DOI 10.36622/VSTU.2021.24.2.003
УДК 004.056

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ ПОДГОТОВКИ КОМПЬЮТЕРНЫХ АТАК В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, Н.С. Пустовалов, М.А. Тарелкин, А.Е. Дешина

Цель проведённых исследований заключалась в формализации действий нарушителя, совершаемых в ходе подготовки компьютерной атаки как основного этапа, на котором можно оказать противодействие нарушителю до того, как защищаемой системе будет нанесён ущерб. В настоящей статье представлены результаты разработки модели сети Петри для этапа подготовки к компьютерной атаке в распределенных компьютерных системах. Модель учитывает причинно-следственные связи между действиями нарушителя, а также условиями и последствиями реализации таких действий. Наличие таких связей позволяет определять сценарии подготовки компьютерных атак в зависимости от структурных и функциональных особенностей объекта защиты и модели нарушителя. Разработанная модель может быть использована в качестве исходных данных при моделировании угроз безопасности информации в части определения способов, используемых нарушителем при выборе объекта атаки, а также в ходе получения необходимых ресурсов для её совершения. Также в настоящей статье продемонстрирована возможность моделирования мер защиты, затрудняющих реализацию сценария к атаке.

Ключевые слова: сеть Петри, ATT&CK, подготовка компьютерной атаки, моделирование.

Введение

В настоящее время существует огромное количество угроз, реализуемых в распределенных компьютерных системах (РКС), таких как раскрытие конфиденциальной информации, уничтожение и искажение данных, вывод компьютерной системы из строя и т.п. Реализация компьютерной атаки является труднореализуемой, если у атакующего отсутствует информация об объекте атаки, поэтому принципиально важное значение имеет предотвращение и пресечение возможностей нарушителя по сбору информации о защищаемой РКС. Реализация этого подразумевает развитие системы защиты информации и эффективное использование ресурсов РКС [1-3].

Для осуществления обоснованного выбора мер и средств защиты от постоянно увеличивающегося и эволюционирующего множества угроз безопасности информации, а также рационального использования имеющихся ресурсов необходимы количественная оценка сценариев реализации угроз в РКС [3-7]. Реализация включает оценку вероятностей осуществления этих сценариев, а также ценность защищаемой информации (с учётом особенностей конкретных информационных систем для соответствующих организаций, чью деятельность обеспечивают такие информационные системы) [8-10].

Одним из подходов оценки риска является использование аппарата сетей Петри-Маркова для определения вероятности наступления состояний, приводящих к ущербу для организации [11, 12].

Реализация подхода применительно к теме исследований предполагает выполнение следующих этапов:

– выявление связей между действиями подготовки нарушителя к компьютерной атаке (построение сети Петри);

– определение вероятностно-временных характеристик процессов, связанных с моделируемыми действиями (моделирование сети Петри-Маркова);

– использование построенной модели в моделях сценариев реализации компьютерных атак, для которых требуется учёт подготовительного этапа;

– расчёт рисков реализации угроз безопасности информации на РКС.

Реализация первого этапа данного подхода было продемонстрировано на примере моделирования действий киберпреступных группировок [13, 14], а также сценариев реализации угроз безопасности информации на корпоративные распределенные компьютерные системы [15]. Для его осуществления также, как и в настоящей работе в качестве исходных данных была использована база данных ATT&CK [16], в которой объединены сведения о способах реализации компьютерных атак (в том числе, реализуемых на этапе подготовки компьютерных атак в РКС).

Ведением базы данных ATT&CK занимаются ведущие организации в области защиты информации, а также частные исследователи. Руководство проектом осуществляет компания MITRE Corporation. База данных ATT&CK содержит описания сотен технических приёмов, используемых нарушителями в ходе проведения компьютерных атак. Способы разбиты на несколько групп, соответствующих различным этапам подготовки и реализации компьютерных атак в РКС [17].

При этом необходимо отметить, что в данной базе отсутствуют сведения о причинно-следственных связях между способами. В связи с этим первой задачей является формирование модели причинно-следственных связей между способами подготовки и реализации компьютерных атак в РКС.

Таким образом, объектом исследования являются РКС под воздействием атак, реализуемых с использованием технических приемов подготовки, направленных на получение предварительных сведений об атакуемой информационной системе и на способы подготовки средств осуществления компьютерной атаки.

В свою очередь, предметом исследования является формирование основы для регулирования и оценки рисков реализации угроз безопасности информации в РКС, заключающейся в построении модели сценариев подготовки к компьютерной атаке, а также мер противодействия таким сценариям.

Содержание основных результатов

В рамках разработки модели действий нарушителя на этапе подготовки компьютерной атаки в РКС установлены причинно-следственные связи между техническими приемами используемыми, злоумышленниками при выборе объекта атаки, а также в ходе получения необходимых ресурсов для её совершения. Исходные данные для моделирования получены их матрицы PRE ATT&CK v8 [18-19]. В результате их анализа были определены причинно-следственных связи между основными техническими приёмами и построена сеть Петри, в которой переходам соответствовали процессы реализации рассмотренных технических приёмов, а позициям – условия и последствия реализации таких действий.

Рассмотренные технические приёмы соответствовали следующим группам способов, реализуемых нарушителем в ходе подготовки к проведению компьютерной атаки в РКС:

– способы получения предварительных сведений об атакуемой информационной системе:

а) поиск по открытым веб-сайтам или доменам:

1) поиск по социальным медиа;

2) поиск с использованием глобальных поисковых систем;

3) поиск на официальных сайтах и других информационных ресурсах атакуемой организации;

4) поиск в открытых технических базах данных (таких как CDN, DNS, WHOIS);

5) сканирование в открытых технических базах данных;

6) анализ цифровых сертификатов;

б) поиск в информационных источниках с ограниченным доступом:

1) покупка данных о составе и структуре информационной системы;

в) сбор информации о хосте пользователя:

1) оборудование;

2) программное обеспечение;

3) конфигурация клиента;

г) сбор информации о сети:
1) устройство сетевой безопасности;
2) IP-адреса;
3) свойства домена;
4) DNS;
д) фишинг с целью получения предварительной информации:
1) с помощью службы и приложения Spearphishing;
2) целевой фишинг;
е) активное сканирование информационных ресурсов организации:
1) сканирование IP-блоков;
2) сканирование уязвимостей;

– способы подготовки средств осуществления компьютерной атаки:
а) создание учетных записей:
1) социальные медиа;
2) электронная почта;
б) взлом учетных записей:
1) социальные медиа;
2) электронная почта;
в) разработка средств проведения компьютерной атаки:
1) выявление уязвимостей и разработка эксплойтов;
2) получение легитимных сертификатов и цифровых подписей кода;
3) получение сертификатов SSL/TLS;
4) разработка средства проведения компьютерной атаки;
г) покупка или кража средств проведения компьютерной атаки:
1) вредоносного ПО;
2) сертификатов подписи кода;
3) сертификаты SSL/TLS;
4) эксплойтов;
д) развитие инфраструктуры для проведения компьютерной атаки:
1) формирование ботнета;
2) настройка DNS-серверов;
е) покупка или кража инфраструктур для проведения компьютерной атаки:
1) аренда/«угон» ботнет;
2) покупка домен и/или субдомен/ кибersквотинг;
3) регистрация доменных имён.

Разработка модели осуществлялась в соответствии со схемой, представленной на рис. 1.

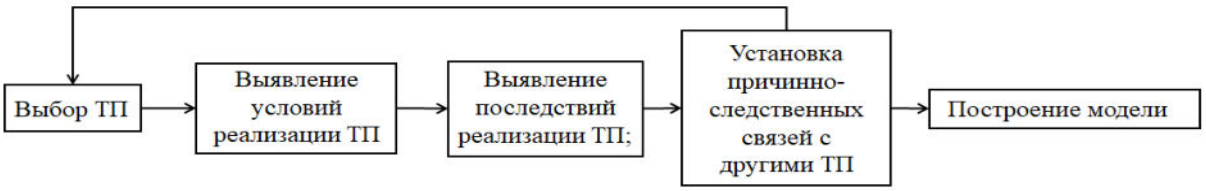

Рис. 1. Процедура моделирования действий нарушителя на этапе подготовки компьютерной атаки в РКС

В соответствии с данной процедурой осуществлены следующие действия:

– выбор технического приема (ТП) из базы данных PRE ATT&CK;

– определение объекта, на который нарушитель воздействует в ходе реализации выбранного технического приёма;

– определение возможных условий реализации технического приема;

– определение возможных последствий реализации технического приема;

– соотнесение с другими техническими приёмами на основании определённых причинно-следственных связей и объекта воздействия;

– соотнесение технического приёма с действием нарушителя (переходом сети Петри);

– соотнесение условий и последствий с позициями сети Петри.

Разработанная модель действий нарушителя на этапе подготовки компьютерной атаки в РКС показана на рис. 2.

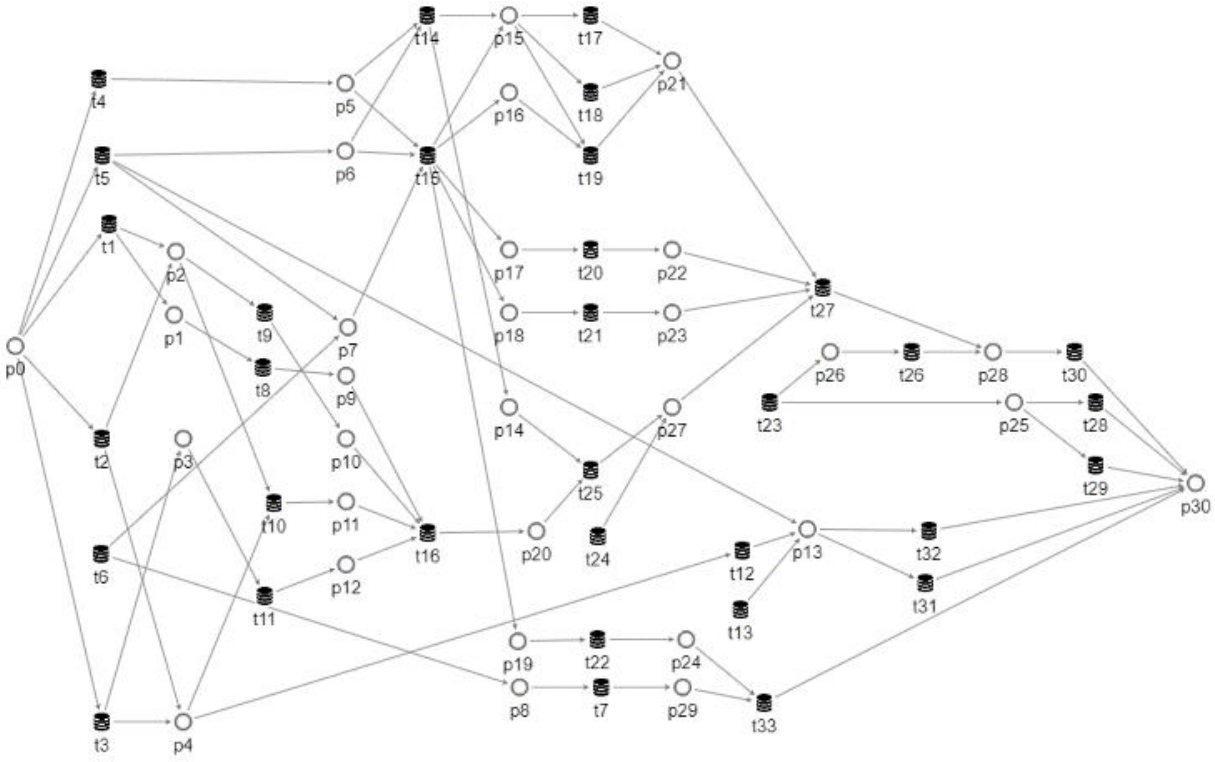

Рис. 2. Модель сценария подготовки к компьютерной атаке на РКС

Сеть Петри, представляющая данную модель, включает следующие позиции и переходы:

−T1 – поиск по социальным сетям (T1593.001);

−T2 – поиск по открытым веб-сайтам (T1593.002);

−T3 – поиск на сайтах, принадлежащим пользователям (T1594);

−T4 – поиск в открытых технических базах данных CDN (T1596.004);

−T5 – сканирование открытых технических баз данных (T1596.005);

−T6 – поиск в открытых технических базах данных WHOIS (T1596.002);

−T7 – поиск в открытых технических баз данных DNS (T1596.005);

−T8 – взлом учетных записей пользователя в социальных сетях(T1586.001);

−T9 – регистрация учетных записей в социальных сетях(T1585.001);

−T10 – регистрация учетных записей электронной почты (T1585.002);

−T11 – взлом учетных записей электронной почты пользователя (T1586.002);

−T12 – поиск в открытых технических базах данных цифровых сертификатов (T1596.003);

−T13 – сбор информации об организации пользователя (T1591);

−T14 – активное сканирование уязвимостей (T1595.002);

−T15 – активное сканирование IP-блоков (T1595.001);

−T16 – фишинг для получения информации (T1598);

−T17 – сбор информации об оборудовании узлов сети (T1592.001);

−T18 – сбор информации о программном обеспечении, установленном на узлах сети (T1592.001);

−T19 – сбор информации о конфигурации узлов сети (T1592.003);

−T20 – сбор информации о средствах защиты периметра РКС (T1590.006);

− T21 – сбор информации об аппаратных средствах защиты периметра РКС (T1590.004);

−T22 – сбор информации о сети пользователя: свойства домена (T1590.001);

−T23 – поиск в закрытых источниках (T1597.002);

−T24 – покупка эксплойтов (T1588.005);

−T25 – разработка эксплойта (T1587.004);

−T26 – покупка вредоносного ПО (T1588.001);

−T27 – разработка вредоносного ПО (T1587.001);

−T28 – покупка сертификата подписи кода (T1588.003);

−T29 – покупка сертификата SLL (T1588.004);

−T30 – применение подготовленного программного кода в качестве программного инструмента (T1587);

−T31 – создание сертификата подписи кода (T1587.002);

−T32 – создание сертификата подписи кода (T1587.003);

−T33 – взлом сторонних DNS-серверов (T1583.002);

−P0 – злоумышленник начал атаку;

−P1 – найдены утечки конфиденциальной информации;

−P2 – найдены учетные записи жертв в социальных сетях;

−P3 – получены адреса электронных почт пользователя;

−P4 – получена информация:

а) название отделов;

б) физическое местонахождение;

в) данные о ключевых сотрудниках;

−P5 – найдены неверные конфигурации CDN, которые привели к утечке конфиденциальной информации;

−P6 – найдены имена хостов и открытые порты;

−P7 – найдены назначенные IP-блоки и активные IP-адреса;

−P8 – найдены DNS-серверы имен;

−P9 – зарегистрированы правдоподобные учетные записи социальных сетей на основании полученной информации;

−P10 – взломана существующая учетная запись в социальных сетях, к которой у потенциального пользователя есть определенный уровень доверия;

−P11 – зарегистрированы правдоподобные, одноразовые учетные записи электронной почты на основании полученной информации;

−P12 – взломана существующая электронная почта, к которой у потенциального пользователя есть определенный уровень доверия;

−P13 – получен сертификат цифровой подписи доверенного разработчика;

−P14 – получена информация о широко известных уязвимостях;

−P15 – установлена связь с хостом пользователя;

−P16 – просканированы IP-блоки пользователя;

−P17 – найдены необходимые порты пользователя;

−P18 – установлена возможность отправки сетевых пакетов;

−P19 – получена информация о возможных сетевых доменах пользователя;

−P20 - фишинг прошел успешно и найдены необходимые сведения об уязвимостях;

−P21 – получена информация об имеющемся оборудовании;

−P22 – получена информация об устройствах сетевой безопасности;

−P24 – получена информация о свойствах домена;

−P25 – найден продавец необходимых сертификатов;

−P26 – найден продавец вредоносного ПО;

−P27 – подготовлен эксплойт;

−P28 – подготовлен код, внедряемый в информационную систему;

−P29 – получена информация:

а) зарегистрированные имена серверов

б) записи, описывающие адресацию для целевых поддоменов, почтовых адресов и других хостов.

−P30 – начало проведения атаки с использованием взломанных DNS-серверов.

Таким образом, разработав модель сценария подготовки компьютерной атаки в РКС необходимо расширить эту модель добавив средства защиты информации. Основным источником исходных данных средств защиты является методический документ ФСТЭК России «Меры защиты

информации в государственных информационных системах» [20].

В качестве примера будет представлен фрагмент сети Петри, описывающий разработку вредоносного кода нарушителем и моделирование фиксирующих эту атаку средств защиты информации для этого участка (рис. 3).

Переходы и позиции на рис. 3 обозначают следующее:

– D1 – превентивные меры защиты:

а) использование ложных информационных систем;

б) инструктаж и регулярная проверка знаний пользователей в отношении реализации политики безопасности;

– D2 – реализация политики защиты учётных данных:

а) запрет на использование одинаковых паролей для доступа к социальным сетям;

б) повышение грамотности пользователей относительно сложности и правил использования паролей и других учётных данных;

– D3 – использование средств защиты от фишинга;

– D4 – выявление, анализ и устранение уязвимостей РКС:

а) проверка программного обеспечения, специализированного ПО, средств защиты информации и технических средств на правильность установки и наличия уязвимостей, а также на корректность работы СЗИ при взаимодействии с техническими средствами. Проверку требуется проводить регулярно в режиме реального времени;

б) в качестве источника информации об уязвимостях необходимо использовать базы данных о широко известных уязвимостях и отчеты антивирусных компаний;

в) анализ уязвимостей и разработка мер по их устранению на основании результатов проверки п. а);

г) устранение уязвимостей с использованием мер из п. б);
если уязвимость невозможно устранить путем установки средств защиты;

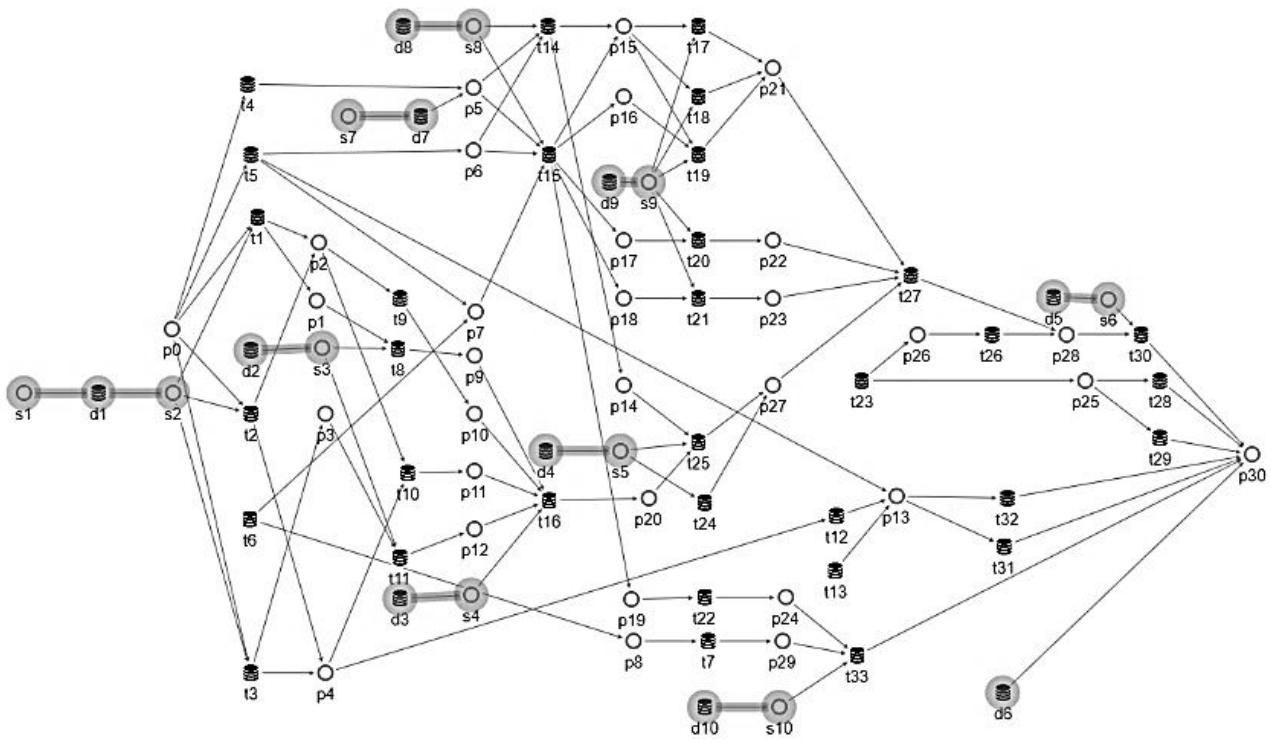

Рис. 3. Модель разработки вредоносного кода, внедряемого в систему и выработанные средства защиты

д) информации, то необходимо отказаться от использования данного фрагмента РКС;

– S4 – организация регулярно выполняет проверку, анализ и устранение угроз в РКС;

– D5 – реализация антивирусной защиты:

а) приобретение организацией актуальных средств антивирусной защиты;

б) применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, средствах защиты периметра РКС (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в РКС;

в) периодические проверки всех элементов РКС на наличие вредоносного ПО;

г) предоставление доступа средствам антивирусной защиты ко всем элементам РКС, на которые потенциально возможно внедрение вредоносного ПО;

д) оповещение отдела безопасности информации об обнаружении вредоносного ПО в элементах РКС. После этого необходима проверка всей системы;

е) информационная система должна обеспечиваться актуальной базой данных о существующих разновидностях и версиях вредоносного ПО;

ж) запрет вноса съемных информационных носителей в здание организации, без полной проверки в отделе по обеспечению информационной безопасности;

– S5 – организация и сотрудники выполняют весь перечень правил, связанный с реализацией антивирусной защиты.

Разработав модель сценария подготовки компьютерной атаки в РКС с выработанными средствами защиты, становится возможным расширение до сетей Петри-Маркова путем наложения вероятностно-временных характеристик.

Расчет риска можно представить в виде трех этапов:

– построение модели причинно-следственных связей между действиями, совершаемыми злоумышленником в ходе подготовки к реализации атаки на РКС при помощи аппарата сетей Петри;

– наложение на построенную модель методики расчета частных показателей вероятностей переходов, путем расширения модели до сети Петри-Маркова, добавив вероятностно-временные характеристики;

– расчет риска, который представлен формулой:

$$R(t) = P(t) * U(t)$$

где *R(t)* - риск;

P(t) – вероятность реализации компьютерной атаки за время *t*;

U(t) – ущерб, наносимый нарушителем в ходе реализации компьютерной атаки за время *t*.

Рассчитать ущерб в рамках данной статьи не представляется возможным, так как для его оценки необходимо знать информационную систему и ценность информации в ней.

Для оценки вероятности можно использовать несколько разных подходов:

- эпидемиологический подход, позволяющий оценить вероятность распространения вредоносного ПО (подход направлен только лишь на вирусные атаки и не учитывает способы, реализуемые внутри атакованного компьютера, например, действия нарушителя по повышению привилегий внутри узла) [20];
- подход расчёта вероятности конкретных атак, основанный на статистике по уязвимостям, связанным с такими атаками (такой подход не позволяет получить точные оценки, а также упускает из вида ресурсы нарушителя, не учитывает связи между его действиями [21]).

В настоящей работе использован ресурсно-временной подход, в рамках которого моделирование сценария подготовки атаки и возможных действий нарушителей осуществляется с учетом их причинно-следственных связей, а также вероятностно-временных характеристик, зависящих как от наличия у нарушителя определённых знаний, навыков, информационных и вычислительных

ресурсов, так и от параметров защищаемой системы. средств защиты информации. Такой подход позволяет не только связать элементы сценария нарушителя с мерами защиты от них, но и количественно оценивать риски, связанные с реализацией того или иного сценария.

Для расчета вероятности Ф переходов необходимо использовать систему уравнений [11]:

$$\Phi_{ij}(d,t) = \pi_{ik}(d) \cdot \int_0^t f_{ik}(d,\tau) \times \times P_{kj}(d, t-\tau) \cdot d\tau$$

где $\Phi_{ij}(d,t)$ — вероятность перемещения процесса по траектории d за время t из позиции с номером i в переход с номером j.

$f_{ik}(d,\tau)$ — плотность распределения вероятностей времени перемещения процесса по траектории d из i -й позиции в k -й переход.

$\pi_{ik}(d)$ — вероятность того, что процесс пойдет по дуге, соединяющей i -ю позицию с k -м переходом, находящимся на траектории d.

Заключение

Основными полученными результатами являются:

– модель способов подготовки компьютерных атак в РКС с учетом выявленных причинно-следственных связей между техническими приемами PRE ATT&CK;

– модель мер защиты от угроз безопасности информации для сценария подготовки компьютерных атак на РКС.

При этом новизна работы заключается в использовании аппарата сетей Петри для моделирования способов подготовки к реализации компьютерной атаки, а также мер защиты от них, на основании сведений о соответствующих технических приёмах стандарта ATT&CK.

Перспективным направлением настоящего исследования является определение вероятностно-временных характеристик участков построенной модели с целью преобразования сети Петри в сеть Петри-Маркова и расчёт вероятности достижения определённых позиций сети Петри. На основе результатов исследования планируется разработка системы поддержки принятия решений, которая позволит, основываясь на вероятностях достижения определённых позиций сети Петри количественно оценить возможный эффект применения мер защиты, что позволит обосновать эффективность применения того или иного средства защиты информации от актуального множества угроз, реализуемого при помощи разработанных сценариев реализации подготовки к компьютерной атаке.

Список литературы

1. Современные угрозы в информационных системах. URL: https://www.infowatch.ru/sites/default/files/docs/pamyatka_sovremenye_ugrozi_IW.pdf (дата обращения 28.04.2021).

2. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. М.: Дашков и Ко., 2006. 336 с.

3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002. 656 с.

4. Федотов А.М. Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций. М.: ВИНИТИ, 2008. № 2. С. 88–101.

5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В. Ф. Шаньгин. М.: ИНФРА-М, 2010. 592 с.

6. Климова С.М., Сычев М.П., Астрахов А.В. Противодействие компьютерным атакам. Технологические основы. URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-exp.pdf (дата обращения 28.04.2021).

7. Климов С.М., Сычев М.П., Астрахов А.В. Противодействие компьютерным атакам. URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-exp.pdf (дата обращения 28.04.2021).

8. Климов С.М., Сычёв М.П., Астрахов А.В. Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне. URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-exp.pdf (дата обращения 28.04.2021).

9. Артюхов Ю.В. Некоторые аспекты информационной безопасности в распределенной компьютерной системе / Ю.В. Артюхов. // Молодой ученый. 2011. № 2 (25). Т.1. С.60-62.

10. Андрончик А.Н. Защита информации в компьютерных сетях. / А. Н. Андрончик; под ред. Н. И. Синадского. Екатеринбург: УГТУ-УПИ, 2008. 248 с.

11. Ю.К. Язов, О.С. Авсентьев, А.О. Авсентьев, И.О. Рубцова. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри-Маркова. // Тр. СПИИРАН. 2019. Вып. 18. Т.6. С. 1269-1300.

12. Ивутин А.Н., Страхов И.А. Фреймворк для построения и исследования сетей Петри и их модификаций // Известия ТулГУ, серия Технические науки. 2013. Вып.9. Ч. 2. С.135-140.

13. 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.

14. 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.

15. 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.

16. Информационный ресурс MITER ATT & CK. URL: https://blog.tiger-optics.ru/2018/12/what-is-mitre-attack (дата обращения 28.04.2021).

17. MITRE ATT&CK Matrix for Enterprise covering preparatory techniques. URL: https://attack.mitre.org/matrices/enterprise/pre (дата обращения 28.04.2021).

18. MITRE ATT&CK Matrix for Reconnaissance. URL: https://attack.mitre.org/tactics/TA0043 (дата обращения 28.04.2021).

19. MITREATT&CK MatrixforResourceDevelopment. URL: https://attack.mitre.org/tactics/TA0042 (дата обращения 28.04.2021).

20. Меры защиты информации в государственных информационных системах / ФСТЭК России – 2020. URL: https://fstec.ru/component/attachments/download/675 (дата обращения 28.04.2021).

21. Остапенко А.Г. Эпидемии в телекоммуникационных сетях: монография / А.Г. Остапенко [и др.] М.: Горячая линия – Телеком, 2017. 282 с.

22. Risk Assessment Method for Cyber Security of Cyber Physical Systems. – URL: https://sci-hub.do/10.1109/ICRSE.2015.7366430/ (дата обращения 28.04.2021).

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 29.04.2021

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

Пустовалов Никита Сергеевич – студент, Воронежский государственный технический университет, e-mail: mike6845@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

Дешина Анна Евгеньевна – канд. техн. наук, старший преподаватель, Воронежский государственный технический университет, e-mail: 2199199@mail.ru

A.L. Serdechnyy, N.S. Pustovalov, M.A. Tarelkin, A.E. Deshina

MODELING, ANALYSIS AND COUNTERING THE SCENARIOS OF PREPARING COMPUTER ATTACKS IN DISTRIBUTED COMPUTER SYSTEMS

The purpose of the research was to formalize the actions of the violator committed during the preparation of a computer attack as the main stage at which it is possible to counteract the violator before the protected system is damaged. This article presents the results of the development of a Petri net model for the preparation stage for a computer attack in distributed computer systems. The model takes into account the causal relationships between the actions of the violator, as well as the conditions and consequences of the implementation of such actions. The presence of such links allows you to determine the scenarios for preparing computer attacks, depending on the structural and functional features of the object of protection and the model of the intruder. The developed model can be used as a source data for modeling information security threats in terms of determining the methods used by the violator when choosing the object of the attack, as well as in the course of obtaining the necessary resources for its commission. This article also demonstrates the possibility of modeling security measures that make it difficult to implement a scenario for an attack.

Keywords: Petri net, ATT&CK, computer attack preparation, simulation.

Submitted 29.04.2021

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

Nikita S. Pustovalov – Student, Voronezh State Technical University, email: mike6845@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 E. Deshina – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: 2199199@mail.ru