**DOI 10.36622/VSTU.2021.24.1.008**
**УДК 004.056.53:004.735**

# 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**

Статья посвящена моделированию компьютерных атак на распределённые корпоративные компьютерные системы, на примере действий группировки Advanced Persistent Threat 29 (APT29). В статье предлагается подход моделирования способов, реализуемых указанной группировкой, а также мер защиты от них. Подход основан на использовании аппарата сетей Петри, а также сведений о технических приёмах, предоставляемых в рамках проекта MITRE ATT&CK. Разработанные модели учитывают связи по условиям и последствиям действий, совершаемых группировкой APT29 в ходе атак на распределённые корпоративные системы. Также в статье продемонстрирована возможность наращивания модели за счёт включения в неё моделей мер защиты от рассмотренных способов реализации компьютерных атак. Предлагаемые модели могут быть дополнены за счёт моделирования новых способов реализации компьютерных атак, используемых другими кибергруппировками. Кроме того, модели могут быть расширены до моделей сети Петри-Маркова путём реализации частным методик расчёта вероятностно-временных характеристик для фрагментов предлагаемых моделей.

Ключевые слова: киберпреступные группировки, APT-атаки, сети Петри, ATT&CK, APT 29, распределенные компьютерные системы.

## Введение

Актуальность моделирования сценариев реализации угроз безопасности информации от атак кибергруппировки APT29 на распределенные компьютерные системы, обусловлена постоянным ростом количества таких атак и величиной ущерба для атакуемых организаций. Моделирование атаки позволяет выявить ключевые моменты характерные для кибергруппировки APT29 во время совершения несанкционированных действий. На основе анализа характерных особенностей начать разработку мер для выстраивания системы защиты информации [1-8].

Для эффективного выбора мер защиты необходима оценка вероятности реализации успешных атак кибергруппировки APT29, а также ценности информации с учетом особенностей распределенной компьютерной системы организации подверженной подобным атакам. Настоящая работа направлена на формирование методической основы для оценки показателей вероятности реализации угроз компьютерных атак кибергруппировки APT29 в распределенных компьютерных системах. Расчет ущерба выходит за рамки настоящей работы.

Одним из множества подходов является использование аппарата сетей Петри-Маркова, предполагающее использование сети как математического объекта для моделирования динамических дискретных систем.

Для его реализации требуется:

– определить причинно-следственные связи между действиями, совершаемыми нарушителем в ходе реализации атаки (построение сети Петри);

– определить вероятностно-временные характеристики участков такой модели (построение сети Петри-Маркова);

– рассчитать вероятности достижения определённых позиций сети Петри (связанных с нанесением ущерба информационной системе) за заданное время.

Реализация данного подхода предполагает наличие достаточно полных баз данных, в которых были бы объединены сведения о способах реализации компьютерных атак. 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 данных ATT&CK содержит описания сотен технических приёмов, используемых нарушителями в ходе проведения компьютерных атак. Способы разбиты на несколько групп, соответствующих различным этапам реализации компьютерных атак.

База ATT&CK не содержит сведений о причинно-следственных связях между способами необходимыми для построения цепочки атаки, реализуемой кибергруппировкой APT29 на распределенные компьютерные системы.

Для реализации представленного подхода в первую очередь требуется формирование модели причинно-следственных связей между способами реализации компьютерных атак, которые можно будет соединить в одно целое и получить маршрут атаки.

В рамках настоящей работы осуществляется моделирование атаки кибергруппировки APT29 на распределенные компьютерные системы.

**Технология моделирования**

С момента повсеместного распространения всемирной сети в ней находится огромное количество баз данных, социальных сетей, веб-сайтов и т.п.

Вся информация, которая находится на этих ресурсах, является основой большинства атак. Нарушители перед началом своего нападения тщательно изучают целевого пользователя по открытым источникам, собирая всевозможную информацию. Все эти действия нацелены на изучение пользователя и дальнейшее формирования фишингового сообщения, отправки его в надежде, что пользователь откроет его и перейдет по ссылке в письме, внедрив вредоносный код в систему. Это один из способов внедрения вредоносного ПО в систему.

Для лучшего понимания действий нарушителя, необходимо провести моделирование сценария его атаки на распределенные компьютерные системы. В качестве базисных данных будут использованы технические приемы, представленные в ATT&CK. Начинается все с необходимости проанализировать и отобрать техники, используемые кибергруппировкой APT29 для своей атаки. В качестве математического объекта будет использована сеть Петри. В свою очередь для лучшего понимания и анализа сеть Петри будет разбита на четыре фазы, а каждая фаза в свою очередь на несколько шагов.

Сведения о технических приемах (способах реализации компьютерной атаки) получены из информационного ресурса MITRE ATT&CK (рис. 1) [9]. Отобрав техники и изучив их, находим причинно-следственную связь и строим сеть Петри для сценария атаки.

Технология моделирования сценария, реализуемого группировкой APT29, заключалась в выполнении следующих действий:

– из описанных в базе данных MITRE ATT&CK [4] приемов были выбраны технические приёмы, используемые группировкой APT29 в ходе реализации сценария атаки [5, 6];

– проведён анализ описания каждого выбранного технического приёма с целью определения следующих сведений:

а) условий реализации технического приёма;
б) действий, которые оказывает прием на атакуемую систему;
в) последствий успешной реализации технического приема.

– для каждого технического приёма определялась его взаимосвязь с другими приёмами на основании полученных сведений об условиях и последствиях;

– осуществлялось построение модели с использованием аппарата сетей Петри.

| Privilege Escalation<br>21 items | Defense Evasion<br>57 items | Credential Access<br>16 items | Discovery<br>22 items | Lateral Movement<br>15 items | Collection<br>13 items |
|---|---|---|---|---|---|
| Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | Application Deployment Software | Audio Capture |
| Accessibility Features | Binary Padding | Brute Force | Application Window Discovery | Distributed Component Object Model | Automated Collection |
| AppCert DLLs | BITS Jobs | Credential Dumping | Browser Bookmark Discovery | Exploitation of Remote Services | Clipboard Data |
| AppInit DLLs | Bypass User Account Control | Credentials in Files | Domain Trust Discovery | Logon Scripts | Data from Information Repositories |
| Application Shimming | CMSTP | Credentials in Registry | File and Directory Discovery | Pass the Hash | Data from Local System |
| Bypass User Account Control | Code Signing | Exploitation for Credential Access | Network Service Scanning | Pass the Ticket | Data from Network Shared Drive |
| DLL Search Order Hijacking | Compile After Delivery | Forced Authentication | Network Share Discovery | Remote Desktop Protocol | Data from Removable Media |
| Exploitation for Privilege Escalation | Compiled HTML File | Hooking | Network Sniffing | Remote File Copy | Data Staged |
| Extra Window Memory Injection | Component Firmware | Input Capture | Password Policy Discovery | Remote Services | Email Collection |
| File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Peripheral Device Discovery | Replication Through Removable Media | Input Capture |
| Hooking | Control Panel Items | Kerberoasting | Permission Groups Discovery | Shared Webroot | Man in the Browser |
| Image File Execution Options Injection | DCShadow | LLMNR/NBT-NS Poisoning and Relay | Process Discovery | Taint Shared Content | Screen Capture |
| New Service | Deobfuscate/Decode Files or Information | Network Sniffing | Query Registry | Third-party Software | Video Capture |
| Path Interception | Disabling Security Tools | Password Filter DLL | Remote System Discovery | Windows Admin Shares | |
| Port Monitors | DLL Search Order Hijacking | Private Keys | Security Software Discovery | Windows Remote Management | |
| Process Injection | DLL Side-Loading | Two-Factor Authentication Interception | System Information Discovery | | |
| Scheduled Task | Execution Guardrails | | System Network Configuration Discovery | | |
| Service Registry Permissions Weakness | Exploitation for Defense Evasion | | System Network Connections Discovery | | |
| SID-History Injection | Extra Window Memory Injection | | System Owner/User Discovery | | |
| Valid Accounts | File Deletion | | System Service Discovery | | |

Рис. 1. Фрагмент матрицы MITRE ATT&CK, на которой серым фоном отмечены основные технические приёмы, использованные группировкой APT29

Общая модель действий APT29 выглядит следующим образом. Осуществив первоначальное проникновение в систему, злоумышленник осуществляет сбор предварительных сведений об объекте атаки и передаёт их на командный сервер, с которого получает дополнительные модули. Далее, с помощью полученных модулей, злоумышленник повышает свои привилегии и закрепляется в системе, после чего осуществляет более глубокий поиск как информации о системе, так и её пользователей. При получении доступа к учётным записям пользователей у злоумышленника появляется возможность сбора информации ограниченного доступа. Все собранные сведения нарушитель архивирует и отправляет на командный сервер с использованием нестандартного протокола взаимодействия.

На каждом этапе атаки злоумышленник зачищает свои следы.

В результате реализации технологии, описанной в настоящей работе, разработана модель проведения компьютерных атак кибергруппировки APT29 в распределенной компьютерной системе, представляющая собой сеть Петри (рис. 2):

$$C=(P, T, I, O), \quad (1)$$

где P – множество позицией, моделирующих условия/последствия для действий, выполняемых группировкой APT29;

T – множество переходов, моделирующих действия, выполняемые группировкой APT29;

I и O – входные и выходные функции для участка сети Петри, моделирующего действия группировки APT29.

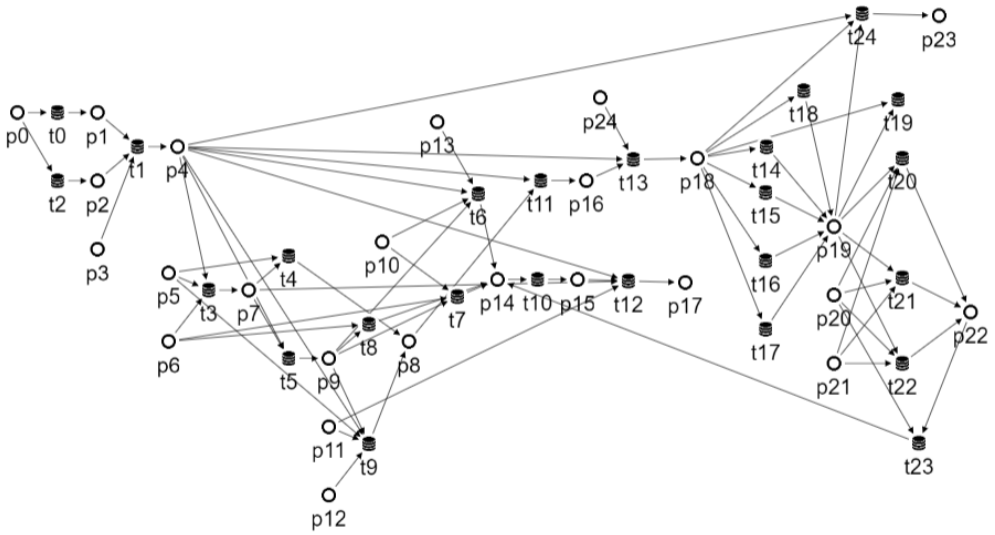


Рис. 2. Сеть Петри, моделирующая сценарий атаки, реализованный группировкой APT29

На рис. 2 обозначают следующее позиции и переходы:

- p0 – Злоумышленник начал атаку;
- p1 – Пользователь получил письмо от злоумышленника, содержащее исполняемый файл;
- p2 – Пользователь мотивирован на запуск исполняемого файла;
- p3 – Пользователь открыл файл;
- p4 – Имеется возможность выполнения вредоносного кода;
- p5 – Имеется возможность доступа к командному серверу злоумышленника;
- p6 – Имеются привилегии доступа к системным вызовам Windows;
- p7 – Установлено сетевое соединение с командным сервером злоумышленника;
- p8 – Получены файлы с командного сервера злоумышленника;
- p9 – Сформированы команды на поиск файлов в локальной файловой системе, а так команды для взаимодействия с командным сервером с целью загрузки дополнительных модулей;
- p10 – Определён перечень файлов, необходимых злоумышленнику;
- p11 – Доступен командный сервер злоумышленника;
- p12 – Подана команда на загрузку вредоносного файла;
- p13 – Наличие привилегий для доступа к файлам;
- p14 – Получен доступ к нужным сведениям;
- p15 – Созданный файл готов к передаче;
- p16 – Обойдён механизм защиты UAC;
- p17 – Злоумышленник передал файлы на удаленный сервер;
- p18 – Имеется возможность выполнения вредоносного кода с полномочиями привилегированного пользователя;
- p19 – Получена информация о системе;
- p20 – Злоумышленнику требуются привилегии доступа к файлам пользователя;
- p21 – Злоумышленник получает постоянный доступ в систему и начинает поиск учетных данных в локальном пространстве;
- p22 – Получены учетные данные пользователя;
- p23 – Следы присутствия нарушителя в системе зачищены;
- p24 – Имеются привилегии на изменение значений ключей реестра;

- t0 – Отправка пользователю электронного письма с вредоносным кодом злоумышленника;
- t1 – Пользователь открывает письмо и запускает содержащийся в нём исполняемый файл;
- t2 – Злоумышленник маскирует имя исполняемого файла под текстовый документ, используя специальные Unicode-символы;
- t3 – Создание соединения с командным сервером злоумышленника с использованием нестандартного номера порта;
- t4 – Передача файла через существующий канал связи с командным сервером злоумышленника;
- t5 – Использование интерпретатора командной строки для выполнения команд;
- t6 – Поиск документов и мультимедиа файлов в файловой системе;
- t7 – Поиск интересующей информации в локальных базах данных;
- t8 – Сбор снимков экрана;
- t9 – Загрузка дополнительных вредоносных средств с командного сервера злоумышленника;
- t10 – Сбор и сжатие найденной информации в один файл;
- t11 – Обход управления учетными записями пользователя (UAC);
- t12 – Передача файла через существующий канал связи C2;
- t13 – Подмена в реестре ссылки на привилегированный COM-объект;
- t14 – Информация о настройке группы и уровне доступа каждого пользователя;
- t15 – Обнаружение запущенных процессов в системе;
- t16 – Поиск конфигурации сети и настройки системы;
- t17 – Обнаружение системной информации;
- t18 – Идентификация пользователей;
- t19 – Создание или изменение системных служб Windows;
- t20 – Сброс паролей от учетных записей;
- t21 – Сбор закрытых ключей и хешей паролей;
- t22 – Поиск незащищенных учетных данных в файлах;
- t23 – Поиск документов, доступ к которым ограничен;
- t24 – Зачистка следов присутствия в системе.

**Разработка мер защиты с учетом специфики объекта исследования**

Целенаправленным угрозам со стороны APT-группировок следует противодействовать на всех этапах реализации атаки и с использованием комплексного набора организационно-технических мер и средств защиты.

Для разработки мер противодействия были использованы данные об организационно-технических мерах защиты, которые изложены в методическом документе ФСТЭК России «Меры защиты информации в государственных информационных системах» [10].

В документе определены 13 групп мер защиты информации.

Основными особенностями, характерными для кибергруппировки APT29 является использование сложных технических приёмов (способов реализации компьютерных атак), нацеленных на повышение привилегий и обход средств защиты, поэтому именно на этих этапах требуется оказать максимальное противодействие. Одной из эффективных мер противодействия данным способам является использование антивирусных средств защиты. Пример модели меры защиты АВЗ.1 «Реализация антивирусной защиты» [9] для фрагмента сети Петри для сценария атаки, реализованного группировкой APT29 представлен на рис. 3.

Меры защиты описываются следующим фрагментом сети Петри:

$$C^m=(\{s1, s2, s3\}, \{d1, d2\}, I^m, O^m), \quad (2)$$

где s1 – позиция «Установлено средство антивирусной защиты»;

s2 – позиция «Вредоносный код злоумышленника обнаружен»;

s3 – позиция «Вредоносный код злоумышленника не обнаружен»;

d1 – переход «Антивирусная проверка входящих писем»;

d2 – переход «Антивирусная проверка файлов».

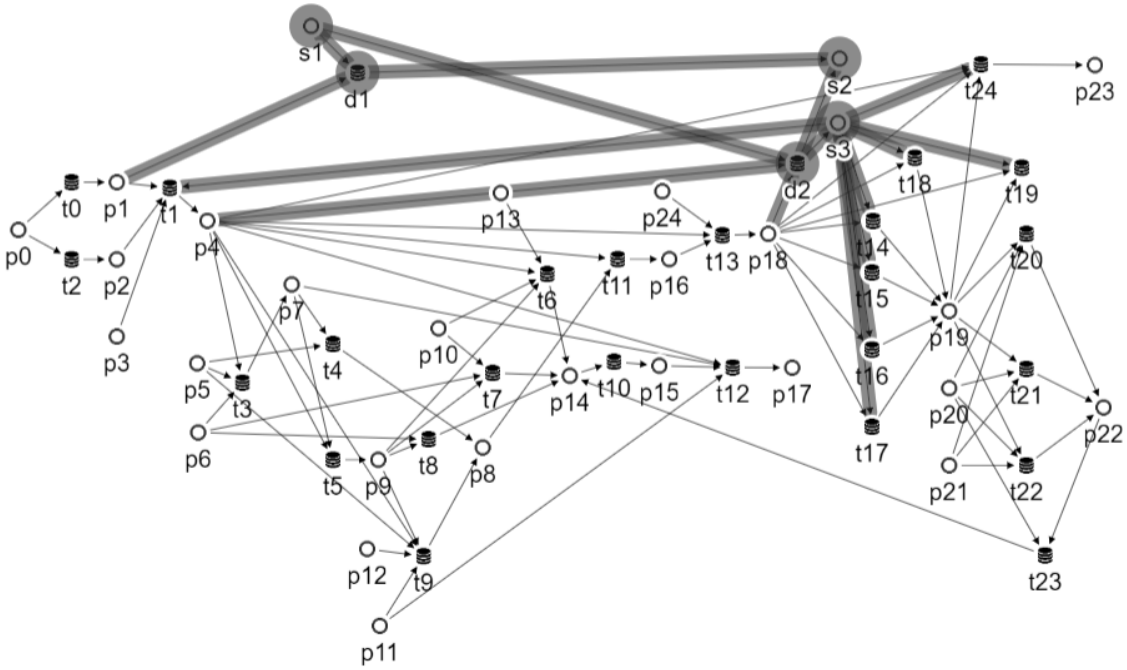


Рис. 3. Пример модели меры защиты АВЗ.1 «Реализация антивирусной защиты» [9] для фрагмента сети Петри для сценария атаки, реализованного группировкой APT29

Входные и выходные функции для фрагмента $C^m$ представлены в табл. 1.

Таблица 1

Входные и выходные функции участка сети Петри для меры АВЗ.1 «Реализация антивирусной защиты»

| t⊂{d1,d2} | Входные функции, $I^m(t)$ | Выходные функции, $O^m(t)$ |
|---|---|---|
| {d1} | {p1, s1} | {s2} |
| {d2} | {p1, p18, s1} | {t14, t15, t16, t17, t18, t19, t24} |

В приведённом примере мера АВЗ.1 «Реализация антивирусной защиты» [9] включает как проверку входящих электронных писем (применение периметральных средств антивирусной защиты – переход d1), так и периодическую проверку файлов (применение средств антивирусной защиты на автоматизированных рабочих местах – переход d2).

При необходимости моделирования усилений соответствующей меры предлагаемая модель должна быть расширена. Моделирование других мер осуществляется аналогичным образом за счёт встраивания позиций и переходов в соответствующие фрагменты модели (1). Наличие таких позиций и переходов должно приводить к блокировке переходов, моделирующих действия нарушителя, или к увеличению времени достижения состояний,

**Подход количественного оценивания рисков от действий группировок типа APT29**

Для оценки эффективности системы безопасности информации, а также выбора конкретных средств защиты может быть использована количественная оценка риска.

Формула риска имеет вид:

$$Risk\ (\mathrm{t}) = P(\mathrm{t}) \times U(\mathrm{t}), \qquad (3)$$

где P(t) – вероятность наступления ущерба за время t;

U(t) – величина ущерба за время t.

Для получения количественной оценки риска необходимо произвести оценку вероятности реализации успешных сценариев компьютерных атак, а также оценку ценности информации с учетом особенностей конкретных информационных систем.

Для оценки вероятности можем использовать несколько разных подходов, такие как:

– эпидемиологические модели, когда по аналогии заражения организма вирусом, моделируем процесс реализации компьютерной атаки на информационную систему, однако такой подход не обладает высокой точностью и требует, чтобы все узлы были однородны, а также накладывает ряд других ограничений (подход не учитывает возможности оперативного управления атакой в процессе её реализации) [2].

– подход на основе статистики для атак на конкретные типы информационной системы. Так как рассматривается конкретная APT-угроза, которая является частным случаем и для неё отсутствует массовая статистика, то данный подход не может быть реализован (подход ограничивается лишь поверхностными оценками и не учитывает возможности атакующего, причинно-следственные связи между его действиями, а также структурные особенности защищаемых информационных систем).

Существует еще один способ, который заключается в том, чтобы на нижнем уровне попытаться смоделировать все возможные варианты атак и всевозможные действия злоумышленников с учетом наличия тех или иных средств защиты и технологий в информационной системе. Реализация начинается с построения сети Петри на основе взаимосвязей технических приемов, применяемых в атаке группировки APT29.

Построив такую модель, где учитываются все причинно-следственные связи для всех этапов, начиная от проникновения в систему, заканчивая выводом информации из этой системы. Причем все связи учитывают систему разграничения доступа, наличие средств защиты, антивирусных систем, систем обнаружения вторжений, технологий виртуализации и т.д. Собрав для каждой связи свою уникальную статистику по наличию уязвимостей систем или по наличию вероятности преодоления межсетевых экранов того или иного типа, в результате получаем модель причинно-следственных связей (сеть Петри).

Использование сетей Петри-Маркова – есть следующий шаг на пути к расчету рисков, но для построения такой сети недостаточно причинно-следственных связей между техниками, а еще требуется:

– выявить вероятностно-временные характеристики, соответствующие участкам построенной модели;

– определить вероятности достижения выбранных позиций из сети Петри, связанных с нанесением ущерба информационной системе за заданное время.

В результате получим методику расчета частных показателей модели (сеть Петри-Маркова), что будет являться вторым шагом. Только после реализации первых двух ступеней можно переходить к расчету рисков (рис.4).


Рис. 4. Подход расчёта риска на основе сетей Петри-Маркова

В рамках настоящей статьи продемонстрирован подход реализации первого шага – определению причинно-следственных связей для техник, применяемых при совершении атаки группировкой APT29 на распределенные компьютерные системы. Оставшиеся задачи по нахождению рисков должны решаться в последующих работах, путем наложения на структуру сети случайного процесса в виде атаки и определения временных и вероятностных характеристик.

**Заключение**

В ходе работы был выполнен анализ существующих исследований в области моделирования, анализа и выработки средств противодействия атаками группировки APT29 в распределенных компьютерных системах.

Была построена расширяемая комплексная модель реализации сценариев проведения компьютерных атак кибергруппировкой APT29 на распределенные компьютерные системы, предоставлен анализ взаимосвязей между техническими приемами, применяемыми в ходе атаки.

В рамках работы рассматривались лишь причинно-следственные связи между действиями злоумышленника на основании сведений об условиях их реализации и возможных последствий (последствия одних действия являются условиями реализации последующих действий). В качестве таких условий/последствий выступают характеристики как самой группировки APT29, так и характеристики защищаемой системы. В общем случае условия/последствия разделяются на привилегии доступа, а также на сведения о системе или защищаемой информации.

Построенная модель учитывает меры защиты от сценариев реализации целенаправленных атак и может быть расширена до сети Петри-Маркова, путем определения вероятностно-временных характеристик для участков сценария, что позволит проводить количественное оценивание реализуемости соответствующих угроз, а также эффективность мер защиты от них.

Разработанная модель, в практическом плане может быть использована в качестве

основы для разработки средств защиты распределенных компьютерных систем от подобных сценариев APT-атак, так как зачастую группировки используют схожие

сценарии и техники при реализации атаки.

Данные исследования в перспективе станут полезным инструментом в руках IT-специалистов при обеспечении информационной безопасности распределенных компьютерных систем, а постоянно увеличивающиеся база компьютерных атак и развитие модели, построенной в рамках данной работы, позволит разрабатывать успешные практические приемы, необходимые для остановки реализации атак на распределенные компьютерные системы.

Реализованный подход позволяет осуществить моделирование мер защиты, регламентируемых нормативными и методическим документами, что даст возможность принятия количественно обоснованных решений при построении системы защиты с учётом специфики защищаемого объекта.

При этом необходимо отметить, что модель сети Петри, учитывающая большинство основных способов реализации компьютерных атак и мер защиты от них с продемонстрированным уровнем детализации потребует порядка тысячи позиций и переходов, что создаёт определённые сложности для поддержки таких моделей. Преодоление данного ограничения возможно за счёт реализации экспертной системы на базе картографических методов работы с графовыми моделями, примеры использования которых были показаны в [15, 16, 17].

**Список литературы**

1. Кибербезопасность // Официальный сайт компании «Позитив Текнолоджиз» – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/ (дата обращения: 11.12.2020).

2. Калашников А.О. Модели количественного оценивания компьютерных атак (часть 2) / А.О. Калашников, К.А. Бугайский, Е.В. Аникина // Информация и безопасность. 2019. Т. 22 №4. С. 529 – 538.

3. Таргетированные или целевые кибератаки 2014 год. URL: https://www.kaspersky.ru/blog/independent-tests-2014/7293/ (дата обращения: 11.12.2020).

4. Таргетированные или целевые кибератаки 2015 год. URL: http://book.itep.ru/depository/surveys/M-Trends_2015_A_View_From_the_Front_Lines.pdf (дата обращения: 11.12.2020).

5. Таргетированные или целевые кибератаки 2016 год. URL: https://www.pvsm.ru/vzlom/199381 (дата обращения: 11.12.2020).

6. Таргетированные или целевые кибератаки 2017 год. URL: https://plusworld.ru/daily/cat-security-and-id/laboratoriya-kasperskogo-razrabotala-tehnologiyu-zashhity-ot-ugroz-udalennogo-administrirovaniya/ (дата обращения: 11.12.2020).

7. Таргетированные или целевые кибератаки 2019 год. URL: https://www.tadviser.ru/images/6/6b/Microsoft-%D0%B8-Positive-Technologies_Final.pdf (дата обращения: 11.12.2020).

8. Таргетированные или целевые кибератаки 2020 год. URL: https://news.myseldon.com/ru/news/index/241312722 (дата обращения: 11.12.2020).

9. Меры защиты информации в государственных информационных системах. Методический документ. URL: https://fstec.ru/component/attachments/download/675 (дата обращения: 11.12.2020).

10. MITRE ATT&CK. URL: https://attack.mitre.org/ (дата обращения: 11.12.2020).

11. The MITRE Corporation, "Masquerading". URL: https://attack.mitre.org/techniques/T1036/ (дата обращения: 11.12.2020).

12. The MITRE Corporation, "User Execution". URL: https://attack.mitre.org/techniques/1204/ (дата обращения: 11.12.2020).

13. The MITRE Corporation, " Remote Services: Windows Remote Management". URL: https://attack.mitre.org/techniques/1028/ (дата обращения: 11.12.2020).

14. The MITRE Corporation, "Remote System Discovery". URL: https://attack.mitre.org/techniques/1018/ (дата обращения: 11.10.2020).

15. Serdechnyi A.L. Mapping retrieval method for academic publications in the field of aerospace technology safety / Serdechnyi A.L., Goncharov A.A., Ostapenko A.G., Bataronov I.L. // В сборнике: IOP Conference Series: Materials Science and Engineering. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. 2020. С. 52028.

16. Калашников А.О. Картографический подход в библиометрическом исследовании отечественных научных школ, сложившихся в области защиты информации и обеспечения информационной безопасности / Калашников А.О., Сердечный А.Л., Остапенко А.Г. // Информация и безопасность. 2019. Т. 22. № 4. С. 455-484.

17. Сердечный А.Л. Картографический подход к описанию киберпространства в контексте обеспечения безопасности информации и информационной безопасности / Сердечный А.Л., Остапенко А.Г. // Информация и безопасность. 2019. Т. 22. № 3. С. 387-398.

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 20.01.2021

**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

**Краюшкин Павел Сергеевич** – студент, Воронежский государственный технический университет, e-mail: pavelkrayushkin@mail.ru

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

**Язов Юрий Константинович**– д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: yazoff_1946@mail.ru

# MODELING, ANALYSIS AND COUNTERING SCENARIOS OF PREPARING COMPUTER ATTACKS REALIZED BY THE GROUP APT29 IN DISTRIBUTED COMPUTER SYSTEMS

**A.L. Serdechnyy, P.S. Krayushkin, M.A. Tarelkin, Y. K. Yazov**

The article is devoted to modeling computer attacks on distributed corporate computer systems, using the example of the actions of the Advanced Persistent Threat 29 (APT29) group. The article proposes an approach to modeling the methods implemented by this grouping, as well as measures to protect against them. The approach is based on Petri nets and information about the techniques (MITRE ATT&CK project). The developed models take into account the relationship between the conditions and consequences of actions committed by the APT29 group during attacks on distributed enterprise systems. The article also demonstrates the possibility of increasing the model by including models of protection measures against the considered methods of implementing computer attacks. The proposed models can be supplemented by modeling new ways of implementing computer attacks used by other cyber groups. In addition, the models can be extended to Petri-Markov network models by implementing special methods for calculating probabilistic-time characteristics for fragments of the proposed models.

Keywords: cybercrime groups, APT attacks, Petri nets, ATT&CK, APT 29, distributed computer systems.

Submitted 20.01.2021

**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

**Pavel S. Krayushkin –** Student, Voronezh State Technical University, email: pavelkrayushkin@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

**Yurii K. Yazov** – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: yazoff_1946@mail.ru