DOI 10.36622/VSTU.2021.24.2.002
УДК 004.056

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

А.Л. Сердечный, Г.В. Сторожев, М.А. Тарелкин, А.С. Пахомова

В настоящей статье представлены результаты моделирования способов реализации компьютерных атак на мобильные устройства. Актуальность данной статьи обусловлена отсутствием наработок по формированию методического обеспечения, касающегося моделирования способов реализации компьютерных атак на мобильные устройства, учитывающего их специфику. Предложенные модели способов предназначены для формирования методического обеспечения расчета рисков и выявления оценки защищенности таких систем от актуальных сценариев реализации угроз безопасности информации, которое даёт возможность обоснованного выбора мер защиты. Построение моделей способов реализации компьютерных атак осуществлялось с использованием аппарата сетей Петри на основании сведений, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, определённых в базе данных ATT&CK и актуальных для мобильных устройств (условия и последствия моделируются позициями сети Петри, а сами технические приёмы – переходами сети Петри). Также в статье затрагиваются вопросы автоматизации и совместной разработки подобных моделей. Проводится сравнительный анализ различных форм представления участков моделируемой сети Петри в контексте удобства процесса её разработки

Ключевые слова: сети Петри, ATT&CK, атаки на мобильные устройства, анализ, визуализация.

Введение

За последние десятилетия распространенность мобильных устройств значительно выросла, а вместе с тем выросло и количество вредоносного программного обеспечения, направленного на заражение мобильных систем [1]. На данный момент мобильные устройства не уступают по производительности персональным компьютерам, а возможность постоянно оставаться на связи является неотъемлемой частью современной жизни общества [2-6].

Вместе с популярностью использования мобильных устройств и их внедрения в процесс служебной деятельности сотрудников организаций (вплоть до управления ключевыми бизнес-процессами) растет и количество вредоносного программного обеспечения, направленного на кражу конфиденциальной информации и нанесение ущерба пользователям мобильных устройств [7-10].

С учетом стремительного развития вредоносного программного обеспечения, динамического роста количества угроз, направленного на мобильные устройства и недостаточной защищенностью мобильных операционных систем, становится важным количественное оценивание рисков сценариев реализации угроз для обоснованного выбора мер и средств защиты [11]. Количественная оценка риска может использоваться для оценки эффективности защиты системы, а также для выбора конкретных средств защиты [12].

Формула риска выглядит следующим образом:

$$Risk(\Delta t) = P(\Delta t) \cdot U(\Delta t),$$

где P – вероятность наступления;

U – величина ущерба.

Для того чтобы выбранные меры защиты были эффективны, требуется оценка вероятностей реализации таких сценариев, а также ценности информации с учётом особенностей мобильных устройств.

Настоящая работа направлена на формирование методической основы для оценки показателя вероятности реализации

угроз компьютерных атак на мобильные устройства в распределенных компьютерных системах.

Существуют различные подходы к оцениванию вероятности реализации компьютерных атак:

– эпидемиологический подход к расчёту вероятности распространения вредоносного ПО. Недостатком данного подхода является то, что такой подход учитывает только вирусные атаки и рассматривает атаку лишь как процесс распространения вредоносного ПО между узлами, не учитывая процессы внутри узлов [12];

– подход расчёта вероятности конкретных атак, основанный на статистике по уязвимостям, связанным с такими атаками. Минус данного подхода в том, что он даёт слишком грубые оценки, не учитывает ресурсы атакующего и причинно-следственные связи между действиями злоумышленника, совершаемыми в ходе атаки [13];

– ресурсно-временной подход расчёта вероятности успешной реализации компьютерной атаки [14].

Одной из реализаций ресурсно-временного подхода является использование аппарата сетей Петри-Маркова, предполагающего построение модели причинно-следственных связей и последующее наложение вероятностно-временных характеристик [15, 16]. Данный подход и будет использован в настоящих исследованиях.

Описание методики исследования

На рис. 1 предлагается структура исследования, направленная на количественное оценивание сценариев реализации угроз безопасности для мобильных устройств в распределенной компьютерной системе.

Данную структуру можно представить в виде пирамиды, состоящей из трех уровней:

– построение модели причинно-следственных связей (сеть Петри);

– расчет вероятностно-временных показателей (сеть Петри-Маркова);

– расчет риска.

В рамках настоящей работы решается первая задача: построение сети Петри сценариев реализации угроз безопасности мобильных устройств в РКС, посредством определения причинно-следственных связей, совершаемых злоумышленниками в ходе реализации атак на мобильные устройства в распределенной компьютерной сети.

Рис. 1. Подход к анализу рисков для информационных систем, в рамках которого осуществляется моделирование сценариев реализации угроз безопасности информации (в том числе, для мобильных устройств) [17, 18, 19]

Оставшиеся задачи, позволяющие перейти от сети Петри к сети Петри-Маркова, должны быть решены в последующих работах, путем наложения на структуру сети Петри случайного процесса в виде атаки и определения его временных и вероятностных характеристик.

Переход к сети Петри-Маркова позволит не только оценивать эффективность мер защиты мобильных устройств от различных угроз, но и количественно обосновывать требования к времени реакции адаптивных систем защиты на обнаруживаемые действия, направленные на нарушение безопасности мобильных устройств, а также выявлять слабые места в системах защиты, связанные с динамикой реализации угроз и реакцией на такие угрозы систем защиты мобильных устройств.

Технология построения модели причинно-следственных связей

Технология моделирования сценариев реализации угроз безопасности информации для мобильных устройств, базирующаяся на математическом аппарате сети Петри, включает в себя три этапа:

– подготовка исходных данных;

– построение модели причинно-следственных связей реализации угроз

безопасности мобильных устройств на основе исходных данных;

– анализ полученной модели.

Этап подготовки исходных данных включает:

– поиск источника технических приемов;

– отбор технических приемов, относящихся к объекту исследования.

На этапе построения модели причинно-следственных осуществляется:

– выбор технического приема;

– выявление условий реализации технического приема;

– определение воздействия, оказываемого на атакуемый объект;

– определение последствий успешной реализации технического приема;

– определение связей с другими техническими приемами.

Анализа полученной модели проводится с целью обеспечения защиты информационной системы и включает:

– выбор анализируемого участка сети;

– концентрация внимания на связях с другими техническими приемами и воздействии на атакуемый объект;

– определение мер защиты для анализируемого участка сети.

Весь процесс моделирования можно изобразить в виде блок-схемы (рис. 2).

Подготовка исходных данных

Выбранный в настоящей работе подход к моделированию компьютерных атак на мобильные устройства предполагает наличие баз данных, в которых были бы объединены сведения о способах реализации компьютерных атак на мобильные устройства.

В настоящий момент такая база данных формируется в рамках проекта ATT&CK, ведением которого занимаются ведущие организации в области исследования и разработки средств защиты от угроз безопасности информации.

База представляет собой структурированный список известных поведений злоумышленников, разделённый на тактики и техники, выраженный в виде таблиц (матриц). Под тактикой понимается целевое действие, производимое преступником, под техникой – способ реализации этого действия [20]. Например, если сбор данных, согласно MITRE ATT&CK, – это тактика атаки, то способы сбора, такие как автоматический сбор или сбор данных со съемных носителей, – это техника.

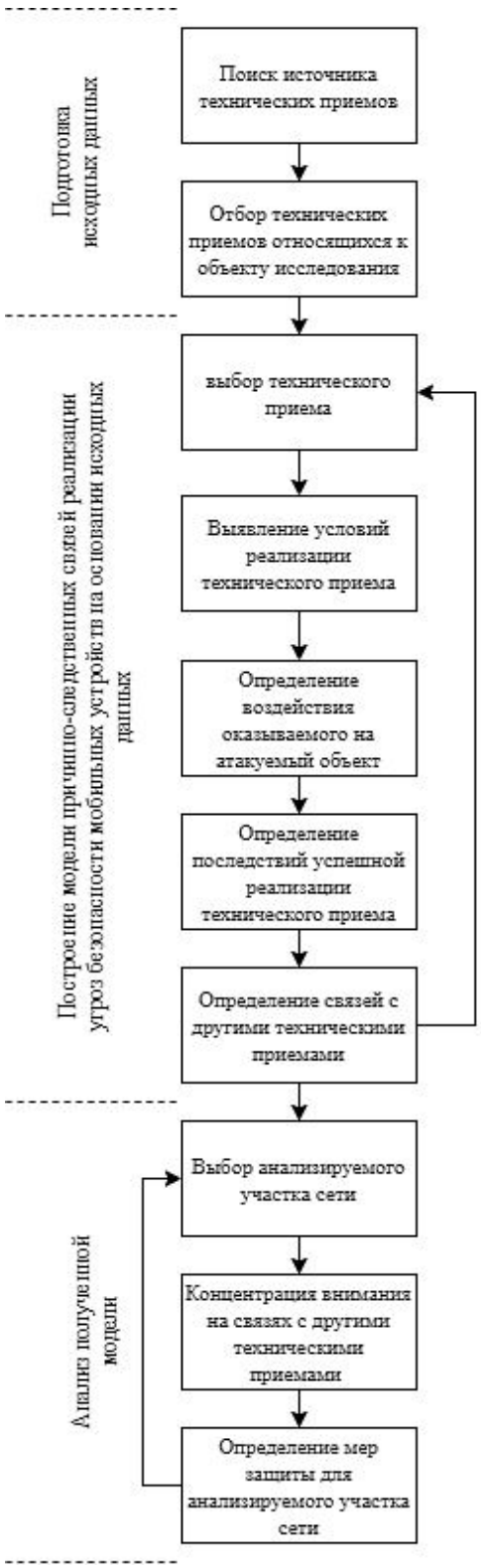

Рис. 2. Технология построения модели причинно-следственных связей

В настоящей статье термины «техника», «технический приём» и «способ реализации» используются в качестве синонимов, а под сценарием реализации компьютерной атаки понимается последовательность выполнения таких технических приёмов от момента начала атаки до нанесение злоумышленником ущерба для защищаемой информационной системе, связанного с нарушением конфиденциальности, целостности и доступности обрабатываемой в ней информации.

В данной работе используется матрица ATT&CK Mobile (рис. 3), которая охватывает технические приемы, направленные на получение доступа к устройству с целью хищения данных и/или управления мобильным устройством пользователя.

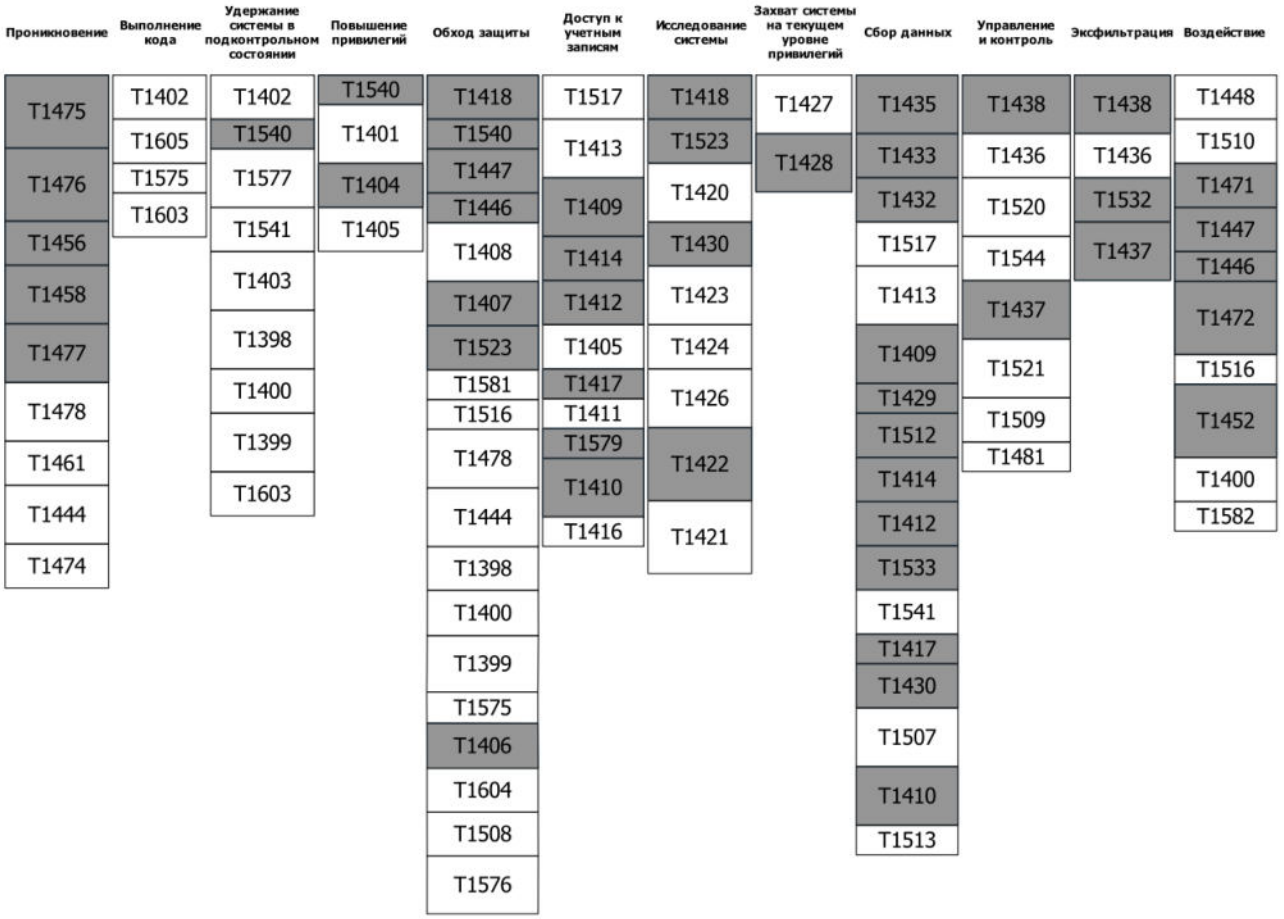

Рис. 3. Матрица ATT&CK Mobile, на которой с обозначены моделируемые техническими приёмы

Все технические приемы делятся на группы тактик. Каждая тактика представляет собой этап атаки злоумышленника на мобильное устройство. Матрица ATT&CK Mobile делит технические приемы на следующие группы тактик:

– получение первоначального доступа – представляет собой технические приемы, которые злоумышленники используют, чтобы проникнуть в мобильное устройство;

– выполнение вредоносного кода – состоит из технических приемов, которые приводят к запуску управляемого злоумышленником кода на мобильном устройстве;

– настойчивость – это технические приемы, представляющие собой действия или изменения конфигурации мобильного устройства, которые обеспечивают постоянное присутствие злоумышленника на устройстве;

– повышение привилегий – включает технические приемы, которые позволяют злоумышленнику получить более высокий уровень разрешений на мобильном устройстве;

– уклонение от защиты – состоит из приемов, которые противник может использовать для уклонения от обнаружения или уклонения от других защитных мер как на мобильном устройстве, так и в магазине приложений;

– учетный доступ – представляет собой технические приемы, которые могут использоваться злоумышленниками для получения доступа или контроля над паролями, токенами, криптографическими ключами или другими значениями, которые могут быть использованы противником для получения несанкционированного доступа к ресурсам;

– открытие – состоит из техник, которые позволяют злоумышленнику получить информацию о характеристиках мобильного устройства и, возможно, других сетевых систем;

– распространение в распределенной компьютерной сети – состоит из техник, которые позволяют злоумышленнику получить доступ к удаленным системам в сети и управлять ими;

– сбор данных – состоит из приемов, используемых для идентификации и сбора информации, такой как конфиденциальные файлы, из целевой сети до вывода их из системы (эксфильтрации). В эту категорию также входят места в системе или сети, где злоумышленник может искать информацию для проникновения;

– командование и управление – тактика, которая показывает, как злоумышленники взаимодействуют с системами, находящимися под их контролем, в целевой сети;

– утечка – состоит из техник кражи данных с мобильного устройства;

– влияние – состоит из приёмов, используемых противником для выполнения целей своей миссии, но которые не совсем подходят к другой категории, такой как «Сбор данных». Цели миссии различаются в зависимости от целей каждого злоумышленника, но примеры включают мошенничество с платными вызовами, уничтожение данных устройства или блокировку доступа пользователя к устройству до тех пор, пока не будет выплачен выкуп [21].

Для построения модели сценариев реализации угроз безопасности информации необходимо для каждого технического приема выявить условия реализации, определить масштаб воздействия на объект атаки, оценить последствия успешной реализации приема и на основании полученных данных построить связь с другими техническими приемами.

Результаты построения и анализа модели сценариев реализации угроз безопасности для мобильных устройств в распределенных компьютерных системах

В результате нахождения причинно-следственных связей между техническими приемами, представленными в базе MITRE ATT&CK, была построена модель сценариев реализации угроз безопасности для мобильных устройств в распределенных компьютерных системах, изображенная на рис. 4 и представленная следующей сетью Петри:

$$C=(P, T, I, O),$$

где P – множество позицией, моделирующих условия/последствия для действий, выполняемых злоумышленником;

T – множество переходов, моделирующих действия, выполняемые злоумышленником;

I и O – входные и выходные функции для участка сети Петри, моделирующего действия злоумышленника.

В процессе анализа полученной модели можно сделать вывод, что атаки на мобильные устройства имеют следующие особенности:

1) основным каналом распространения вредоносного ПО являются магазины приложений;

2) злоумышленникам, как правило, для достижения их целей необходимо получать разрешения у пользователя на использование какого-либо функционала устройства или требуется получить root-права.

С учетом этих особенностей необходимо формировать защитные меры, направленные на противодействие злоумышленникам.

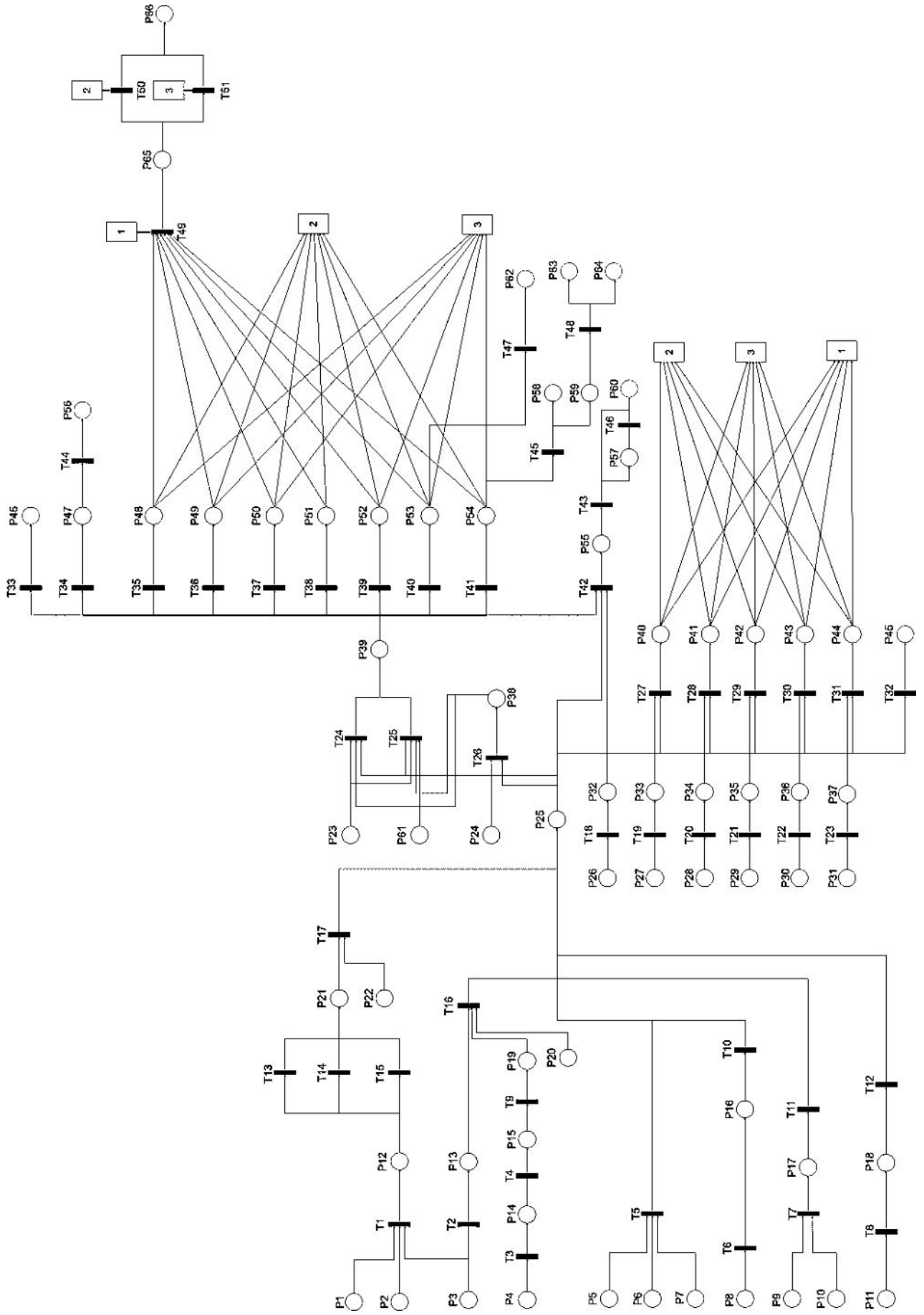

Рис. 4. Изображение модели сценариев реализации угроз безопасности для мобильных устройств в распределенных компьютерных системах

Разработка мер защиты с учетом специфики объекта исследования

Против таких массовых угроз, которые рассмотрены в настоящей работе, надо бороться на всех этапах реализации атаки и с использованием комплексного набора организационно-технических средств.

Для выработки мер противодействия были использованы данные об организационно-технических мерах защиты, которые изложены в методическом документе ФСТЭК России «Меры защиты информации в государственных информационных системах» [22].

В этом документе выделено 13 блоков мер защиты информации в информационной системе. Среди них есть блоки, которые невозможно применить в рамках исследуемых средств массовой деятельности киберпреступных группировок. К таким группам мер можно отнести меры по защите машинных носителей информации, защите технических средств, среды виртуализации, а также меры по обеспечению доступности информации.

Также можно выделить два блока, использование которых позволяет снизить угрозу применительно ко всем рассматриваемым средствам:

1) антивирусная защита;

2) регистрация событий безопасности.

Для остальных блоков требуется выбор и применение специфических мер защиты для конкретных средств с учетом их реализации.

Разработанные меры направлены на снижение вероятности успешной реализации технических приемов, применяемых злоумышленником в ходе атаки на мобильные устройства. Несмотря на то, что смягчающие меры полностью не исключает возможность проведения атак.

В качестве примера возможности моделирования мер защиты рассмотрим основные меры протводействия внедрению на мобильное устройство жертвы вредоносного программного обеспечения.

На рис. 5 показан фрагмент сети Петри для технического приёма «Распространение вредоносного приложения через официальный магазин приложений (общедоступный репозиторий)». Меры защиты обозначены фигурами с серым фоном.

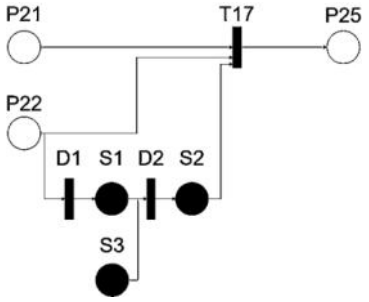

Рис. 5. Фрагмент сети Петри для технического приёма «Распространение вредоносного приложения через официальный магазин приложений (общедоступный репозиторий)»

На рис. 5 обозначены следующие позиции и переходы:

– P21 – мобильное приложение размещено в официальном магазине приложений и доступно для скачивания;

– P22 – пользователь заинтересовался мобильным приложением и хочет его скачать;

– T17 – распространение вредоносного ПО в ходе скачивания пользователем вредоносного приложения из официального магазина приложений;

– P25 – в мобильное устройство пользователя внедрено вредоносное ПО. Вредоносный код может начать выполнение;

– D1 – проверка пользователем рейтинга и отзывов заинтересовавшего приложения и других приложений разработчика;

– S1 – злоумышленнику требуется обеспечить высокий рейтинг и положительные отзывы для своего мобильного приложения, размещаемого в общедоступном репозитории;

– D2 – использование механизмов повышения популярности мобильного приложения;

– S2 – мобильное приложение злоумышленника, размещённое в общедоступном репозитории, имеет высокий рейтинг и положительные отзывы;

– S3 – злоумышленник распространяет мобильное приложение используя личный сертификат разработчика.

Моделируемая мера заключается в использовании официальных репозиториев для скачивания мобильных приложений,

подписанных сертификатом разработчика. Введение данной процедуры требует от злоумышленника дополнительных действий, связанных с необходимостью обеспечения высокого рейтинга своего мобильного приложения, положительных отзывов, а также наличие валидного сертификата разработчика, который может быть отозван владельцем репозитория в случае подтверждения факта недобросовестного использования услуг по размещению приложения в официальном магазине.

На рис. 6 представлен участок сети Петри, модулирующей реализацию технического приема распространения вредоносного ПО через веб-сайты.

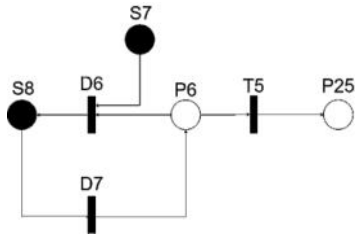

Рис. 6. Фрагмент сети Петри. Распространение вредоносного ПО через веб-сайты

На рис. 6 обозначены следующие позиции и переходы:

– P6 – браузер пользователя имеет известные уязвимости или установленные плагины в браузере пользователя имеют известные уязвимости;

– T5 – распространение вредоносного ПО через веб-сайты;

– S7 – пользователь проводит регулярные обновления системы;

– D6 – обновление системы;

– S8 – обновление устранило уязвимость;

– D7 – злоумышленник ищет новые уязвимости.

– P25 – в мобильное устройство пользователя внедрено вредоносное ПО. Вредоносный код может начать выполнение.

Смягчающие меры предусматривают регулярное выполнение процедуры обновления операционной системы и приложений. С каждым обновлением разработчики устраняют выявленные уязвимости, что усложняет возможность использования уязвимостей, таких как уязвимости в браузере пользователя.

На рис. 7 представлен участок применения технического приема распространение вредоносного ПО через USB-подключение к зараженному ПК (станции).

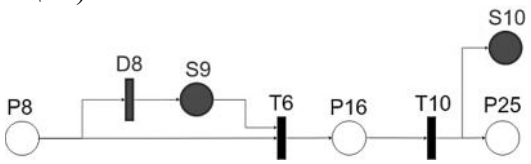

Рис. 7. Фрагмент сети Петри. Распространение вредоносного ПО через USB-подключение к зараженному ПК (станции)

На рис. 7 обозначены следующие позиции и переходы:

– P8 – пользователю требуется зарядное устройство или доступ к ПК;

– T6 – пользователь подключается к зараженной зарядной станции или ПК;

– P16 – пользователь подключен к зараженному ПК или зарядной станции через USB-соединение;

– T10 – распространение вредоносного ПО через USB-подключение к зараженному ПК (станции);

– P25 – в мобильное устройство пользователя внедрено вредоносное ПО. Вредоносный код может начать выполнение.

– D8 – отключение возможности доступа к данным и их передачи через USB-порт устройства при использовании не доверенной зарядной станции или ПК;

– S9 – в системе отключена возможность передачи файлов, USB-соединение используется для зарядки;

– S10 – распространение обернулось неудачей, мобильное устройство находится в безопасности.

Смягчающие меры предусматривают отключение возможности передачи файлов при подключении к потенциально опасным источникам. Данная функциональная возможность доступна для операционных систем iOS и Android, выпускаемых после 2018 года.

Направление дальнейших исследований

В рамках настоящей работы решалась задача построения сети Петри сценариев реализации угроз безопасности мобильных устройств, посредством определения причинно-следственных связей, совершаемых злоумышленниками в ходе реализации атак на мобильные устройства в распределенной компьютерной сети.

Оставшиеся задачи, позволяющие перейти от сети Петри к сети Петри-Маркова, будут решены в последующих работах, путем наложения на структуру сети Петри случайного процесса в виде атаки и определения временных и вероятностных характеристик.

Переход к сети Петри-Маркова позволит не только оценивать эффективность мер защиты мобильных устройств от различных угроз, но и количественно обосновывать требования к времени реакции адаптивных систем защиты на обнаруживаемые действия, направленные на нарушение безопасности мобильных устройств [23].

При этом необходимо отметить, что учёт вероятностно-временных характеристик моделируемых процессов (переход от сети Петри к сети Петри-Маркова), а также расширение предложенной модели на другие объекты и способы реализации компьютерных атак с продемонстрированным уровнем детализации потребуют использование систем автоматизированного моделирования на базе картографических методов с поддержкой возможности совместного картографирования. Без подобных систем невозможно своевременно и качественно осуществлять разработку достаточно больших и точных моделей, так как системы, реалузиующие картографические методы анализа предоставляют исследователям возможность согласованной работы в рамках единой модели и унифицированных обозначений. Визуализация модели в виде информационных карт предоставляет интуитивно понятный язык, позволяющий компактной расположить множество фактов, имеющих отношение к моделируемой области без необходимости переключения внимания исследователей вследствие использования разрозненных источников.

При таком подходе важное значение имеет способ отображения элементов модели. Одним из распространённых на сегодняшний день форм визуализации технических приёмов является матрицы, такие как ATT&CK Mobile (рис. 3). Для интерактивной работы с ними разрабатываются различные инструменты, такие как ATT&CK Navigator. Подобные средства предоставляют единое пространство для анализа способов и сценариев реализации компьютерных атак.

Наиболее часто матрицы используются для исследования шаблонов поведения киберпреступных группировок. Для этого каждый технический приём связывается с помощью направленных линий в соответствии с последовательностью его реализации в рамках атаки на РКС. Также матрицы ATT&CK позволяют оценить покрытие мер защиты, противодействующих реализации компьютерным атакам.

При этом матрицы технических приёмов не позволяют наглядно передать информацию о сложных сценариях компьютерных атак, охватывающих более 20 технических приёмов. Проиллюстрируем данный тезис на примере изображения причинно-следственные связи между техническими приёмами, рассмотренными в настоящей работе.

Технические приёмы считаются связанными, если связаны соответствующие им переходы сети Петри (рис. 8).

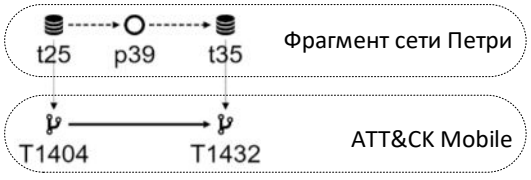

Рис. 8. Пример связи между техническими приёмами T1404 и T1432, определённой на основе причинно-следственных связей элементов построенной модели

На рис. 8 следующие обозначения.

Элементы модели:

t25 – «Использование уязвимостей ОС для повышения привилегий»,

p39 – «Получен root-доступ к устройству»,

t35 – «Осуществление доступа к журналу вызовов и списку контактов».

Технические приемы:

T1404 – «Использование уязвимости ОС»,

T1432 – «Доступ к списку контактов».

Для изображения таких связей использованы следующие способы:

– матрица ATT&CK Mobile (рис. 9);

– граф связей технических приёмов, уложенный с помощью силового алгоритма (рис. 10);

– граф связей технических приёмов, уложенный с помощью алгоритма укладки направленных деревьев (рис. 11).

Для первого способа отношения между техническими приёмами выглядят запутанно из-за неупорядоченного расположения большого количества пересекающихся линий, связывающих технические приёмы, что обусловлено нелинейностью порядка реализации этапов атаки. В реальных компьютерных атаках такие этапы как «Обход защиты», «Исследование системы», «Повышение привилегий» могут выполняться несколько раз для разных объектов.

В способах 2 и 3 данный недостаток устранён. Алгоритм силовой укладки более выгоден для определения наиболее взаимосвязанных техники и их соотношения в рамках различных этапов.

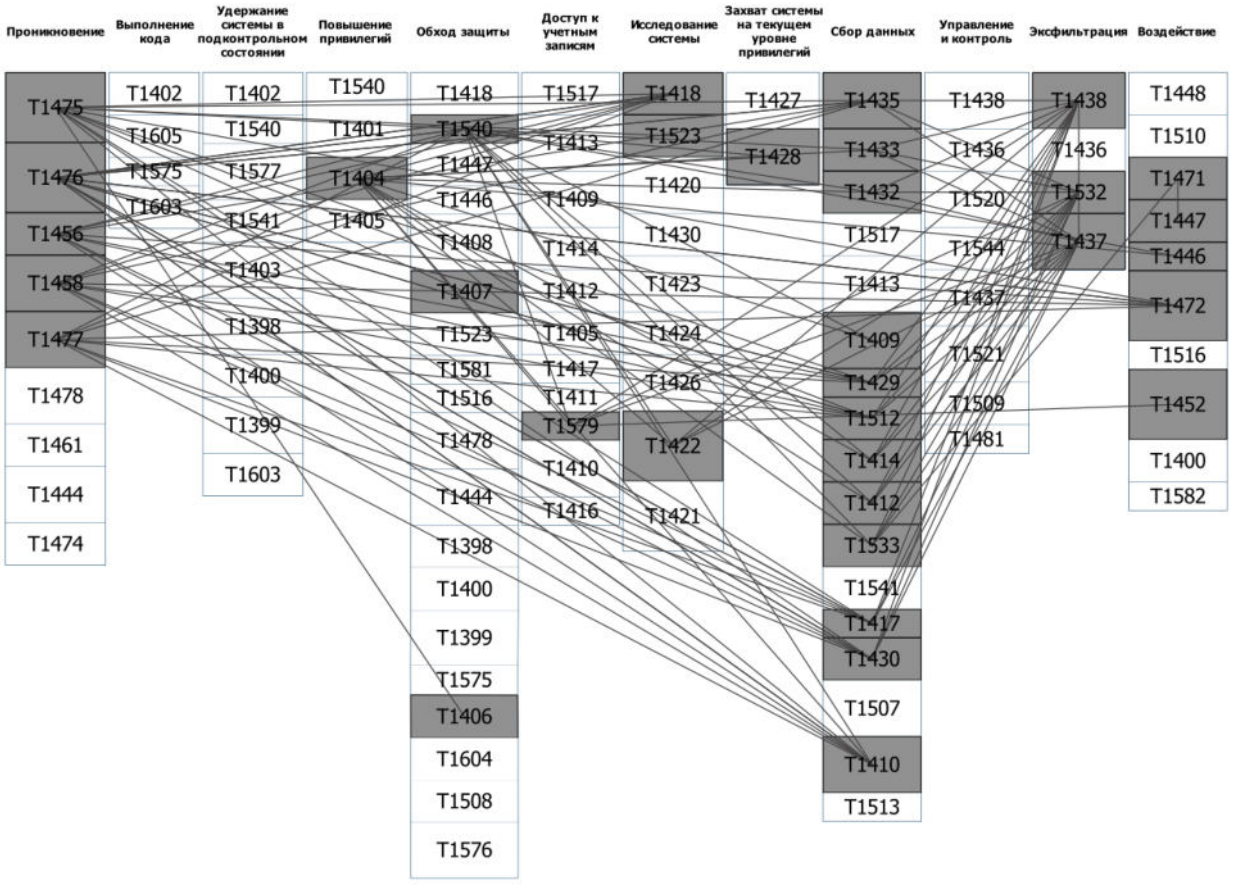

Рис. 9. Связи между техническими приёмами, изображённые с помощью матрицы ATT&CK Mobile

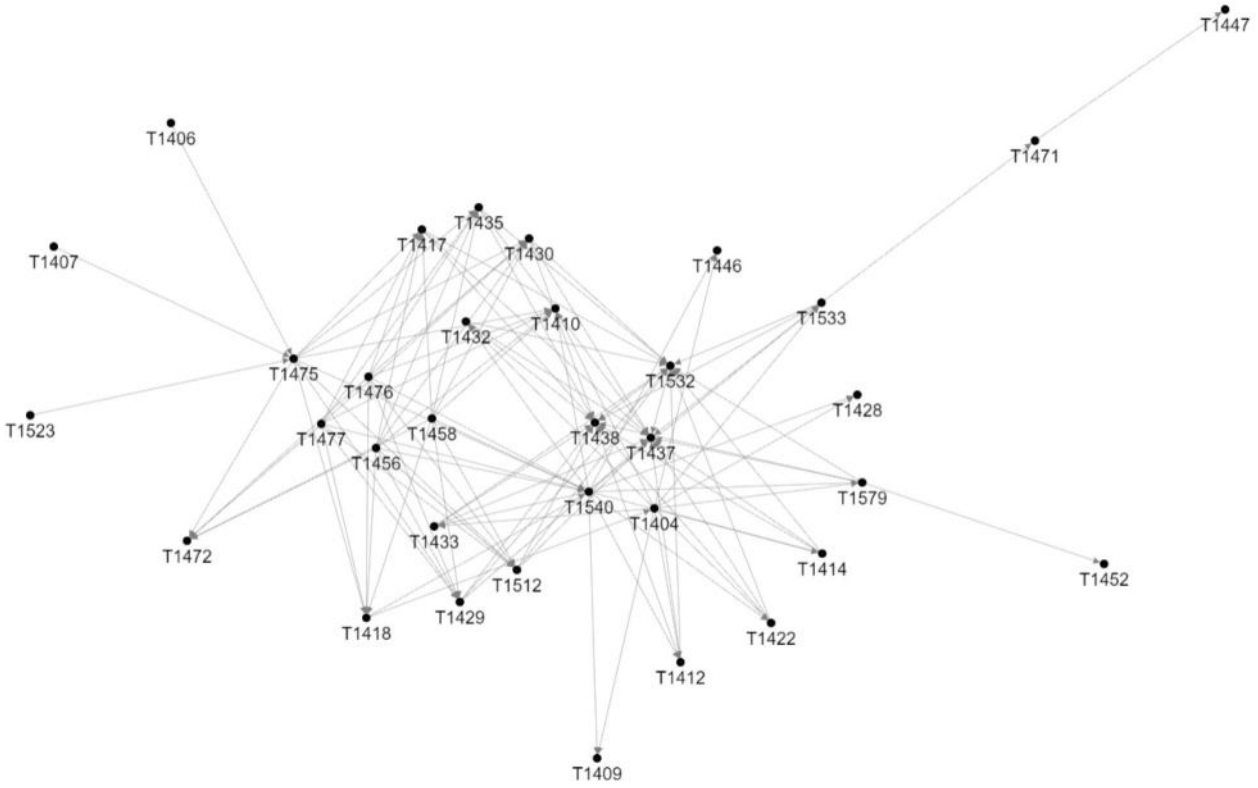

Рис. 10. Связи между техническими приёмами, изображённые с помощью алгоритма силовой укладки ForceAtlas

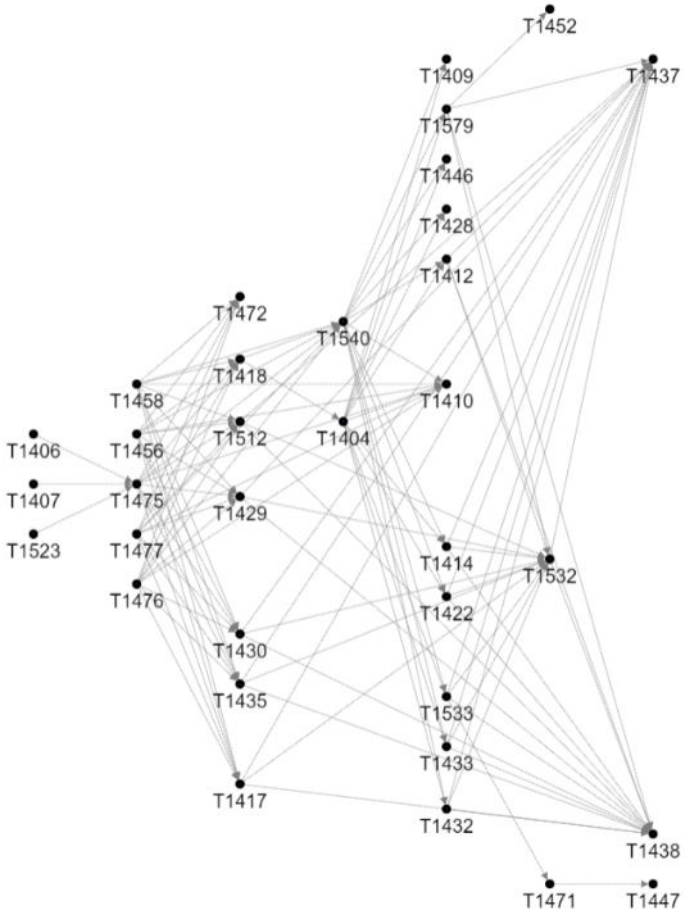

Рис. 11. Связи между техническими приёмами, изображённые с помощью алгоритма укладки направленных деревьев

При этом во втором способе не учитываются направления связей, что затрудняет расположение технических приёмов в соответствии с этапами развития атаки. Укладка графа с помощью деревьев позволяет учесть причинно-следственные связи и выстроить способы в цепочку в соответствии с порядком их реализации в реальной атаке.

Рассмотренные способы отображения реализованы в автоматизированной системе моделирования сценариев реализации компьютерных атак, являющейся частью системы картографирования рисков защищаемого киберпространства, разрабатываемой на кафедре «Системы информационной безопасности» Воронежского государственного технического университета [24].

Заключение

Таким образом, в работы были представлены результаты моделирования способов реализации компьютерных атак на мобильные устройства. Были рассмотрены:

– 5 способов получения доступа к мобильному устройству;

– способ удержания мобильного устройства в подконтрольном состоянии;

– 2 способа повышения привилегий на мобильном устройстве;

– 7 способов обхода защиты мобильного устройства;

– 6 способов доступа к учетным записям мобильного устройства;

– 4 способа исследования мобильного устройства;

– способ захвата системы на текущем уровне привилегий;

– 11 способов, реализуемых на этапе сбора данных;

– 2 способа управления и контроля мобильного устройства;

– 3 способа вывода собранной информации из мобильного устройства;

– 5 способов негативных воздействий на мобильное устройство.

Разработанная модель расширена за счёт включения в неё моделей мер защиты от рассмотренных способов. Все это позволило создать основу количественного оценивания рисков для сценариев реализации угроз безопасности информации для мобильных устройств с использованием моделей на основе аппарата сетей Петри-Маркова. Расширение построенных моделей на базе сети Петри до моделей на базе сети Петри-Марков за счёт определения вероятностно-временных показателей для участков сетей на основании обоснованных методик и доступной статистики является основным направлением дальнейших исследований.

Также в настоящей работе затронут вопрос автоматизации, без которой невозможно расширение и поддержание в актуальном состоянии подобных моделей.

Список литературы

1. T-Mobile Электрон. дан. URL: www.t-mobile.com/hotspot/ (дата обращения 18.04.2021).

2. Статистика популярности мобильных операционных систем Электрон. дан. URL: https://woxapp.com/ru/our-blog/statistics-of-the-popularity-of-mobile-operating-systems/ (дата обращения 18.04.2021).

3. Информационный портал по безопасности SecurityLab.ru. Мобильные угрозы и методы борьбы с ними. Электрон. дан. URL: https://www.securitylab.ru/analytics/501302.php/ (дата обращения 18.04.2021).

4. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements – Электрон. дан. – URL: https://www.iso.org/standard/54534.html/ (дата обращения 18.04.2021).

5. Якушин Петр. Безопасность мобильного предприятия / П.Якушин // Открытые системы – 2013. – № 1 (187). – С. 22–27.

6. Интернет-издание, где МегаФон рассказывает о том, как технологии меняют бизнес. Разновидности актуальных мобильных угроз. – Электрон. дан. – URL: https://update.megafon.ru/post/mobile-threats/ (дата обращения 18.04.2021).

7. Петраков А.В. Основы практической защиты информации: учеб. пособ. / А.В. Петраков. – М., 2005. – 281 с.

8. Cyber Security Report. Отчет кибербезопасности Check Point за 2020 год. / Информационный портал по безопасности Cyber Security Report. – Электрон. дан. – URL:

https://pages.checkpoint.com/cyber-security-report-2020.html/ (дата обращения 18.04.2021).

9. В. Безмалый. Безопасность мобильных устройств / В. Безмалый // Windows IT Pro/re, № 1 / 2014. – С. 5–6.

10. Официальный сайт компании «Лаборатория Касперского». – Электрон. дан. – URL: https://www.kaspersky.ru/ resource-center/threats/mobile/ (дата обращения 18.04.2021).

11. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях / Ю.К. Язов // Ростов-на-Дону: СКНЦ ВШ, 2006. – С. 8–9.

12. Остапенко А.Г. Эпидемии в телекоммуникационных сетях / А.Г. Остапенко // Информация и безопасность. – 2019. – С. 3–4.

13. Risk Assessment Method for Cyber Security of Cyber Physical Systems. – Электрон. дан. – URL: https://sci-hub.do/10.1109/ICRSE.2015.7366430/ (дата обращения 18.04.2021).

14. Калашников А.О. Модели количественного оценивания компьютерных атак. Часть 2 / А.О. Калашников, К.А. Бугайский, Е.В. Аникина // Информация и безопасность. – 2019. – Т. 4. – С. 34–37.

15. Ю.К. Язов, О.С. Авсеньтев, А.О. Авсеньтев, И.О. Рубцова. Метода оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри — Маркова / Ю.К. Язов // SPIIRAS Proceedings. 2019. – №6 – С. 5–8.

16. Язов Ю.К. Анищенко А.В., Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография. // Воронеж: Кварта – 2020. – С. 128 – 151.

17. 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.1 С. 63-72.

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

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

20. Alberts C., Dorofee A. Managing Information Security Risks / C. Alberts, A. Dorofee // The OCTAVE Approach. Addison Wesley Professional. – 2002. – PP. 78–84.

21. MITRE ATT&CK. – Электрон. дан. – URL: https://attack.mitre.org/. (дата обращения 18.04.2021).

22. Меры защиты информации в государственных информационных системах. Методический документ. URL: https://fstec.ru/component/attachments/download/675 (дата обращения 18.04.2021).

23. Lye K., Wing J. Game Strategies in Network Security / Lye K., Wing J. // International Journal of Information Security, February, 2005. – PP. 44–48.

24. Сердечный А.Л. Система картографирования рисков защищаемого киберпространства / А.Л. Сердечный, В.С. Сидельникова, А.А. Петелин и др. // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем. 2020. Т. 18. № 1. С. 32-45.

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 20.04.2021

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: alex-voronezh@mail.ru

Сторожев Глеб Валерьевич – студент, Воронежский государственный технический университет, e-mail: g_storozhev@list.ru

Тарелкин Михаил Андреевич – научный сотрудник, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: mihail.tarelkin.93@mail.ru

Пахомова Анна Степановна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: apal12@mail.ru

A.L. Serdechnyy, G.V. Storozhev, M.A. Tarelkin, A.S. Pahomova

MODELING, ANALYSIS, AND COUNTERACTION MEASURES FOR IMPLEMENTATION SCENARIOS OF INFORMATION SECURITY THREATS ON MOBILE DEVICES

This article presents the results of modeling methods for implementing computer attacks on mobile devices. The relevance of this article is due to the lack of developments in the formation of methodological support for modeling methods for implementing computer attacks on mobile devices, taking into account their specifics. These models are intended for the formation of methodological support for calculating risks and identifying the assessment of the security of such systems from current scenarios of information security threats, which makes it possible to make an informed choice of security measures. The construction of models of ways to implement computer attacks was carried out using the device of Petri nets based on the information contained in the MITRE ATT&CK database. These models are interconnected by the conditions and consequences of the implementation of the main techniques defined in the ATT&CK database and relevant for mobile devices (conditions and consequences are modeled by the positions of the Petri net, and the techniques themselves are modeled by the transitions of the Petri net). In article also addresses the issues of automation and joint development of such models. A comparative analysis of various forms of representation of the sections of the simulated Petri net in the context of the convenience of its development process is carried out.

Keywords: Petri nets, ATT&CK, attacks on mobile devices, analysis, visualization.

Submitted 20.04.2021

Information about the authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

Gleb V. Storozhev – Student, Voronezh State Technical University, email: g_storozhev @mail.ru

Mihail A. Tarelkin – Scientific researcher, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: mihail.tarelkin.93@mail.ru

Anna S. Pahomova – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: apal12@mail.ru