успешно пройден;

T41 Отправка пользовательских команд (T0855);

T43 Перехват и повторная отправка командных сообщений (T0887);

T44 Отключение служб в системе (T0881);

p35 Отказ в обслуживании до перезапуска устройства;

p36 Получен доступ к системе управления устройством;

p37 Недоступность системы управления устройством;

p38 Недоступность функций мониторинга состояний устройства;

p39 Нарушение или изменение работы устройства путем повторного направления командных сообщений.

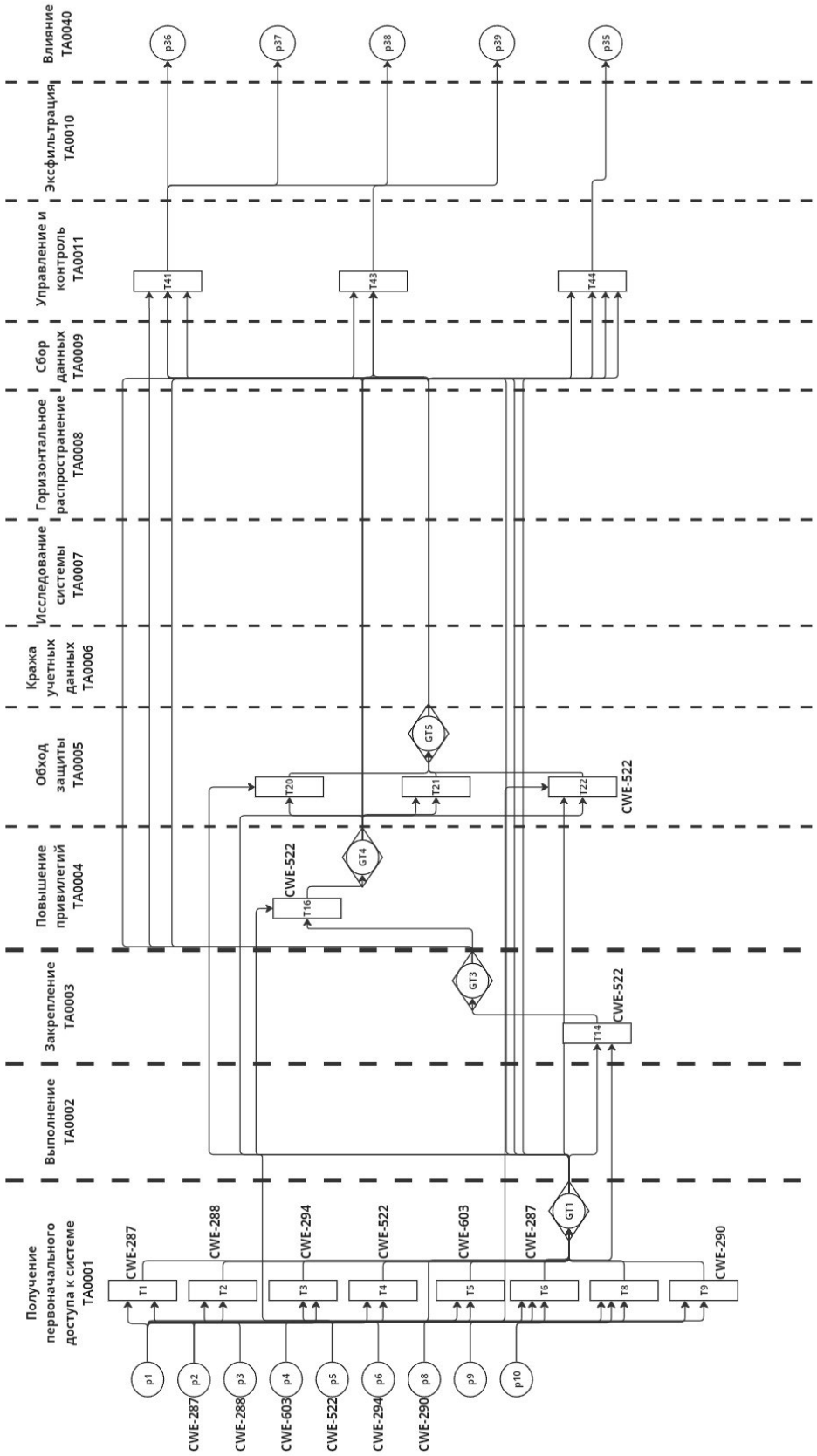

Рис. 5. Участок графа, связанный с обходом процедуры аутентификации

Объединяя все имеющиеся микрографы и дополняя их причинно-следственными связями между позициями и переходами, была получена итоговая графовая модель множества сценариев реализации кибератак на сетевые технологии компьютерных сетей, построенных на базе встраиваемых операционных систем (рис. 6).

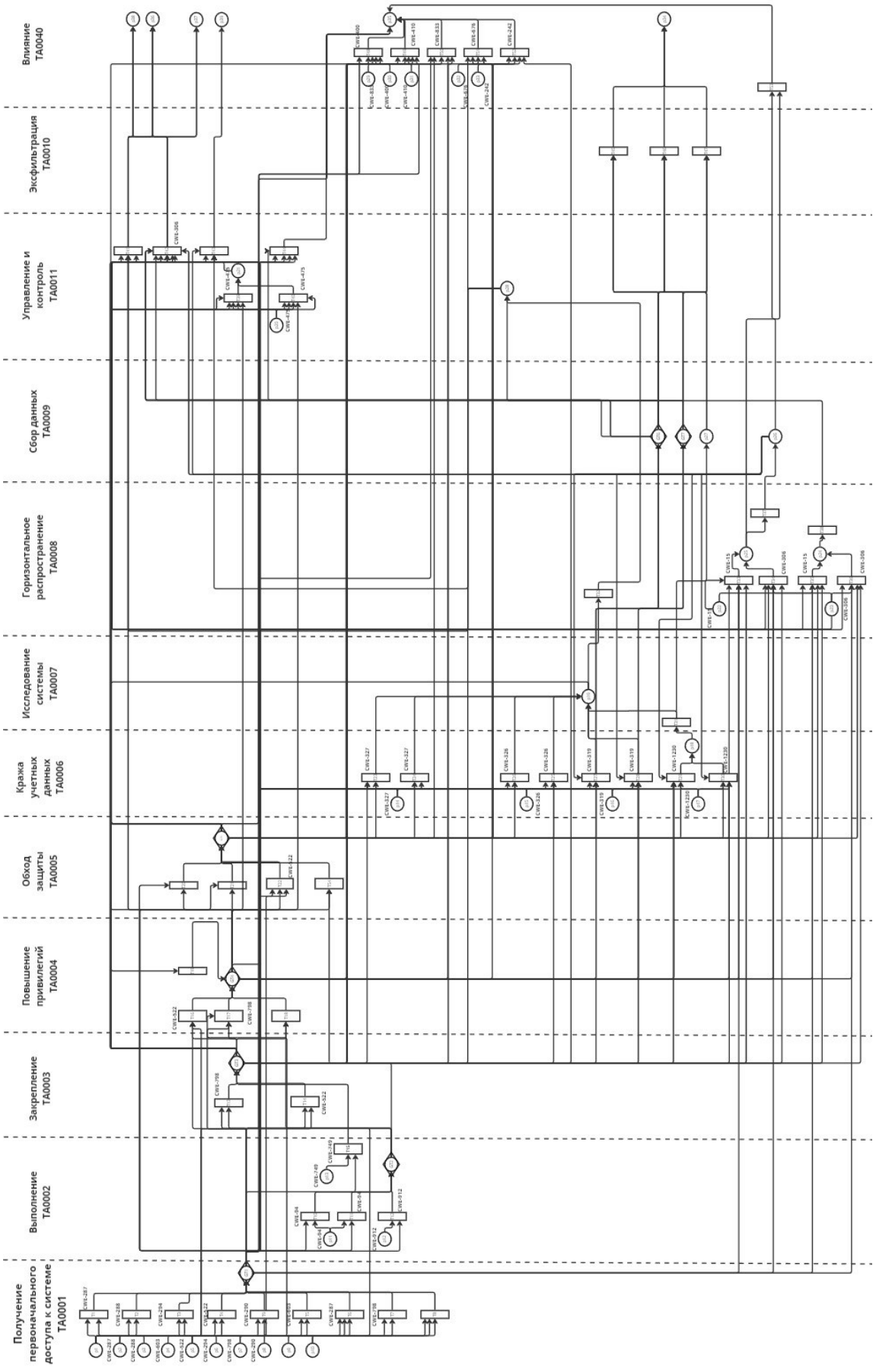

Рис. 6. Графовая модель множества сценариев реализации кибератак на встраиваемые устройства

На основе данной модели стало возможным провести расчет рисков успешной реализации кибератак. Для этого прежде всего необходимо было произвести расчеты вероятностей реализации атак и определить величину ущерба, наносимого системе в результате их успешной реализации. Данные расчеты были произведены с использованием метода имитационного моделирования, для осуществления которого было необходимо рассчитать пороговое значение, определяющее наличие маркера уязвимости в системе. Данное значение возможно получить на основе частотного анализа имеющихся сведений в базах данных БДУ ФСТЭК России, NVD NIST и CVE относительно уязвимостей сетевых технологий компьютерных систем, построенных на базе операционной системы Android.

Расчет частоты наличия уязвимостей в компрометируемой системе

Для оценки данного параметра воспользуемся данными БДУ ФСТЭК России, NVD NIST и CVE, где в достаточно полном объеме представлены описания уязвимостей встраиваемых устройств с операционной системой Android. На основе собранных данных распределение частоты наличия уязвимостей в выбранном объекте исследования выглядит следующим образом (табл. 3).

Расчеты производились по формуле (1) исходя из количества подходящий для построенной модели уязвимостей и общего количества CVE, присущих соответствующему типу ошибки.

$$\nu_{\,\mathrm{i}} = \frac{\mathrm{N_{TID}}}{\mathrm{N_{CWE}}}, \qquad (1)$$

где vi – частота наличия уязвимости;

N_{TID} – количество уязвимостей, используемых для реализации атаки;

N_{CWE} – количество уязвимостей для встраиваемых устройств в соответствующем классе уязвимостей.

Таблица 3

Частота наличия уязвимостей с определенным типом ошибки

CWE	**Частота наличия уязвимости с данным типом ошибки**
CWE-287	0,31
CWE-288	0,4
CWE-603	0,3
CWE-522	0,08
CWE-294	0,34
CWE-798	0,09
CWE-290	0,2
CWE-94	0,11
CWE-912	0,25
CWE-749	0,14
CWE-327	0,1
CWE-326	0,14
CWE-319	0,18
CWE-1230	0,27
CWE-475	0,05
CWE-15	0,15
CWE-306	0,11
CWE-833	0,1
CWE-400	0,07
CWE-410	0,57
CWE-676	0,07
CWE-242	0,09

Исходя из собранных сведений стало возможно осуществить имитационное моделирование множества сценариев заданных атак.

Расчет вероятности реализации комплексных кибератак и ожидаемых ущербов на основе построенной модели сценариев действий нарушителя

Для оценки вероятности успешной реализации различных сценариев кибератак в данной работе был использован комплексный подход, основанный на анализе вероятностей успеха каждой техники, а также на оценке воздействия успешной атаки.

Для расчета вероятности успешной реализации атак применялся метод имитационного моделирования, для которого было разработано программное обеспечения, в основу которого был положен метод Монте Карло.

Метод Монте-Карло представляет собой статистический метод моделирования, который используется для оценки вероятности и рисков, связанных с неопределённостью в системе. В контексте анализа киберугроз метод Монте-Карло позволяет учитывать случайные вариации параметров атак и вероятностей успешной реализации сценариев [17].

Основная идея метода состоит в использовании выборки случайных чисел для получения искомых оценок. Вместо того чтобы описывать процесс с помощью аналитического аппарата (дифференциальных или алгебраических уравнений), производится «розыгрыш» случайного явления с помощью специально организованной процедуры [18].

Метод Монте-Карло предполагает многократное случайное моделирование процессов с учетом вероятностных распределений для ключевых параметров, таких как вероятность успешной реализации техник и воздействия на систему [17].

Моделирование работает по следующему принципу:

1. Ввод параметров. Перед моделированием необходимо ввести общее количество проводимых экспериментов.

2. Инициализация:

- определение начальных позиций для моделирования и добавление их в список позиций 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.

3. Цикл моделирования. Обработка каждой позиции из списка позиций для моделирования (Для каждой позиции проверяются следующие после нее переходы, и для каждого перехода, связанного с рассматриваемой позицией, проверяются следующее условие, что все входящие позиции достигнуты и в каждой из позиций присутствует маркер).

Если данное условие выполняется, то все последующие позиции после перехода отмечаются как достигнутые, добавляются в текущий список для моделирования.

Если есть позиция, для которой данные условие выполняется то позиция добавляется в текущий список для моделирования.

4. Конец цикла. Возвращается список достигнутых позиций в формате позиция – количество достижений.

Известно, что точность экспериментов, проведенных с помощью метода Монте-Карло, равна выражению, определяемому по следующей формуле (2):

$$\varepsilon = \frac{1}{\sqrt{m}}, \qquad (2)$$

где m – количество проводимых экспериментов.

На основе статистики количества атак на устройства со встраиваемой операционной системой, приведенной в предыдущих разделах, за период 2023 года и первой половины 2024 года, получено, что всего за 18 месяцев было проведено примерно 225 млн атак. Произведем расчёт среднего количества атак на встраиваемые устройства в час и примем данную величину за максимальное количество атак для имитационного моделирования. Получено, что в среднем за полтора года каждый час осуществлялось 17000 кибератак на встраиваемые устройства.

Таким образом, 17000 итераций дают ошибку эксперимента равную 0,01 или 1%.

Результаты моделирования методом Монте-Карло и полученные частоты успешности атак приведены в таблице (табл. 4):

Таблица 4

Результаты моделирования множества сценариев кибератак

Частота достижения позиций наступления ущерба	**Позиции наступления ущерба (атака успешна)**						
	p34	**p35**	**p36**	**p37**	**p38**	**p39**	**p34**
	0,001071895	0,043482353	0,039761246	0,039761246	0,039761246	0,023827731	0,001071895

В ходе моделирования методом Монте Карло программа выдает приблизительно одинаковые значения по истечению некоторого количества повторений. Такое поведение модели говорит о том, что происходит стационарный процесс, поэтому для расчета вероятности реализации комплексных кибератак на сетевые технологии компьютерных систем, построенных на базе операционной системы Android, предлагается использовать стационарный поток Пуассона [18, 19] (3):

$$\mathrm{P}(\mathrm{n}, t) = \frac{(\lambda \mathrm{t})^{\mathrm{n}}}{\mathrm{n!}} \mathrm{e}^{-(\lambda \mathrm{t})}, \tag{3}$$

где: $P(n, t)$ – вероятность осуществления n успешных атак за время t;

n – количество «успехов» атаки;

λ – средне ожидаемое количество успешных атак

В силу большого числа испытаний m и сравнительно малой частоты появления события p, интенсивность λ может быть задана следующим выражением (4):

$$(\lambda t) = \mathrm{p} * \mathrm{m}\,, \tag{4}$$

где: p – частота успешной атаки, полученная в результате моделирования методом Монте-Карло.

Значения вероятностей для позиции наступления ущерба p34 «Утечка конфиденциальной информации» имеет следующий вид (рис. 7):

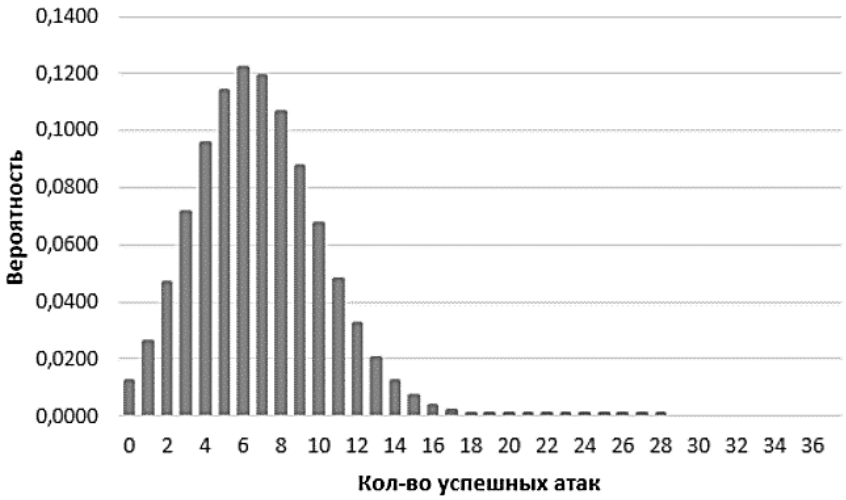

Рис. 7. Значения вероятностей для распределения Пуассона для позиции наступления ущерба p34 «Утечка конфиденциальной информации»

Аналогичные графики распределения были получены для каждой позиции наступления ущерба. Правомерность пуассоновского стационарного потока была доказана через критерий согласия Пирсона.

Таким образом, в ходе математического анализа, полученные результаты моделирования были приведены к стационарному потоку Пуассона и представлены в виде графика, показывающего зависимость между вероятностью успешности атаки и количеством успешных на сетевые технологии компьютерных систем, построенных на базе встраиваемых операционных систем.

Расчет вероятности реализации атак с учетом меняющейся интенсивности

Для расчета вероятности реализации атак на сетевые технологии устройств со встраиваемой операционной системой с меняющимся показателем интенсивности и доли успешных атак необходимо перейти к описанию нестационарного потока Пуассона. На основе статистики, приведенной выше, выполнена аппроксимация данных. Наблюдается экспоненциальный рост интенсивности. Исходный набор данных отражает количество атак в млн за год в виде последовательности: 2; 3.5; 5; 8; 12; 18; 25; 35; 50; 75; 120. Данную последовательность достаточно точно описывается по следующему закону зависимости от времени (5):

$$F(t) = 1.38 * 1.498^{t-2013} \quad (5)$$

где: $F(t)$ – количество атак за год.

Результат изменения интенсивности реализуемых кибератак на устройства со встраиваемой операционной системой приведен на рисунке (рис. 8).

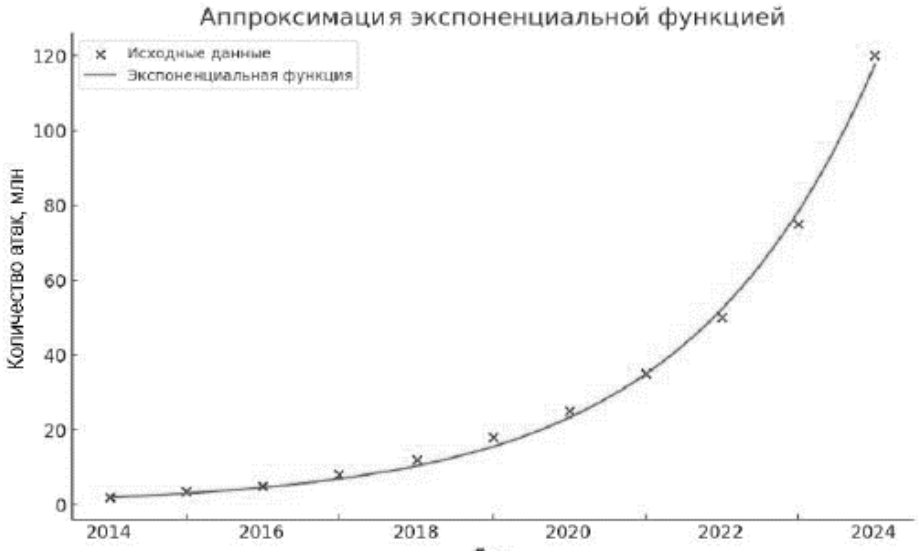

Рис. 8. Рост интенсивности кибератак

Далее был произведен расчет вероятности реализации кибератак, приводящих к позициям наступления ущерба p34-p39, из учета увеличения каждый месяц интенсивности атак на 12% и увеличения доли успешных атак на 3% за аналогичный период (рис. 9-12). Так как по результатам расчетов в предыдущем пункте было выявлено, что позиции p36-p38 достигаются с одинаковой частотой, то для них будет приведено одно графическое изображение расчётов, которые равнозначны для каждой из позиций.

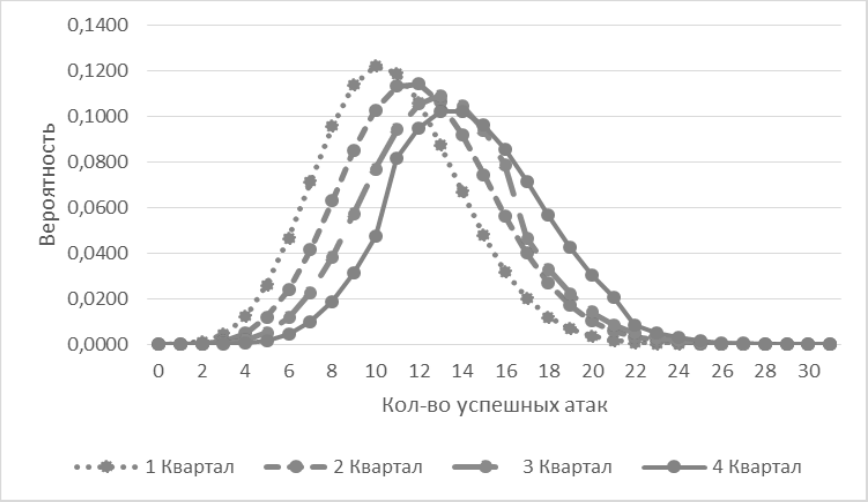

Рис. 9. Распределение вероятности наступления позиции ущерба p34 при меняющейся интенсивности кибератак

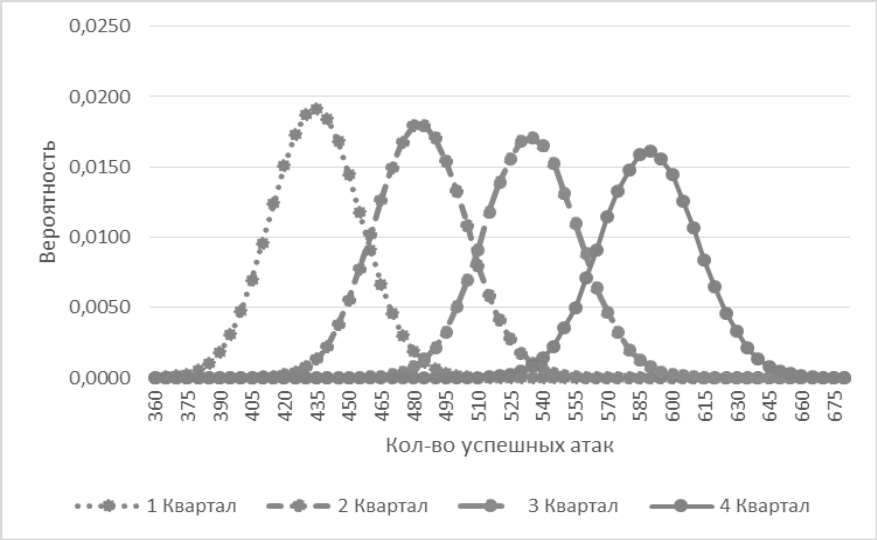

Рис. 10. Распределение вероятности наступления позиции ущерба p35 при меняющейся интенсивности кибератак

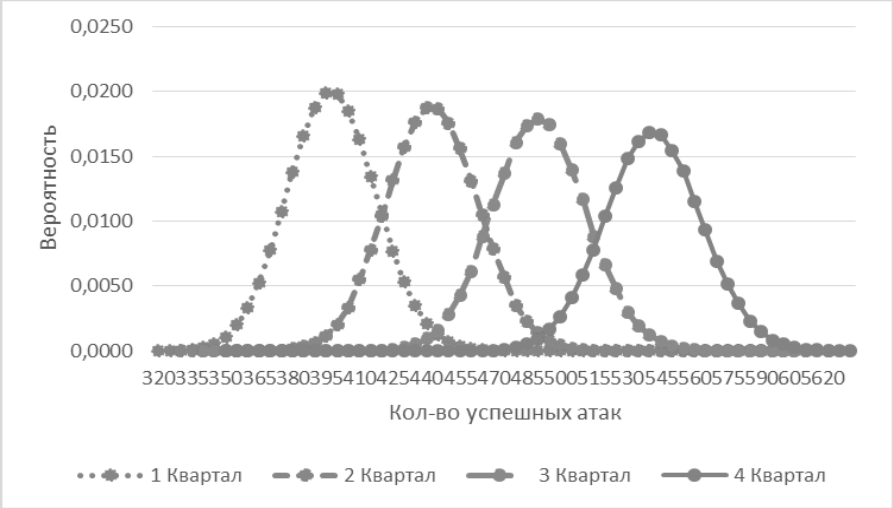

Рис. 11. Распределение вероятности наступления позиции ущерба p36-p38 при меняющейся интенсивности кибератак

Рис. 12. Распределение вероятности наступления позиции ущерба p39 при меняющейся интенсивности кибератак

Полученные распределения вероятностей позволили провести расчет рисков реализации комплексных кибератак на сетевые технологии компьютерных систем, построенных на базе встраиваемых операционных систем.

Расчет рисков реализации комплексных кибератак на сетевые технологии компьютерных систем, построенных на базе встраиваемых операционных систем

Ранее были получены все данные, необходимые для проведения риск-анализа, а именно была произведена оценка вероятности реализации атак, выраженная вероятностным приближением Пуассона, и получена величина ожидаемого ущерба.

Расчет рисков реализации кибератак направленных на сетевые технологии встраиваемых устройств с операционной системой Android будет осуществлялся по формуле (6):

$$\text{Risk} = P * \overline{\text{U}}\,, \tag{6}$$

где P – вероятность реализации кибератаки;

$\overline{\text{U}}$ – нормированный ущерб.

Ущерб будет оцениваться в количестве успешно реализованных атак. Тогда, нормировка величины наносимого ущерба будет производить по следующей формуле (7):

$$\overline{U} = \frac{n \times c}{m}, \tag{7}$$

где c – ценность ресурса;

n – количество успешно реализованных атак;

m – общее количество проведенных экспериментов.

Тогда формула риска примет следующий вид (8):

$$\overline{Risk} = \frac{P \times \overline{U}}{c}. \tag{8}$$

Расчет величины рисков реализации кибератак для позиций наступления ущерба имеет следующий вид (рис. 13-16):

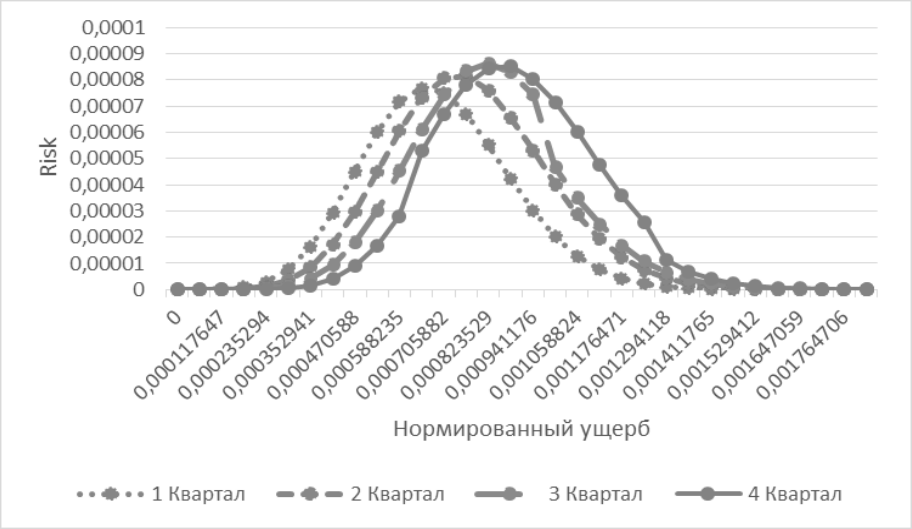

Рис. 13. Величина рисков реализации кибератак для позиции наступления ущерба p34 «Утечка конфиденциальной информации»

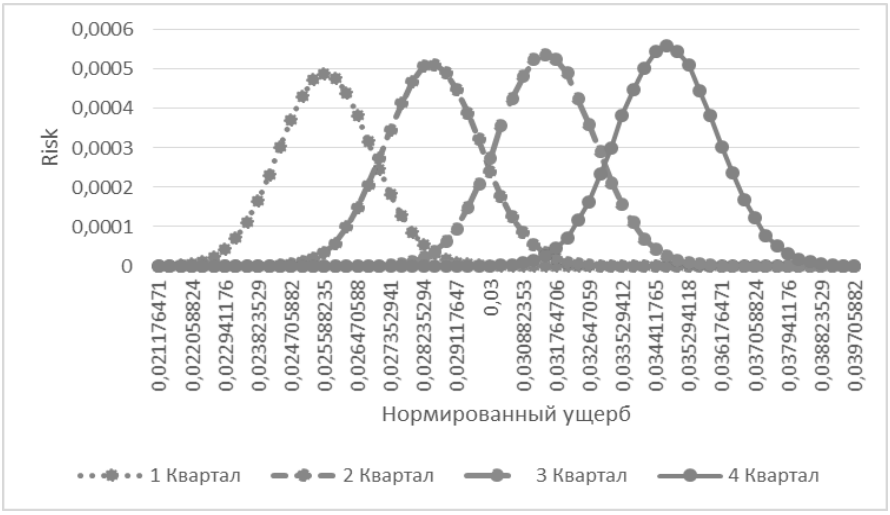

Рис. 14. Величина рисков реализации кибератак для позиции наступления ущерба p35 «Отказ в обслуживании до перезапуска устройства»

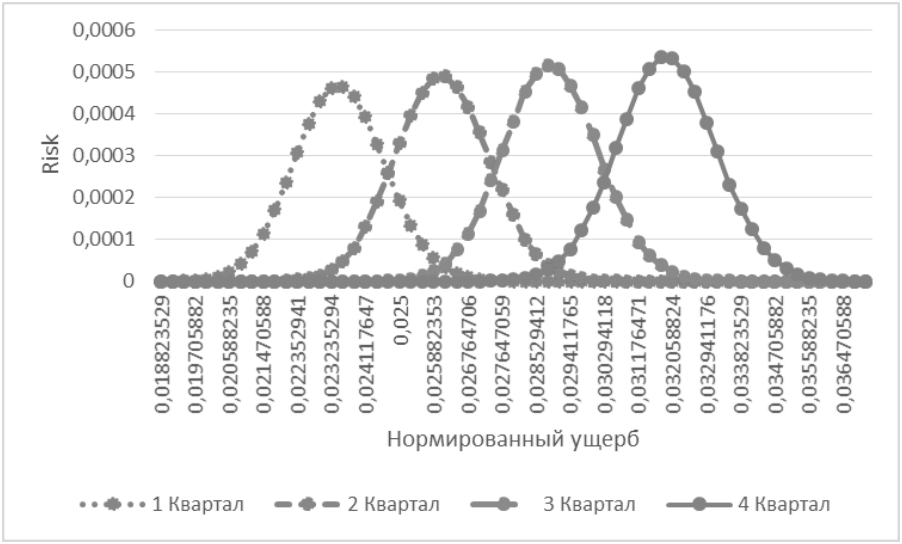

Рис. 15. Величина рисков реализации кибератак для позиции наступления ущерба p36-p38

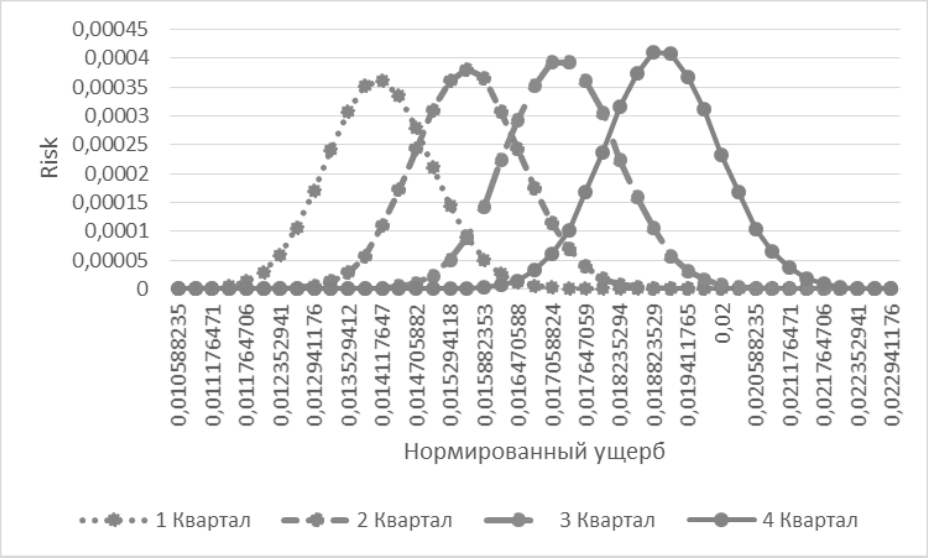

Рис. 16. Величина рисков реализации кибератак для позиции наступления ущерба p39 «Нарушение или изменение работы устройства путем повторного направления командных сообщений»

Таким образом была произведена оценка рисков реализации комплексных кибератак, направленных на сетевые технологии компьютерных систем, построенных на базе встраиваемой операционной системы Android. Построенные таблицы для каждой позиции наступления ущерба наглядно отражают величину риска наступления каждого ущерба и позволяют выявить наиболее критичные точки системы, требующие своевременного регулирования в сторону их минимизации.

Заключение

Установление взаимосвязей между моделями TID, техниками и уязвимостями позволило понять, какие уязвимости могут быть использованы в рамках различных шаблонов атак, и какие риски с этим связаны. Это способствует выявлению слабых мест системы и построению эффективных моделей защиты.

Анализ баз EMB3D, MITRE ATT&CK, NIST, БДУ ФСТЭК России и других показал их важность для систематизации информации о киберугрозах и уязвимостях, что позволяет разрабатывать более точные и обоснованные сценарии атак.

Составление сценариев атаки с использованием техник MITRE ATT&CK и построение микромоделей для их реализации обеспечивают глубокое понимание потенциальных путей атаки и помогают выявить возможные уязвимости, которые могут быть использованы злоумышленниками. Это позволяет предсказать последствия атак и более эффективно планировать защитные мероприятия.

Полученные оценки рисков успешной реализации рассматриваемого множества атак открывают перспективу их регулирования в целях повышения защищенности атакуемых объектов.

В целях регулирования могут быть предложены следующие меры регулирования полученных значений рисков: использование менеджера доступности системных служб, установление ограничений на обработку сетевых запросов, запрет использования и удаление недокументированных функций, внедрение процесса обязательной аутентификации для выполнения критически важных функций и выполнения команд от имени администратора, использование механизмов проверки физического присутствия оператора в момент выполнения команд.

Список литературы

1. Встроенная операционная система // URL:https://en.wikipedia.org/wiki/Embedded_operating_system (дата обращения: 03.02.2025).

2. Отслеживание и прогноз подключения к сотовой сети IoT (обновление за 4-й квартал 2024 года) // URL: https://iot-

analytics.com/product/cellular-iot-connectivity-tracker-forecast-q4-2024-update/ (дата обращения: 03.02.2025).

3. Отчёт SonicWall о киберугрозах за середину 2024 года // URL: https://www.sonicwall.com/blog/sonicwall-2024-mid-year-cyber- threat-report-iot-madness-powershell-problems-and-more (дата обращения: 03.02.2025).

4. Доля рынка встроенных систем | Глобальный отчет, 2023-2032 // URL: https://www.gminsights.com/ru/industry-analysis/embedded-system-market (дата обращения: 03.02.2025).

5. Обзор угроз для IoT-устройств в 2023 году // URL: https://securelist.ru/iot-threat-report-2023/108088/ (дата обращения: 03.02.2025).

6. Ежемесячное количество вредоносных атак на Интернет вещей (IoT) по всему миру // URL: https://www.statista.com/statistics/1322216/worldwide-internet-of-things-attacks/ (дата обращения: 03.02.2025).

7. MITRE EMB3D // URL: https://emb3d.mi- tre.org/ (дата обращения: 03.02.2025).

8. CWE - Common Weakness Enumeration // URL: https://cwe.mitre.org/index.html (дата обращения: 03.02.2025).

9. Сердечный А.Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT3 в распределенных компью- терных системах / А.Л. Сердечный, А.В. Айдаркин, М.А. Тарелкин, А.Е. Дешина // Информация и безопасность. 2021. Т. 24. Вып. 1. С. 35-46.

10. Сердечный А.Л. Моделирование, анализ и противодействие сценариям реализации угроз безопасности информации на корпоративные распределенные компьютерные системы / А.Л. Сердечный, А.А. Шевелюхин, М.А. Тарелкин, А.В. Бабурин // Информация и безопасность. 2021. Т. 24. Вып. 1. С. 63-72

11. Сердечный А.Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT29 в распределенных компью- терных системах / А.Л. Сердечный, П.С. Краюшкин, М.А. Тарелкин, Ю.К. Язов // Информация и безопасность. 2021. Т. 24. Вып. 1. С. 83-92

12. Сердечный А.Л. Моделирование, анализ и противодействие сценариям подготовки компьютерных атак в распределенных компьютерных системах / А.Л. Сердечный, Н.С. Пустовалов, М.А. Тарелкин, А.Е. Дешина // Информация и безопасность. 2021. Т. 24. Вып. 2. -. 193-202

13. Сердечный А.Л. Моделирование, анализ и противодействие сценариям реализации угроз безопасности информации для мобильных устройств / А.Л. Сердечный, Г.В. Сторожев, М.А. Тарелкин, А.С. Пахомова // Информация и безопасность. 2021. Т. 24. Вып. 2. С. 179-192

14. Язов Ю.К. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз безопасности информации / Ю.К. Язов, А.П. Панфилов // Вопросы кибербезопасности. 2024. Т. 60. Вып. 2. С. 53-65

15. Сети Петри и их расширения. // URL: https://studref.com/389023/ekonomika/seti_petri_rasshireniya (дата обращения: 03.02.2025).

16. Имитационное моделирование и верификация вложенных сетей Петри с использованием CPNTools // URL: https://publications.hse.ru/pubs/share/folder/fuqk08cng1/67479270.pdf. (дата обращения: 03.02.2025).

17. Метод Монте-Карло для оценки рисков в кибербезе // URL: https://habr.com/ru/articles/822719 (дата обращения: 03.02.2025).

18. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М: РадиоСофт, 2010. 232 с.

19. Очерки по математической теории систем / Рудольф Э. Калман [и др.]; [под ред. Я.З. Цыпкина]. 2-е изд., стереотипное. М.: Едиториал УРСС, 2004. 400 с.

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 5.02.25

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

Гайсина Камила Денисовна – студент, Воронежский государственный технический университет, e-mail: gaysina.kamila01@mail.ru

Покудин Данила Сергеевич – аспирант, Воронежский государственный технический университет, e-mail: danila.pokudin@inbox.ru

Юрасов Владислав Георгиевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Барапников Николай Ильич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

RISK ANALYSIS OF COMPLEX CYBER ATTACKS ON NETWORK TECHNOLOGIES OF COMPUTER SYSTEMS BASED ON EMBEDDED OPERATING SYSTEMS

A.L. Serdechnyy, **K.D. Gaysina**, **D.S. Pokudin, V.G. Yurasov, N.I. Barannikov**

The article analyzes the risks of cyber attacks on network technologies of computer systems using embedded operating systems. Modern threats to information security identified on the basis of the EMBED knowledge base are considered, with an emphasis on the vulnerability of network technologies. A statistical analysis of the increase in the number of attacks on embedded devices from 2014 to 2024, including attacks on IoT and Android devices, has been conducted. The authors have established relationships between vulnerabilities, attack techniques, and possible scenarios for their implementation. Petri-Markov networks were used to model attack scenarios, and the probability of successful attacks was estimated using the Monte Carlo method. Based on the data obtained, the risks of attacks are calculated taking into account the dynamics of their growth.

Keywords: embedded operating system, IoT, Android, EMB3D, MITRE, threats, risk, attack scenario, Monte Carlo, Petri-Markov networks.

Submitted 5.02.25

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

Камила Д. Гайсина – student, Voronezh State Technical University, e-mail: gaysina.kamila01@mail.ru

Danila S. Pokudin – graduate student, Voronezh State Technical University, e-mail: danila.pokudin@inbox.ru

Vladislav G. Yurasov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Nikolay I. Barannikov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com