DOI 10.36622/VSTU.2021.24.1.006
УДК 004.056.53:004.75:004.735

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

В настоящей статье представлены результаты моделирования способов реализации компьютерных атак на корпоративные распределенные компьютерные системы. 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 корпоративных распределённых компьютерных сетей (условия и последствия моделируются позициями сети Петри, а сами технические приёмы – переходами сети Петри). Также в статье продемонстрирована возможность наращивания модели за счёт включения в неё моделей мер защиты, используемых в нормативных и методических документах ФСТЭК России.

Ключевые слова: корпоративные распределённые компьютерные систем, способы реализации компьютерных атак, ATT&CK, сети Петри, моделирование мер защиты.

Введение

Актуальность моделирования сценариев реализации угроз безопасности информации обусловлена необходимостью выбора эффективных мер защиты от них в условии всё нарастающего многообразия способов реализации компьютерных атак, из которых формируются сценарии. Данная задача имеет особое значение для корпоративных распределённых компьютерных систем (РКС) как одних из наиболее распространённых информационных систем, в которых обрабатывается защищаемая информация.

При выборе средств защиты для конкретной информационной системы необходимо учитывать то, что средства защиты обладают различными параметрами и разрабатываются с учётом специфики информационных систем. Для корпоративных РКС такой спецификой является гетерогенность защищаемой среды, а также её высокая изменчивость. В настоящий момент существует большая номенклатура технологий и различных платформ, которые лежат в основе корпоративных систем. Кроме того, часть инфраструктуры корпоративных информационных систем может располагаться в облаке и не быть полностью контролируемой их владельцами.

Обоснованный выбор средств защиты предполагает проведение количественной оценки реализуемости угроз безопасности информации, что требует расчёта вероятности реализации наиболее актуальных сценариев проведения компьютерных атак, а также определение величины возможного ущерба, в случае их успешной реализации. Настоящая работа направлена на формирование методической основы для оценки показателя вероятности реализации угроз компьютерных атак на корпоративные распределённые компьютерные системы. Однако, расчет ущерба выходит за рамки данной работы.

Существуют различные подходы оценивания показателя вероятности реализации угроз, среди которых:

– эпидемиологический подход к расчёту вероятности распространения вредоносного ПО [1] (подход не учитывает возможности

оперативного управления атакой в процессе её реализации);

– подход расчёта вероятности конкретных атак, основанный на статистике по уязвимостям, связанным с такими атаками [2] (подход ограничивается лишь поверхностными оценками и не учитывает возможности атакующего, причинно-следственные связи между его действиями, а также структурные особенности защищаемых информационных систем);

– ресурсно-временной подход расчёта вероятности успешной реализации компьютерной атаки [3] (не предполагает моделирование мер защиты информации с уровнем детализации, соответствующим описанию мер в документах ФСТЭК России [4, 5]).

При этом необходимо отметить, что для комплексного оценивания показателя вероятности реализации угроз с учётом структурных и функциональных особенностей защищаемых информационных систем требуется детальное представление сценариев реализации компьютерных атак в виде последовательности действий, совершаемых злоумышленниками. Поэтому для оценивания вероятности реализации угроз предполагается использование аппарата сетей Петри-Маркова [6]. Данный подход предполагает построение моделей причинно-следственных связей между действиями, совершаемыми злоумышленниками в ходе реализации атак, а также определение для построенной модели вероятностно-временных характеристик её элементов.

Для его реализации требуется:

– определить причинно-следственные связи между действиями, совершаемыми злоумышленниками в ходе реализации атаки (причинно-следственные связи определяются условиями и последствиями действий злоумышленника);

– осуществить моделирование действий злоумышленника с помощью переходов аппарата сетей Петри, а условий и последствий таких действий – с помощью позиций;

– определить вероятностно-временные характеристики участков построенной модели с целью преобразования сети Петри в сеть Петри-Маркова;

– рассчитать вероятности достижения определённых позиций сети Петри (позиций, при достижении которых за заданное время защищаемой информационной системе наносится ущерб).

Целью настоящих исследований является формирование основы для реализации данного подхода. В настоящей работе исследования ограничены первыми двумя этапами, по результатам выполнения которых разработана модель сценариев реализации компьютерных атак на корпоративные РКС с использованием аппарата сетей Петри.

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, разработкой 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 [7]. Способы разбиты на группы, соответствующие различным этапам реализации компьютерных атак.

В данной базе не содержатся сведения о причинно-следственных связях между способами реализации компьютерных атак. Отсутствие связей означает, что на основе имеющихся данных невозможно построить модель проведения компьютерных атак на элементы корпоративной распределенной компьютерной системы.

Таким образом, для реализации представленного подхода в первую очередь требуется формирование модели причинно-следственных связей между способами реализации компьютерных атак.

Ввиду большого объёма базы данных ATT&CK, в рамках настоящей работы осуществляется моделирование лишь основных сценариев угроз безопасности

информации на корпоративные распределенные компьютерные системы.

В существующих работах по теме обеспечения безопасности информации в корпоративных РКС [8-16] основное внимание уделено выработке мер защиты против отдельных технических приемов проведения компьютерных атак (КА). При этом остается непроработанным вопрос исследования связей между техническими приемами проведения КА и возможностью противодействия им со стороны средств защиты.

По результатам исследования существующих работ по моделированию и анализу сценариев реализации угроз безопасности информации в корпоративных РКС [17-20] и их недостатков возникает целый ряд противоречий:

– между сложившейся практикой оценки защищенности, основанной на анализе существующих технических приемов проведения КА, и необходимостью анализа КА на элементы корпоративной РКС с учетом выявленных связей между техническими приемами их проведения;

– между сложившейся методологией защиты, основанной на технических приемах проведения компьютерных атак, и необходимостью регулирования защищенности объекта с учетом рисков успешности проведения атак на корпоративные РКС.

Объектом настоящего исследования являются корпоративные РКС под воздействием атак, реализуемых с использованием технических приемов, на конфиденциальные данные в корпоративных РКС.

В свою очередь, предметом исследования является формирование основы для регулирования и оценки рисков успешной реализации угроз безопасности информации в РКС, заключающееся в построении модели успешных сценариев компьютерных атак в корпоративных РКС, а также мер противодействия таким сценариям.

Постановка задач исследования.

Основной целью исследования следует считать повышение защищенности конфиденциальных данных корпоративных РКС от заданных атак за счет создания соответствующего методического обеспечения, которое впоследствии можно использовать для расчета рисков и выявления оценки защищенности современных корпоративных РКС.

Для достижения сформулированной цели представляется необходимым решение следующих задач:

– построение модели успешности проведения компьютерных атак на элементы корпоративной РКС с учетом выявленных связей между техническими приемами с использованием аппарата сетей Петри;

– моделирование средств защиты на основе анализа построенной модели проведения компьютерных атак на элементы корпоративной РКС.

Содержание основных результатов

Технология моделирования сценариев угроз безопасности информации на корпоративные РКС заключалась в выполнении следующих действий:

– из описанных в базе данных MITRE ATT&CK приемов были выбраны наиболее актуальные технические приёмы, относящиеся объекту исследования;

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

а) условия реализации технического приёма;
б) действия, которые оказывает прием на атакуемую систему;
в) последствия успешной реализации технического приема.

– определение взаимосвязей между действиями злоумышленника на основании полученных сведений об условиях и последствиях их реализации;

– построение модели с использованием аппарата сетей Петри.

В результате выполнения указанных действий построена модель проведения компьютерных атак на корпоративные РКС, описываемая следующей сетью Петри:

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

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.

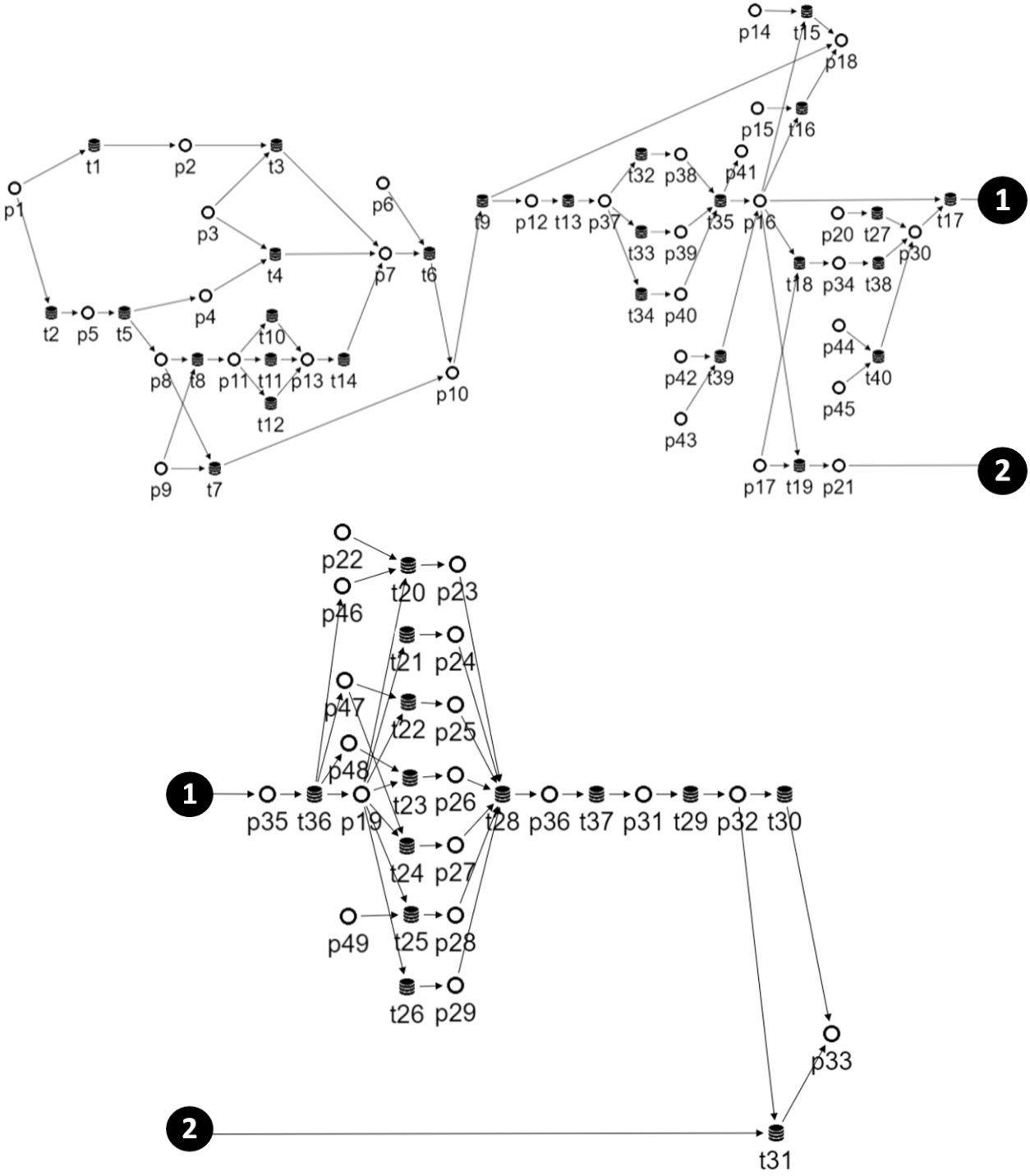

Рис. 1. Построенная в виде сети Петри модель проведения компьютерных атак на корпоративные РКС

На рис. 1 обозначают следующее позиции и переходы:

– p1 – злоумышленники владеют email-адресами, принадлежащими организации/ работникам организации;

– p2 – пользователь получил письмо от злоумышленника и открыл его;

– p3 – на компьютере пользователя установлено ПО для работы с подходящим типом файлов;

– p4 – вредоносный файл загружен на компьютер пользователя;

– p5 – пользователь получил письмо от злоумышленника и открыл его;

– p6 – в системе пользователя используется протокол аутентификации SMB или WebDAV;

– p7 – вредоносный код, содержащийся в файле, может начать выполнение;

– p8 – пользователь посещает легитимный веб-сайт, скомпрометированный злоумышленниками;

– p9 – браузер пользователя имеет известные уязвимости или установленные плагины в браузере пользователя имеют известные уязвимости;

– p10 – злоумышленники получают hash учетных данных пользователя;

– p11 – вредоносный код попадает в систему пользователя;

– p12 – злоумышленники получают учетные данные аккаунта пользователя в незашифрованном виде;

– p13 – в системе пользователя появились вредоносные файлы, маскирующиеся под безопасные;

– p14 – наличие в атакуемой системе «Сервера проверки подлинности локальной системы безопасности» Windows;

– p15 – наличие в атакуемой системе службы «Диспетчер учётных записей безопасности» Windows;

– p16 – злоумышленник получает доступ в систему пользователя под видом существующего пользователя;

– p17 – пользователь обладает правами администратора;

– p18 – злоумышленники получают доступ к новым hash данным учетных записей пользователя;

– p19 – в системе пользователя появляются задания, которые с заданной периодичностью выполняют некоторые действия необходимые злоумышленнику, например, сбор и поиск защищенных данных, поиск различной системной информации в сети пользователя и т.д.;

– p20 – злоумышленники создают учетные записи, которые выглядят как легитимные;

– p21 – злоумышленники получают доступ к методам «эксфильтрации»;

– p22 – наличие в атакуемой системе сервера Microsoft Exchange Server;

– p23 – злоумышленники находят и сохраняют конфиденциальную электронную почту;

– p24 – злоумышленники сохраняют конфиденциальную информацию, отображающуюся на экране пользователя;

– p25 – злоумышленники находят и сохраняют искомую конфиденциальную информацию;

– p26 – получен список учетных записей домена;

– p27 – получен список файлов и папок;

– p28 – получен список файлов, папок и дисков с общим доступном внутри сети;

– p29 – создано временное хранилище;

– p30 – для дальнейших действий злоумышленники используют созданные ими учетные записи;

– p31 – собранные конфиденциальные данные перемещены во временное хранилище;

– p32 – собранные конфиденциальные данные заархивированы;

– p33 – эксфильтрация конфиденциальных данных происходит небольшими порциями в автоматическом режиме;

– p34 – оператором установлены и реализованы функции управления учетными записями пользователей;

– p35 – оператором реализованы меры управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа;

– p36 – в информационной системе осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы;

– p37 – активирован механизм реализации меры управления доступом субъектов доступа к объектам доступа;

– p38 – оператором обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей);

– p39 – в информационной системе обеспечено оповещение пользователя о дате и времени предыдущего входа в информационную систему от имени этого пользователя;

– p40 – в информационной системе обеспечивается ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы;

– p41 – осуществлена неудачная аутентификация пользователя;

– p42 – в системе обеспечивается многофакторная аутентификация для удаленного и локального доступа в систему с правами привилегированных и непривилегированных учетных записей;

– p44 – в системе обеспечивается многофакторная аутентификация для удаленного и локального доступа в систему с правами привилегированных и непривилегированных учетных записей;

– p43 –обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними;

– p45 – обеспечивается аутентификация устройств до начала информационного взаимодействия с ними;

– p46 – наличие привилегий доступа к электронной почте;

– p47 – наличие привилегий доступа к файлам пользователя;

– p48 – наличие привилегий доступа к файлам пользователя;

– p49 – наличие привилегий доступа к сетевым ресурсам;

– t1 – целевые фишинговые вложения в электронном письме;

– t2 – целевые фишинговые ссылки в электронном письме;

– t3, t4 и t14 – пользователь открывает вредоносный файл;

– t5 – пользователь переходит по вредоносной ссылке;

– t6 и t7 – форсированная аутентификация;

– t8 – выполнение вредоносного кода в системе пользователя, посредством эксплуатации уязвимости браузера или его компонента;

– t9 – взлом паролей;

– t10 – выполнение вредоносного кода в системе пользователя с помощью имеющегося ПО;

– t11 – использование шаблонов документов как средства доставки вредоносного кода;

– t12 – маскирование созданных файлов;

– t13 и t27 – использование существующих учетных записей;

– t15 – выгрузка данных из «Сервера проверки подлинности локальной системы безопасности» Windows;

– t16 – выгрузка данных об учетных записях через «Диспетчер учётных записей безопасности» Windows;

– t17 – выполнение заданий по расписанию;

– t18 – управление аккаунтами в системе пользователя;

– t19 – отключение межсетевого экрана или изменение его настроек;

– t20 – поиск и выгрузка электронной почты с почтового сервера;

– t21 – создание и сохранение снимков экрана;

– t22 – поиск конфиденциальных файлов;

– t23 – поиск доменных аккаунтов;

– t24 – поиск файлов и папок в системе пользователя;

– t25 – поиск файлов, папок и дисков с общим доступном внутри сети;

– t26 – создание временного хранилища для найденной информации;

– t28 – выполнение заданий по расписанию;

– t29 – архивирование, сжатие и шифрование собранных данных;

– t30 – ограничение размера скачиваемых данных при эксфильтрации;

– t31 – автоматическая эксфильтрация;

– t32 – производится проверка, достаточно ли пользователю полномочий для выполнений текущего действия;

– t33 – после входа в систему, пользователь видит оповещение о дате и времени предыдущего входа в информационную систему от имени этого пользователя;

– t34 – производится проверка количества одновременных сеансов текущего пользователя в информационной системе;

– t35 – аутентификация пользователя;

– t36 – авторизация пользователя;

– t37 – производится сканирование и анализ информационных потоков в рамках информационной системы;

– t38 – система по управлению учетными записями пользователей производит проверку вновь созданной учетной записи на соответствие установленным политикам;

– t39 – производится дополнительная идентификация и аутентификация пользователей при входе в систему;

– t40 – производится дополнительная идентификация и аутентификация пользователей при входе в систему;

Позиции {p34 – p49} и переходы {t32 – t40} моделируют меры защиты РКС от рассмотренных способов. В качестве основного источника мер использован методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» [4], так как в нем представлен наиболее полный перечень разработанных мер защиты информации в информационной системе, а уровень детализации мер достаточен для задач администрирования безопасности.

Заключение

Получены следующие результаты:

– построена модель сценариев реализации компьютерных атак на элементы корпоративной РКС, учитывающая связи между техническими приемами, используемыми в ходе реализации сценариев атак;

– проведено моделирование мер защиты от сценариев реализации угроз безопасности информации на корпоративные РКС.

Новизна вышеперечисленных результатов просматривается в том, что:

– построена расширяемая комплексная модель реализации сценариев проведения компьютерных атак на элементы корпоративной РКС, отличающаяся от известных моделей (построенных с использованием аппарата сетей Петри) составом и уровнем детализации действий нарушителя, реализуемых в ходе атаки, а также наличием мер защиты от таких действий;

– впервые сформированы основы для регулирования и оценки рисков реализации угроз безопасности информации в РКС, с использованием аппарата сетей Петри-Маркова и расширяемой комплексной модели реализации сценариев проведения компьютерных атак, учитывающей основные способы реализации компьютерных атак, представленные в базе данных MITRE ATT&CK, а также меры защиты от них.

Проведение дальнейших исследований будет направлено на определение вероятностно-временных характеристик участков построенной модели с целью преобразования сети Петри в сеть Петри-Маркова и расчёт вероятности достижения определённых позиций сети Петри (позиций, при достижении которых за заданное время защищаемой информационной системе наносится ущерб).

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 [22-26].

Список литературы

1. Эпидемии в телекоммуникационных сетях / Остапенко А.Г., Радько Н.М., Калашников А.О., и др.; [Под ред. Гл. корр. РАН Д.А. Новикова.] М.: Горячая линия – Телеком. 2018. (серия «Теория сетевых войн»; Вып. 1). 284 с.:

2. Risk Assessment Method for Cyber Security of Cyber Physical Systems. URL: https://sci-hub.do/10.1109/ICRSE.2015.7366430 (дата обращения: 23.12.2020).

3. 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.

4. Меры защиты информации в государственных информационных системах / ФСТЭК России — 2020 / URL: https://fstec.ru/component/attachments/download/675 (дата обращения: 14.12.2020).

5. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17/ ФСТЭК России — 2020 / URL: https://fstec.ru/component/attachments/download/1499 (дата обращения: 11.02.2021).

6. 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.

7. Информационный ресурс MITRE ATT & CK. URL: https://blog.tiger-optics.ru/2018/12/what-is-mitre-attack (дата обращения: 18.12.2020).

8. Карасёв П.А. Информационная безопасность в корпоративных сетях // Таврический научный обозреватель. 2017. №3-1 (20). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-korporativnyh-setyah (дата обращения: 14.01.2021).

9. Сборник исследований по практической информационной безопасности. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf (дата обращения: 19.12.2020).

10. Итоги внешних пентестов — 2020. URL: https://www.ptsecurity.com/ru-ru/research/analytics/external-pentests-2020/ (дата обращения: 15.12.2020).

11. Статистика уязвимостей корпоративных информационных систем. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Corporate-vulnerability-2014-rus.pdf (дата обращения: 11.12.2020).

12. Уязвимости корпоративных информационных систем, 2015. URL: https://docplayer.ru/33148775-Uyazvimosti-korporativnyh-informacionnyh-sistem.html (дата обращения: 14.12.2020).

13. Уязвимости корпоративных информационных систем, 2019. URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/ (дата обращения: 13.12.2020).

14. Уязвимости периметра корпоративных сетей. URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-corporate-networks-2020/#id3 (дата обращения: 11.10.2020).

15. Итоги внутренних пентестов — 2020. URL: https://www.ptsecurity.com/ru-ru/research/analytics/internal-pentests-2020/ (дата обращения: 11.12.2020).

16. Корниенко А. А. Моделирование компьютерных атак на распределенную информационную систему / А. А. Корниенко, А. Б. Никитин, С. В. Диасамидзе // Известия Петербургского университета путей сообщения. 2018. №4. С. 208-213.

17. Добкач Л.Я. Анализ методов распознавания компьютерных атак // Правовая информатика. 2020. №1. С. 51-63.

18. Казимир В. В., Серая А. А. Метод построения моделей информационных атак // ММС. 2010. №4. С. 97-102.

19. Тумоян Е. П. Методы формального моделирования сетевых атак // Известия ЮФУ. Технические науки. 2007. 1. С. 82-92.

20. Трещев И.А., Вильдяйкин Г. Ф., Ядыменко К.А. О подходе к анализу защищенности корпоративных информационных систем // Мир науки. Педагогика и психология. 2014. №3. С. 105-112.

21. Меры защиты информации в государственных информационных системах / ФСТЭК России — 2020 / URL: https://fstec.ru/component/attachments/download/675 (дата обращения: 14.12.2020).

22. 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.

23. 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.

24. 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.

25. Сердечный А.Л. Технологии картографирования защищаемого киберпространства / А.Л. Сердечный, М.А. Тарелкин, А.А. Ломов и др. // Информация и безопасность. 2019. Том 21. Ч.3. С. 399-410.

26. Сердечный А.Л. Карты источников, содержащих сведения об уязвимостях программного обеспечения / А.Л. Сердечный, М.А. Тарелкин, А.А. Ломов // Информация и безопасность. 2019. Том 21. Ч.3. С. 399-410.

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
Шевелюхин Артем Александрович – студент, Воронежский государственный технический университет, e-mail: artem_16_97@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
Бабурин Александр Вильямович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mr.bav49@mail.ru

MODELING, ANALYSIS AND COUNTERING SCENARIOS OF INFORMATION SECURITY THREATS ON CORPORATE DISTRIBUTED COMPUTER SYSTEMS

A.L. Serdechnyy, A.A. Sheveliukhin, M.A. Tarelkin, A.V. Baburin

This article presents the results of modeling computer attack methods on corporate distributed computer systems. The proposed models of methods 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 choice of informed security measures. The model development of ways to implement computer attacks was carried out using the Petri nets approach based on the information contained in the MITRE ATT&CK database. The developed model is interconnected on the conditions and consequence of the basic techniques defined in the database ATT&CK and relevant for enterprise distributed computer networks (conditions and consequence are simulated positions Petri nets themselves and techniques – transitions Petri nets). In addition, the article demonstrates the possibility of increasing the model by including models of protection measures against the considered methods of implementing computer attacks, defined in the regulatory and methodological documents of the FSTEC of Russia

Key words: corporate distributed computer systems, model of computer attacks methods, ATT&CK, Petri nets, modeling of security measures.

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
Artem S. Sheveliukhin – Student, Voronezh State Technical University, email: artem_16_97@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
Alexander V. Baburin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mr.bav49@mail.ru