УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2021 Том 21 № 5 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2021 Vol. 21 No 5 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

COMPUTER SCIENCE

doi: 10.17586/2226-1494-2021-21-5-694-701
УДК 621.3; УДК 004.056

Методика эксперимента для оценивания вероятности и опасности реализации сетевых атак в автоматизированных системах

Ирина Григорьевна Дровникова[1], Елена Сергеевна Овчинникова[2], Антон Дмитриевич Попов[3], Илья Иосифович Лившиц[4]✉, Олег Олегович Басов[5], Евгений Алексеевич Рогозин[6]

[1,2,3,6] Воронежский институт МВД России, Воронеж, 394065, Российская Федерация
[4,5] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2] yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[3] anton.holmes@mail.ru, https://orcid.org/0000-0002-6583-102X
[4] livshitz.il@yandex.ru✉, https://orcid.org/0000-0003-0651-8591
[5] oobasov@mail.ru, https://orcid.org/0000-0001-5788-4845
[6] evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Аннотация

Предмет исследования. Разработана новая методика проведения эксперимента для оценивания динамики протекания информационного конфликта «Сетевая атака — Система защиты» в автоматизированных системах. В результате применения методики получены количественные значения исходных данных, необходимые для оценки вероятности и опасности реализации сетевых атак в автоматизированных системах. **Метод.** Метод исследования — эксперимент отображения динамики информационного конфликта «Сетевая атака — Система защиты» в автоматизированных системах. **Основные результаты.** Разработана методика для определения количественных значений характеристик, а также размера ущерба от типовых сетевых атак, которые воздействуют на элементы автоматизированных систем. **Практическая значимость.** Использование полученных результатов позволяет в динамике наблюдать протекание информационного конфликта «Сетевая атака — Система защиты», выполнить расчет вероятностно-временных характеристик реализации сетевых атак и осуществить точную количественную оценку опасности их реализации в автоматизированных системах в программных средах «CPN Tools» и MathCad. Перспективы использования полученных результатов связаны с построением частных моделей актуальных атак и повышением степени устойчивости автоматизированных систем.

Ключевые слова

эксперимент, автоматизированная система, сетевая атака, система защиты информации, информационный конфликт, вероятность реализации сетевой атаки, опасность реализации сетевой атаки, количественная оценка

Ссылка для цитирования: Дровникова И.Г., Овчинникова Е.С., Попов А.Д., Лившиц И.И., Басов О.О., Рогозин Е.А. Методика эксперимента для оценивания вероятности и опасности реализации сетевых атак в автоматизированных системах // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 5. С. 694–701. doi: 10.17586/2226-1494-2021-21-5-694-701

An experimental methodology for assessing the probability and danger of network attacks in automated systems

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2], Anton D. Popov[3], Ilya I. Livshitz[4]✉, Oleg O. Basov[5], Evgeniy A. Rogozin[6]

[1,2,3,6] Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, 394065, Russian Federation
[4,5] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2] yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[3] anton.holmes@mail.ru, https://orcid.org/0000-0002-6583-102X
[4] livshitz.il@yandex.ru✉, https://orcid.org/0000-0003-0651-8591
[5] oobasov@mail.ru, https://orcid.org/0000-0001-5788-4845
[6] evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Abstract

The paper proposes a new method of conducting an experiment to assess the dynamics of the information conflict "Network attack – Protection system" in automated systems. As a result of the application of the methodology, quantitative values of the initial data necessary for assessing the probability and danger of network attacks in automated systems were obtained. The research method implied an experiment that displayed the dynamics of the information conflict "Network attack – Protection system" in automated systems. The authors developed a methodology to determine the quantitative values of the characteristics, as well as the amount of damage from standard network attacks that affect the elements of automated systems. The use of the results makes it possible to observe the course of the information conflict "Network attack – Protection System" in dynamics, to calculate the probabilistic and temporal characteristics of network attacks and to carry out an accurate quantitative assessment of the danger of their implementation in automated systems in the "CPN Tools" and MathCad software environments. The prospects for using the obtained results deal with the construction of particular models of actual attacks and increase of stability of automated systems.

Keywords

experiment, automated system, network attack, information protection system, information conflict, probability of a network attack, danger of a network attack, quantitative assessment

For citation: Drovnikova I.G., Ovchinnikova E.S., Popov A.D., Livshitz I.I., Basov O.O., Rogozin E.A. An experimental methodology for assessing the probability and danger of network attacks in automated systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 5, pp. 694–701 (in Russian). doi: 10.17586/2226-1494-2021-21-5-694-701

Введение

Обеспечение эффективного функционирования современных автоматизированных систем (АС), приводит к необходимости учета возможной опасности реализации сетевых атак для соответствующих элементов [1]. Это предполагает проведение точной количественной оценки опасности и построение частной модели актуальных атак для конкретной АС еще на начальных этапах ее разработки. Получение точных количественных оценок требует, в свою очередь, научного осмысления процесса функционирования защищенных АС в условиях реализации сетевых атак, что предполагает моделирование динамики их реализации в указанных системах и оценивания степени устойчивости [2, 3].

Анализ открытых научных работ, посвященных данной проблеме, позволяет констатировать, что предлагаемые в большинстве из них формальные модели — статические, позволяющие проводить лишь качественную оценку опасности реализации сетевых атак, не обеспечивающую достаточную точность оценивания [4–8]. Немногочисленные научные труды, рассматривающие динамические модели злоумышленного удаленного доступа и предлагающие проведение количественной оценки опасности [9, 10], являются теоретически интересными, но недостаточно обеспечивающими практическую реализацию сетевых атак в современных и перспективных АС. Важно отметить то обстоятельство, что кроме научного интереса, задача оценивания сетевых атак совместно с практической работой по выявлению мер противодействий представляет важный этап обучения студентов (курсантов) по соответствующим специальностям.

В настоящей работе предложена методика проведения эксперимента по исследованию динамики конфликтного взаимодействия сетевых атак с системой защиты информации (СЗИ), и представлены результаты ее реализации для типовых сетевых атак в защищенных АС. Полученные результаты могут быть использованы в качестве исходных данных при проведении экспериментов для определения вероятностно-временных характеристик типовых сетевых атак, выполнении точной количественной оценки опасности реализации сетевых атак в защищенных АС на основе разработанных моделей динамики информационного конфликта «Сетевая атака — Система защиты» [11, 12].

Новизна представленного подхода заключается в применении новой динамической модели, предоставляющей количественные оценки опасности реализации сетевых атак с заданной точностью и оценивания устойчивости к воздействию указанных атак.

Постановка задачи

Целью проведения эксперимента, описывающего процесс взаимодействия сетевой атаки и СЗИ, является определение количественных значений необходимых исходных данных для дальнейшего проведения экспе-

римента. Эксперимент позволит: в динамике наблюдать протекание информационного конфликта «Сетевая атака — Система защиты» в АС; рассчитать вероятности и провести точную количественную оценку опасности реализации типовых сетевых атак в защищенных АС; оценить степень устойчивости к воздействию типовых сетевых атак.

В соответствии с исходными данными, требующими определения в процессе проведения эксперимента, сформулированы его основные задачи:

— определение объема памяти, производительности и временных характеристик, характеризующих реализацию типовых сетевых атак, воздействующих на элементы защищенных АС;
— определение объема памяти, производительности и временных характеристик, требуемых для функционирования СЗИ в условиях реализации типовых сетевых атак в АС;
— определение размеров ущерба от реализации типовых сетевых атак в защищенных АС.

Определение субъектов конфликтного взаимодействия

Объект исследования при проведении эксперимента — динамика конфликтного взаимодействия сетевой атаки и СЗИ в процессе реализации атаки в защищенной АС. Для проведения эксперимента выбраны 8 типов сетевых атак, наиболее часто реализуемых в настоящее время в защищенных АС [13]. В качестве СЗИ рассмотрена «Dallas Lock 8.0-C»[1], которая является сертифицированным в Российской Федерации (РФ) программным комплексом защиты конфиденциальной информации.

Сценарий проведения эксперимента

Очевидно, что АС, эксплуатируемые в защищенном исполнении, например, на объектах информатизации органов внутренних дел РФ, отличаются своим предназначением, а следовательно, и структурой (используемое программное обеспечение, вычислительные ресурсы и др.). В связи с этим существуют различные подходы к преодолению известных СЗИ. Рассмотрим общую методику решения поставленных задач для варианта реализации структуры АС в виде простейшей локальной компьютерной сети, которая может быть интегрирована в новые перспективные модели АС с различными характеристиками используемых и перспективных СЗИ. На рисунке представлен сценарий проведения эксперимента в виде структурной схемы с обозначением его основных этапов (термин «ОВД» означает «Органы внутренних дел»).

[1] Система защиты информации от несанкционированного доступа «Dallas Lock 8.0». Руководство по эксплуатации [Электронный ресурс]. Режим доступа: https://dallaslock.ru/upload/medialibrary/cp/documents/C%20ИК5%202017/RU.48957919.501410-02%2092%20Руководство%20по%20эксплуатации.pdf. Яз.рус. (дата обращения: 27.08.2021).

Рисунок. Сценарий проведения эксперимента

Figure. Scenario for conducting an experiment

Характеристика этапов проведения эксперимента и его результаты

1 этап. Для создания АС в виде локальной компьютерной сети топологии «звезда» создан лабораторный стенд, состоящий из сервера и трех автоматизированных рабочих мест со следующими характеристиками: процессор Intel Core i3-2100 с тактовой частотой 3.1 ГГц, оперативная память (ОЗУ) 4 ГБ, дисковая память (HDD) 500 ГБ, функционирующими под управлением 32-разрядной операционной системой (ОС) Windows 7. Вне локальной сети на отдельном персональном компьютере установлена ОС Kali Linux с целью реализации деструктивных воздействий в виде сетевых атак.

Инсталляция СЗИ в АС основывалась на рекомендациях разработчика. При этом была собрана полная версия СЗИ на трех автоматизированных рабочих местах, и совместно с нею установлено прикладное программное обеспечение в виде пакета Microsoft Office 13 и антивируса «Kaspersky». В рамках эксперимента произведена настройка СЗИ согласно технической документации [14]. Отметим, что не существует принципиального отличия этапов настройки различных типов СЗИ. Отличия заключаются в интерфейсе, программной реализации компонентов СЗИ и их составе в рамках концепции разработчика.

2 этап. Тактика реализации типовых сетевых атак заключалась в проведении поэтапного воздействия и, следовательно, в осуществлении последовательной реализации этапов каждой атаки в виде последовательности выполнения всех деструктивных функций в соответствии с ранее разработанной ее графовой моделью [14]. Практическая составляющая поэтапного удаленного несанкционированного доступа к элементам защищенной АС реализовалась в виде скриптов, написанных на языке Bash. Запуск данных скриптов производился с персонального компьютера, функционирующего под управлением ОС Kali Linux, посредством разработанного для каждого типа атаки программного кода.

3 этап. На данном этапе определялись параметры (объем памяти, время запуска, оценка производительности, время выполнения вредоносных функций), характеризующие реализацию конкретной атаки. В частности, объем требуемой памяти при реализации сетевой атаки рассматривается как количество информации, «отвлекаемой» из оперативной памяти АС, используемой для инициирования данной атаки. Под оценкой производительности понимается количество информации, «отвлекаемой» в единицу времени на запуск атаки из оперативной памяти АС, используемой для инициирования данной атаки соответственно. Для фиксации времени запуска каждой из сетевых атак использован исполняемый файл в виде скрипта, предназначенный для мониторинга в масштабе реального времени всех процессов в оперативной памяти в ОС семейств «Windows» и «Linux». Эмпирические значения объема памяти и времени запуска типовых сетевых атак, а также расчетные значения их производительности, полученные на основе эмпирических данных, представлены в табл. 1.

После запуска типовых сетевых атак работа пользователя имитируется путем осуществления стандартных манипуляций с файлами и папками в АС. Эти действия необходимы для того, чтобы задействовать все механизмы защиты и зафиксировать выполнение вредоносных функций несанкционированного доступа в защищенной АС. Сбор статистических данных в виде соответствующего времени реализации типовых сетевых атак в защищенной АС осуществляется на основе их графовых моделей [14]. Для фиксации временных характеристик при реализации конкретных атак применяется разработанный исполняемый файл (скрипт). Полученные результаты представлены в табл. 2.

4 этап. На данном этапе оценивается влияние СЗИ на загрузку вычислительного ресурса АС, т. е. определяется объем памяти и производительность СЗИ. Заметим, что при установке СЗИ существенно увеличилось время загрузки вычислительного ресурса АС, что объективно объясняется «отвлечением» конечного размера вычислительных ресурсов АС на загрузку конкретного типа СЗИ. Под объемом памяти СЗИ понимается количество информации, «отвлекаемой» из оперативной памяти защищаемой АС, на загрузку СЗИ при нормальной загрузке данного ресурса АС.

Таблица 1. Значения объема памяти, времен запуска и производительности типовых сетевых атак в автоматизированных системах

Table 1. Values of memory volumes, startup times, and performance of typical network attacks in an automated system

Тип сетевой атаки	Объем памяти сетевой атаки, КБ	Время запуска сетевой атаки, с	Производительность сетевой атаки, КБ/с
Сканирование сети	3388	0,137	24 729,93
Анализ сетевого трафика (сниффинг пакетов)	16 212	16,420	987,33
Парольная атака	3456	15,160	227,97
Подмена доверенного объекта сети (IP-spoofing)	3616	252,306	14,33
Навязывание ложного маршрута	3444	0,502	6860,56
Внедрение ложного объекта сети (ARP-spoofing)	3516	44,581	78,87
Отказ в обслуживании» (SYN-flood)	3248	13,792	235,50
Удаленный запуск приложений (IP-hijacking)	3576	62,420	57,29

Таблица 2. Эмпирические значения временных характеристик реализации типовых сетевых атак в защищенной автоматизированной системе

Table 2. Empirical values of the time characteristics for the implementation of standard network attacks in a protected automated system

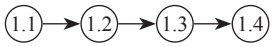
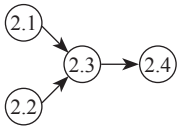
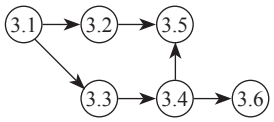
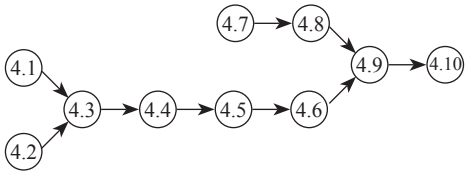
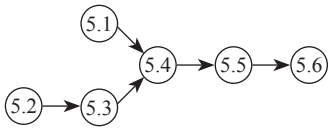
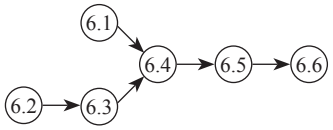
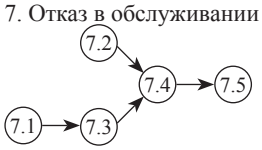
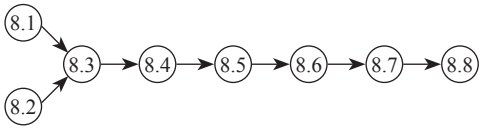
Тип сетевой атаки и граф динамики ее реализации	Вредоносные функции, выполняемые сетевой атакой	Время, с
1. Сканирование сети 	1.1. Готовность хоста злоумышленника, настройка и запуск программы 1.2. Определение активных хостов сети при помощи ICMP-запроса (запроса по протоколу Internet Control Message Protocol) 1.3. Определение типов ОС активных хостов сети 1.4. Сканирование сервисов на активных хостах сети	1 15 3 1
2. Анализ сетевого трафика (сниффинг пакетов) 	2.1. Готовность атакуемых хостов 2.2. Физическая готовность хоста злоумышленника к перехвату трафика 2.3. Передача пакета между атакуемыми хостами, перехват пакета 2.4. Анализ пакета, извлечение из него полезных данных (пароля, имени пользователя)	2 2 21 57
3. Парольная атака 	3.1. Готовность хоста злоумышленника, включение его в сеть общего пользования 3.2. Запрос пароля атакуемым хостом 3.3. Подбор пароля, не знающим его хостом злоумышленника, по специальному словарю или путем прямого перебора 3.4. Завершение подбора пароля хостом злоумышленника 3.5. Осуществление несанкционированного доступа к атакуемому хосту в случае правильного подбора пароля 3.6. Срыв атаки в случае неправильного подбора пароля	1 5 5 450 300 0
4. Подмена доверенного объекта сети (IP-spoofing) 	4.1. Готовность атакуемого хоста 4.2. Готовность хоста злоумышленника к проведению атаки SYN-flood и ожидание перезагрузки атакуемого хоста 4.3. Перезагрузка атакуемого хоста (в результате атаки SYN-flood или самопроизвольная), недоступность атакуемого хоста 4.4. Отправка C-SYN и обработка его сервером 4.5. Прием S-SYN хостом злоумышленника 4.6. Отправка C-SYN2 от имени атакуемого хоста и обработка его сервером 4.7. Готовность хоста злоумышленника к подбору S-ACK2 4.8. Подбор S-ACK2 хостом злоумышленника 4.9. Отправка подходящего S-ACK2 и его принятие, установка соединения с правами атакуемого хоста 4.10. Отправка данных, результат — выполнение сервером команды злоумышленника	1 1 2 4 25 2 1 19 9 21
5. Навязывание ложного маршрута 	5.1. Готовность атакуемого хоста 5.2. Активность злоумышленника 5.3. Настройка программы 5.4. Передача на атакуемый хост и принятие им ложных ICMP-redirect-сообщений 5.5. Изменение таблицы маршрутизации атакуемого хоста 5.6. Перехват и анализ трафика атакуемого хоста (для внутрисегментной атаки)	1 1 116 35 72 80
6. Внедрение ложного объекта сети (ARP-spoofing) 	6.1. Формирование атакуемым хостом широковещательного ARP-запроса 6.2. Нахождение хоста злоумышленника внутри сегмента сети атакуемого хоста 6.3. Подготовка хоста злоумышленника к проведению атаки (сканирование MAC-адресов хостов сети и настройка программы) 6.4. Отправка ложного ARP-ответа и принятие его атакуемым хостом 6.5. Изменение ARP-таблицы атакуемого хоста 6.6. Перехват и анализ трафика атакуемого хоста	1 1 5 27 4 15

Таблица 2. Продолжение

7. Отказ в обслуживании (SYN-flood) 	7.1. Готовность хоста злоумышленника 7.2. Готовность атакуемого хоста принять SYN-пакеты с несуществующим обратным адресом в очередь неоткрытых соединений 7.3. Запуск и настройка программы для SYN-flood 7.4. Отправка SYN-пакетов и постановка их в очередь атакуемому хосту 7.5. Переполнение очереди атакуемого хоста, когда он не в состоянии обрабатывать другие запросы	1 1 12 15 52
8. Удаленный запуск приложений (IP-hijacking) 	8.1. Готовность атакуемых хостов 8.2. Готовность хоста злоумышленника к перехвату трафика 8.3. Обмен пакетами между атакуемыми хостами для установления соединения, перехват S-SYN и C-ACK 8.4. Отправка RST от имени второго атакуемого хоста, закрытие соединения между атакуемыми хостами для первого из них 8.5. Отправка первым атакуемым хостом S-SYN2 для второго хоста, перехват S-SYN2, обработка первым атакуемым хостом C-SYN2 8.6. Отправка C-SYN2 от имени второго атакуемого хоста, перехват S-SYN2, возникновение ACK-бури между атакуемыми хостами 8.7. Отправка S-ACK2 от имени второго атакуемого хоста, принятие S-ACK2, установка соединения с правами второго атакуемого хоста 8.8. Обмен модифицированными данными со вторым атакуемым хостом по ACK, с первым — по ACK-2	1 1 5 2 35 11 3 13

Соответственно, производительность СЗИ рассматривается как количество информации, «отвлекаемой» в единицу времени из оперативной памяти защищаемой АС. Значения объема памяти и времени загрузки СЗИ (изменения времени загрузки) определялись при помощи программного продукта «Process Monitor», предназначенного для наблюдения в реальном масштабе времени за протеканием различных процессов в ОС семейства «Windows». Представлены эмпирические значения объема памяти 9928 КБ и времени загрузки 1,7 с СЗИ «Dallas Lock 8.0-C» в АС, а также полученное на их основе расчетное значение производительности 5840 КБ/с системы защиты.

После загрузки СЗИ имитируется работа пользователя (табл. 1), чтобы задействовать все механизмы защиты и зафиксировать их выполнение в процессе противодействия СЗИ реализации сетевых атак. Сбор эмпирических данных в виде времени функционирования (выполнения защитных функций) СЗИ применительно к реализации каждой из рассматриваемых типовых сетевых атак в АС осуществляется на основе вербальной модели системы защиты. Модель получена путем анализа руководящей документации по эксплуатации СЗИ «Dallas Lock 8.0-C»[1]. Для фиксации времени функционирования СЗИ использован программный

[1] Система защиты информации от несанкционированного доступа «Dallas Lock 8.0». Руководство по эксплуатации [Электронный ресурс]. Режим доступа: https://dallaslock.ru/upload/medialibrary/cp/documents/C%20ИК5%202017/RU.48957919.501410-02%2092%20Руководство%20по%20эксплуатации.pdf. Яз.рус. (дата обращения: 27.08.2021).

Таблица 3. Эмпирические значения времени функционирования средств защиты информации в условиях реализации типовых сетевых атак в автоматизированных системах

Table 3. Empirical values of operating time for the security protection system during the implementation of standard network attacks in an automated system

Тип сетевой атаки	Время реализации сетевой атаки, с	Время функционирования СЗИ, с
Сканирование сети	20	34,507*
Анализ сетевого трафика (сниффинг пакетов)	80	92,311*
Парольная атака	756	913,623*
Подмена доверенного объекта сети (IP-spoofing)	64	302,340**
Навязывание ложного маршрута	304	323,067**
Внедрение ложного объекта сети (ARP-spoofing)	52	60,712**
Отказ в обслуживании (SYN-flood)	80	289,34*
Удаленный запуск приложений (IP-hijacking)	70	81,23**

*Сетевая атака реализована частично (на сервер).
** Сетевая атака реализована полностью (на всю локальную сеть).

Таблица 4. Эмпирические значения размеров ущерба от реализации типовых сетевых атак в автоматизированных системах
Table 4. Empirical values of the amount of damage caused by the implementation of standard network attacks in an automated system

Тип сетевой атаки	Предельно допустимый размер ущерба, ГБ	Размер ущерба от реализации сетевой атаки, ГБ	Размер суммарного ущерба от реализации сетевых атак, ГБ
Сканирование сети	1720	2	1570
Анализ сетевого трафика (сниффинг пакетов)		560	
Парольная атака		980	
Подмена доверенного объекта сети (IP-spoofing)		1100	
Навязывание ложного маршрута		300	
Внедрение ложного объекта сети (ARP-spoofing)		500	
Отказ в обслуживании» (SYN-flood)		80	
Удаленный запуск приложений (IP-hijacking)		1380	

продукт «Process Monitor». Полученные результаты представлены в табл. 3.

5 этап. Предельно допустимый размер ущерба, который можно нанести вычислительным ресурсам АС реализацией деструктивного воздействия, приравнен к общему количеству обрабатываемой в системе служебной информации, хранящейся на жестких дисках АС (сервера и автоматизированных рабочих мест). Размер ущерба ресурсам АС, нанесенного сетевой атакой, соответствует уменьшению количества информации на жестких дисках в результате действия атаки. При этом время воздействия сетевой атаки после ее реализации в защищенной АС, определяемое инициативой злоумышленника, составило 2 ч. Полученные эмпирические результаты размеров ущерба от реализации типовых сетевых атак при их воздействии на элементы АС, представлены в табл. 4.

Заключение

В работе представлена новая методика проведения эксперимента по исследованию динамики конфликтного взаимодействия сетевых атак и известных средств защиты в автоматизированных системах. В результате применения методики получены эмпирические значения объема памяти, оценки производительности и временные характеристики, требуемые для функционирования средств защиты информации в условиях реализации типовых сетевых атак в автоматизированных системах.

Полученные результаты, а также значения размера нанесенного ущерба могут быть использованы в качестве исходных данных при проведении экспериментов по исследованию процесса реализации сетевых атак в соответствии с разработанными моделями динамики информационного конфликта «Сетевая атака — Система защиты» и алгоритмами в программных средах «CPN Tools» и MathCad.

Результаты эксперимента в виде количественных значений вероятностно-временных характеристик реализации сетевых атак и показателей их опасности являются важной компонентой для формирования частной модели актуальных атак для существующих и перспективных автоматизированных систем, что позволит повысить степень защищенности указанных автоматизированных систем. Полученные результаты существенно дополняют курс лекций по теории и практике защиты от сетевых атак для студентов (курсантов) соответствующих специальностей.

Литература

1. Melnikov D.A., Durakovsky A.P., Dvoryankin S.V., Gorbatov V.S. Concept for increasing security of national information technology infrastructure and private clouds // Proc. 5th International Conference on Future Internet of Things and Cloud (FiCloud 2017). 2017. P. 155–160. https://doi.org/10.1109/FiCloud.2017.11
2. Butusov I.V., Romanov A.A. Methodology of security assessment automated systems as objects critical information infrastructure // Вопросы кибербезопасности. 2018. № 1(25). С. 2–10. https://doi.org/10.21681/2311-3456-2018-1-2-10
3. Kalashnikov A., Sakrutina E. Towards risk potential of significant plants of critical information infrastructure // Proc. of the International Russian Automation Conference (RusAutoCon). 2018. P. 8501644. https://doi.org/10.1109/RUSAUTOCON.2018.8501644
4. Дровникова И.Г., Овчинникова Е.С., Рогозин Е.А. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования // Вестник Воронежского института МВД России. 2019. № 4. С. 51–63.

References

1. Melnikov D.A., Durakovsky A.P., Dvoryankin S.V., Gorbatov V.S. Concept for increasing security of national information technology infrastructure and private clouds. *Proc. 5th International Conference on Future Internet of Things and Cloud (FiCloud 2017)*, 2017, pp. 155–160. https://doi.org/10.1109/FiCloud.2017.11
2. Butusov I.V., Romanov A.A. Methodology of security assessment automated systems as objects critical information infrastructure. *Voprosy kiberbezopasnosti*, 2018, no. 1(25), pp. 2–10. https://doi.org/10.21681/2311-3456-2018-1-2-10
3. Kalashnikov A., Sakrutina E. Towards risk potential of significant plants of critical information infrastructure. *Proc. of the International Russian Automation Conference (RusAutoCon)*, 2018, pp. 8501644. https://doi.org/10.1109/RUSAUTOCON.2018.8501644
4. Drovnikova I.G., Ovchinnikova E.S., Rogozin E.A. Analysis of existing methods and procedures for assessing the risk of network attacks in automated systems of internal affairs bodies and aspects of their improvement. *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2019, no. 4, pp. 51–63. (in Russian)

5. Sher A. Simulation of Attacks in a Wireless Sensor Network using NS2: graduate project report // The School of Engineering & Computing Sciences. Texas A&M University-Corpus Christi. Spring 2015. 49 p.
6. Yao Y., Viswanath B., Cruan J., Zheng H., Zhao B.Y. Automated crowdturfing attacks and defenses in online review systems // Proc. 24th ACM SIGSAC Conference on Computer and Communications Security (CCS 2017). 2017. pp. 1143–1158. https://doi.org/10.1145/3133956.3133990
7. Solic K., Ocevcic H., Golub M. The information systems' security level assessment model based on an ontology and evidential reasoning approach // Computers & Security. 2015. V. 55. P. 100–112. https://doi.org/10.1016/j.cose.2015.08.004
8. Lan Y., Liu S.-P., Lin L., Ma Y.-Y. Effectiveness evaluation on cyberspace security defense system // Proc. of the International Conference on Network and Information Systems for Computers (ICNISC). 2015. P. 576–579. https://doi.org/10.1109/ICNISC.2015.120
9. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. 232 с.
10. Радько Н.М., Язов Ю.К., Корнеева Н.Н. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа: учебное пособие. Воронеж: Воронежский государственный техничический университет, 2013. 265 с.
11. Bokova O.I., Drovnikova I.G., Ovchinnikova E.S., Rodin S.V. Innovative technology in the research of implementation dynamics of network attacks on the digital educational resources // Journal of Physics: Conference Series. 2020. V. 1691. P. 12063. https://doi.org/10.1088/1742-6596/1691/1/012063
12. Дровникова И.Г., Овчинникова Е.С., Рогозин Е.А., Калач А.В. Моделирование динамики информационного конфликта в защищенных автоматизированных системах органов внутренних дел на основе сети Петри-Маркова // Вестник Воронежского института ФСИН России. 2020. № 4. С. 37–44.
13. Дровникова И.Г., Овчинникова Е.С., Конобеевских В.В. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел // Вестник Дагестанского государственного технического университета. Технические науки. 2020. Т. 47. № 1. С. 72–85. https://doi.org/10.21822/2073-6185-2020-47-1-72-85
14. Овчинникова Е.С. Графовые модели динамики реализации сетевых атак в автоматизированных системах органов внутренних дел // Вестник Дагестанского государственного технического университета. Технические науки. 2021. Т. 48. № 1. С. 116–129. https://doi.org/10.21822/2073-6185-2021-48-1-119-129

5. Sher A. *Simulation of Attacks in a Wireless Sensor Network using NS2*. Graduate Project Report. The School of Engineering & Computing Sciences. Texas A&M University-Corpus Christi. Spring 2015, 49 p.
6. Yao Y., Viswanath B., Cruan J., Zheng H., Zhao B.Y. Automated crowdturfing attacks and defenses in online review systems. *Proc. 24th ACM SIGSAC Conference on Computer and Communications Security (CCS 2017)*, 2017, pp. 1143–1158. https://doi.org/10.1145/3133956.3133990
7. Solic K., Ocevcic H., Golub M. The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers & Security*, 2015, vol. 55, pp. 100–112. https://doi.org/10.1016/j.cose.2015.08.004
8. Lan Y., Liu S.-P., Lin L., Ma Y.-Y. Effectiveness evaluation on cyberspace security defense system. *Proc. of the International Conference on Network and Information Systems for Computers (ICNISC)*, 2015, pp. 576–579. https://doi.org/10.1109/ICNISC.2015.120
9. Radko N.M., Skobelev I.O. *Risk-Models of Information and Telecommunication Systems at the Threat of Remote and Direct Access*. Moscow, RadioSoft Publ., 2010, 232 p. (in Russian)
10. Radko N.M., Iazov Iu.K., Korneeva N.N. *Penetration Into the Computer Operating System: Models of Malicious Remote Access*. Voronezh, Voronezh State Technical University Publ., 2013, 265 p. (in Russian)
11. Bokova O.I., Drovnikova I.G., Ovchinnikova E.S., Rodin S.V. Innovative technology in the research of implementation dynamics of network attacks on the digital educational resources. *Journal of Physics: Conference Series*, 2020, vol. 1691, pp. 12063. https://doi.org/10.1088/1742-6596/1691/1/012063
12. Drovnikova I.G., Ovchinnikova E.S., Rogozin E.A., Kalach A.V. Modeling the dynamics of information conflict in secure automated systems of internal affairs bodies based on the Petri-Markov network. *Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service*, 2020, no. 4, pp. 37–44. (in Russian)
13. Drovnikova I.G., Ovchinnikova E.S., Konobeevsky V.V. Analysis of typical network attacks on automated systems of internal affairs departments. *Herald of Daghestan State Technical University. Technical Sciences*, 2020, vol. 47, no. 1, pp. 72–85. (in Russian). https://doi.org/10.21822/2073-6185-2020-47-1-72-85
14. Ovchinnikova E.S. Graph models of the dynamics of network attacks in automated systems of internal affairs bodies. *Herald of Daghestan State Technical University. Technical Sciences*, 2021, vol. 48, no. 1, pp. 116–129. (in Russian). https://doi.org/10.21822/2073-6185-2021-48-1-119-129

Авторы

Дровникова Ирина Григорьевна — доктор технических наук, доцент, профессор, Воронежский институт МВД России, Воронеж, 394065, Российская Федерация, SC 57195219530, https://orcid.org/0000-0001-5265-5875, idrovnikova@mail.ru

Овчинникова Елена Сергеевна — адъюнкт, Воронежский институт МВД России, Воронеж, 394065, Российская Федерация, SC 57221051860, https://orcid.org/0000-0003-4139-9524, yelena_ovchinnikova1@mail.ru

Попов Антон Дмитриевич — кандидат технических наук, преподаватель, Воронежский институт МВД России, Воронеж, 394065, Российская Федерация, SC 57195214635, https://orcid.org/0000-0002-6583-102X, anton.holmes@mail.ru

Лившиц Илья Иосифович — доктор технических наук, профессор практики, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57191569306, https://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Басов Олег Олегович — доктор технических наук, доцент, ординарный профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 16400670700, https://orcid.org/0000-0001-5788-4845, oobasov@mail.ru

Рогозин Евгений Алексеевич — доктор технических наук, профессор, профессор, Воронежский институт МВД России, Воронеж, 394065, Российская Федерация, SC 55579562100, https://orcid.org/0000-0002-4455-7535, evgenirogozin@yandex.ru

Authors

Irina G. Drovnikova — D.Sc., Associate Professor, Professor, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, 394065, Russian Federation, SC 57195219530, https://orcid.org/0000-0001-5265-5875, idrovnikova@mail.ru

Elena S. Ovchinnikova — Postgraduate, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, 394065, Russian Federation, SC 57221051860, https://orcid.org/0000-0003-4139-9524, yelena_ovchinnikova1@mail.ru

Anton D. Popov — PhD, Lecturer, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, 394065, Russian Federation, SC 57195214635, https://orcid.org/0000-0002-6583-102X, anton.holmes@mail.ru

Ilya I. Livshitz — D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57191569306, https://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Oleg O. Basov — D.Sc., Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 16400670700, https://orcid.org/0000-0001-5788-4845, oobasov@mail.ru

Evgeniy A. Rogozin — D.Sc., Full Professor, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, 394065, Russian Federation, SC 55579562100, https://orcid.org/0000-0002-4455-7535, evgenirogozin@yandex.ru

Статья поступила в редакцию 05.06.2021
Одобрена после рецензирования 09.08.2021
Принята к печати 17.09.2021

Received 05.06.2021
Approved after reviewing 09.08.2021
Accepted 17.09.2021