Для цитирования: *Е.С.Овчинникова. Графовые модели динамики реализации сетевых атак в автоматизированных системах органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2021; 48 (1): 119-129. DOI:10.21822/2073-6185-2021-48-1-119- 129*
For citation: *E.S. Ovchinnikova. Graph models of the dynamics of network attacks in automated systems of internal affairs bodies. Herald of Daghestan State Technical University. Technical Sciences. 2021; 48(1): 119-129. (In Russ.) DOI:10.21822/2073-6185-2021-48-1-119-129*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 004.056
DOI:10.21822/2073-6185-2021-48-1-119-129

ГРАФОВЫЕ МОДЕЛИ ДИНАМИКИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Е.С. Овчинникова
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия,

Резюме: Цель. *Важнейшей задачей теории и практики обеспечения информационной безопасности автоматизированных систем при их эксплуатации в защищенном исполнении на объектах информатизации органов внутренних дел является анализ процесса функционирования систем защиты конфиденциального информационного ресурса от несанкционированного доступа в условиях сетевых атак, что предполагает моделирование процесса их реализации и, в первую очередь, разработку графовых моделей динамики реализации основных типов сетевых атак.* ***Метод.*** *Методом решения данной задачи является математическое моделирование процесса реализации сетевых атак в защищенных автоматизированных системах органов внутренних дел посредством построения и описания графовых моделей типовых сетевых атак на конфиденциальный информационный ресурс в динамике их реализации.* ***Результат.*** *На основе анализа типовых сетевых атак на информационный ресурс современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел, разработаны графовые модели данных атак в динамике их реализации с выделением ключевых элементов и функциональных компонентов моделей, идентичных реальным сетевым атакам. Разработанные графовые модели позволяют наглядно представить процесс реализации основных вредоносных функций рассмотренных сетевых атак и учесть предполагаемые действия злоумышленника.* ***Вывод.*** *Результаты проведенного исследования могут быть использованы при разработке имитационных моделей процесса реализации типовых сетевых атак на конфиденциальный информационный ресурс с целью получения вероятностно-временных характеристик в виде времен выполнения каждой атакой вредоносных функций для проведения количественной оценки опасности их реализации. Результаты исследования могут стать основой для формирования частной модели актуальных атак для конкретной АС и обоснования количественных требований к перспективным программным средствам и системам информационной безопасности на объектах информатизации органов внутренних дел в соответствии с требованиями действующей нормативной документации.*

Ключевые слова: *автоматизированная система, система защиты информации, несанкционированный доступ, сетевая атака, графовая модель*

GRAPH MODELS OF THE DYNAMICS OF NETWORK ATTACKS IN AUTOMATED SYSTEMS OF INTERNAL AFFAIRS BODIES

E.S. Ovchinnikova
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov St., Voronezh 394065, Russia

Abstract. Objective. *The most important task of the theory and practice of ensuring the information security of automated systems during their operation in a secure version at the objects of computerization of internal affairs bodies is to analyze the functioning process of systems for protecting confidential information resources from unauthorized access in case of network attacks, which involves modeling the process of their implementation and the development of graph models of the implementation dynamics of the main types of network attacks.* ***Methods****. The method for solving this problem is a mathematical simulation of implementing network attacks in protected automated systems of internal affairs bodies by constructing and describing graph models of typical network attacks on a confidential information resource in the dynamics of their implementation.* ***Results.*** *Based on the analysis of typical network attacks on the information resource of modern automated systems operated in a secure version at the objects of computerization of internal affairs bodies, graph models of these attacks in the dynamics of their implementation were developed, with the allocation of key elements and functional components of models identical to real network attacks. The developed graph models allow visualizing the process of implementing the main malicious functions of the considered network attacks and consider the attacker's alleged actions.* ***Conclusion****. The conducted research results can be used to develop simulation models of typical network attacks on a confidential information resource to obtain probabilistic-temporal characteristics in the form of the execution times of each attack of malicious functions for a quantitative risk assessment of their implementation. This can become the basis for forming a specific model of actual attacks for a specific automated system and substantiating quantitative requirements for promising software and information security systems at the computerization facilities of the internal affairs bodies following the current regulatory documentation requirements.*

Keywords*: automated system, information security system, unauthorized access, network attack, graph model*

Введение. Для предотвращения попыток осуществления удаленного несанкционированного доступа (НСД), реализуемого посредством сетевых атак на конфиденциальный информационный ресурс автоматизированных систем (АС) органов внутренних дел (ОВД), широко используются системы защиты информации (СЗИ) от НСД [1,2]. Разработка и эксплуатация данных систем на объектах информатизации ОВД приводит к необходимости научного осмысления процесса их функционирования в условиях реализации сетевых атак, что, в свою очередь, предполагает моделирование динамики реализации сетевых атак в защищенных АС ОВД [3,4]. Анализ научных работ, посвященных исследованию угроз НСД в АС, показал, что предлагаемые, в большинстве из них, формальные модели являются статическими, позволяющими проводить лишь качественную оценку опасности реализации угроз, не обеспечивающую достаточную точность оценивания [5-9]. Немногочисленные научные труды, исследующие процесс реализации угроз удаленного доступа применительно к элементам информационно-телекоммуникационных систем и предлагающие аналитические модели количественной оценки опасности [10,11], являются теоретически интересными, но недостаточно обеспечивающими практическую реализацию сетевых атак в современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД.

Таким образом, существует объективная необходимость разработки совокупности математических моделей процесса реализации основных (типовых) сетевых атак на информационный ресурс АС, реально эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, что требует, в первую очередь, построения их графовых моделей.

Постановка задачи. Целью исследования является разработка графовых моделей динамики реализации основных типов сетевых атак на информационный ресурс современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД. Разработанные графовые модели послужат основой для дальнейшего создания аналитических и имитационных моделей, которые в отличие от существующих математических моделей позволят исследовать процесс реализации типовых сетевых атак в динамике конфликтного взаимодействия

путем определения вероятностно-временных характеристик (ВВХ) для построения точных количественных оценок опасности их реализации на этапах всего жизненного цикла функционирования защищенных АС ОВД.

Методы исследования. Методом исследования является математическое моделирование процесса реализации сетевых атак на информационный ресурс защищенных АС ОВД посредством построения и описания графовых моделей типовых сетевых атак в динамике их реализации. На основе анализа 217 угроз, представленных в настоящее время в банке данных угроз безопасности информации, разработанном Федеральной службы по техническому и экспертному контролю (ФСТЭК) России (bdu.fstec.ru) [12], особенностей эксплуатации современных защищенных АС на объектах информатизации ОВД, результатов опроса экспертов в области информационной безопасности (ИБ) выделены типовые (наиболее опасные и часто реализуемые) сетевые атаки на информационный ресурс АС ОВД с учетом их источников, объектов воздействия и возможных последствий реализации (причиненного ущерба): анализ сетевого трафика, сканирование сети, «парольная» атака, подмена доверенного объекта сети, навязывание ложного маршрута, внедрение ложного объекта сети, отказ в обслуживании, удаленный запуск приложений [13, 14].

Моделирование динамики реализации типовых сетевых атак в защищенных АС ОВД представляет собой сложную двухэтапную задачу. На начальном этапе разработки графовых моделей для каждой сетевой атаки осуществляется определение их элементов и взаимосвязей между ними, полностью идентичных основным типам сетевых атак, реально реализуемых в защищенных АС ОВД, с целью дальнейшего получения их свойств и характеристик. Для визуального представления процесса функционирования вредоносных механизмов реализации сетевых атак в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, необходимо разработать модели динамики реализации основных типов сетевых атак на конфиденциальный информационный ресурс на основе теории графов с конечным числом состояний [15-17].

Модель процесса функционирования каждой из основных типов сетевых атак может быть представлена в виде простого ориентированного графа $D = (V,E)$, в котором: V – конечное множество вершин $v_1,v_2,\ldots v_n$, обозначающих все возможные состояния (вредоносные функции) рассматриваемой сетевой атаки; E – конечное множество дуг $e_1,e,\ldots e_m$, обозначающих все возможные переходы между состояниями. Переходы обозначены как $e_k = (v_i,v_j)$ в случае выхода из вершины графа нескольких дуг. Маршрут в графе D представляет собой последовательность действий злоумышленника при реализации сетевой атаки на информационный ресурс защищенной АС ОВД [16].

Обсуждение результатов. Графовая модель, описывающая основные этапы процесса реализации сетевой атаки «Анализ сетевого трафика» (сниффинг пакетов) на информационный ресурс АС ОВД, представлена на рис.1, а описание ее вредоносных функций – в табл.1.

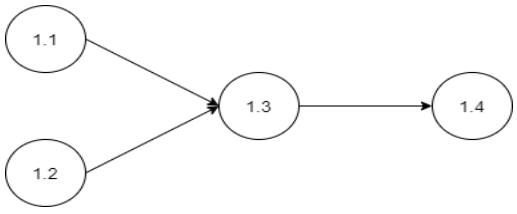

Рис.1. Граф, описывающий механизм реализации атаки «Анализ сетевого трафика»
Fig. 1. Graph describing the mechanism for implementing the Network Traffic Analysis attack

Таблица 1. Сетевая атака «Анализ сетевого трафика»
Table 1. Network attack «Network traffic analysis»

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
1.1	Атакуемые хосты готовы The attacked hosts are ready	$e_{1.1}$	$(v_{1.1},v_{1.3})$,
1.2	Хост злоумышленника физически готов к перехвату трафика The attacker's host is physically ready to intercept traffic	$e_{1.2}$	$(v_{1.2},v_{1.3})$
1.3	Передача пакета между атакуемыми хостами, перехват пакета Transferring a packet between attacked hosts, intercepting a packet	$e_{1.3}$	$(v_{1.3},v_{1.4})$
1.4	Анализ пакета, извлечение из него полезных данных (пароля, имени пользователя) Analysis of the package, extracting useful data from it (password, username)	$e_{1.4}$	

Рис. 1 показывает, что в состоянии 1.4 происходит реализация атаки «Анализ сетевого трафика» (сниффинг пакетов).

На рис. 2 представлена графовая модель, описывающая основные этапы процесса реализации сетевой атаки «Сканирование сети», а в табл. 2 приведено описание ее вредоносных функций.

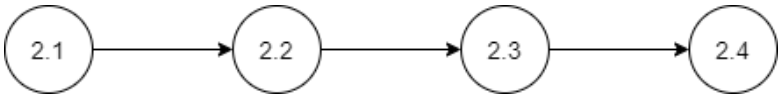

Рис. 2. Граф, описывающий механизм реализации атаки «Сканирование сети»
Fig. 2. A graph describing the mechanism for implementing the Network Scanning attack

Рис. 2 показывает, что состояние 2.4 соответствует реализации атаки «Сканирование сети».

Таблица 2. Сетевая атака «Сканирование сети»
Table 2. Network attack «Scanning the network»

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
2.1	Хост злоумышленника готов, программа настроена и запущена The attacker's host is ready, the program is configured and running	$e_{2.1}$	$(v_{2.1},v_{2.2})$
2.2	Определение активных хостов сети при помощи ICMP-запроса Identifying active hosts on a network using an ICMP request	$e_{2.2}$	$(v_{2.2},v_{2.3})$
2.3	Определение типов операционных систем активных хостов сети Determining the types of operating systems of active hosts on the network	$e_{2.3}$	$(v_{2.3},v_{2.4})$
2.4	Сканирование сервисов на активных хостах сети Scanning services on active hosts on the network	$e_{2.4}$	

Графовая модель, описывающая основные этапы процесса реализации «Парольной» сетевой атаки на информационный ресурс АС ОВД, представлена на рис. 3, а описание ее вредоносных функций – в табл. 3.

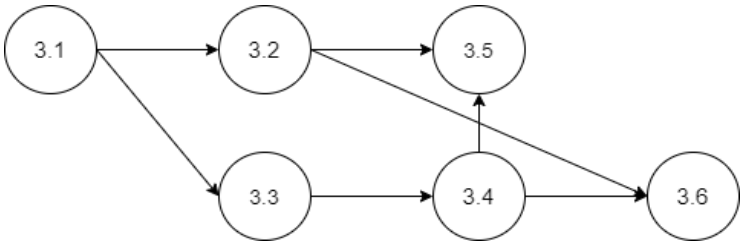

Рис. 3. Граф, описывающий механизм реализации «Парольной» сетевой атаки
Fig. 3. A graph describing the mechanism for implementing a «Password» network attack

Рис. 3 показывает, что в состоянии 3.5 происходит реализация «Парольной» сетевой атаки, а в состоянии 3.6 – ее срыв.

Таблица 3. «Парольная» сетевая атака
Table 3. «Password» network attack

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
3.1	Хост злоумышленника готов, включился в сеть общего пользования The attacker's host is ready, connected to the public network	$e_{3.1}$	$(v_{3.1},v_{3.2})$, $(v_{3.1},v_{3.3})$
3.2	Атакуемый хост запрашивает пароль The attacked host asks for a password	$e_{3.2}$	$(v_{3.2},v_{3.5})$, $(v_{3.2},v_{3.6})$
3.3	Хост злоумышленника, не зная пароля, подбирает его по специальному словарю или путем прямого перебора The attacker's host, not knowing the password, picks it up using a special dictionary or by brute-force	$e_{3.3}$	$(v_{3.3},v_{3.4})$
3.4	Хост злоумышленника завершил подбор пароля Attacker host completed password guessing	$e_{3.4}$	$(v_{3.4},v_{3.5})$, $(v_{3.4},v_{3.6})$
3.5	Пароль подобран правильно, осуществление НСД к атакуемому хосту The password was chosen correctly, the implementation of the unauthorized attack to the attacked host	$e_{3.5}$	
3.6	Пароль подобран неправильно, срыв атаки Wrong password, attack thwarted	$e_{3.6}$	

На рис. 4 представлена графовая модель реализации сетевой атаки «Подмена доверенного объекта сети» (IP-spoofing).

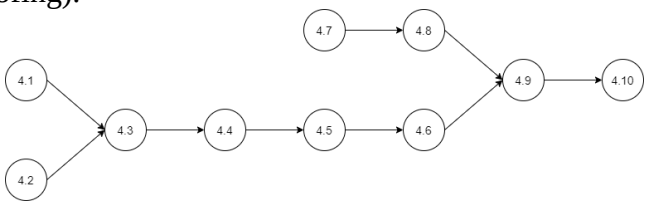

Рис. 4. Граф, описывающий механизм реализации сетевой атаки «Подмена доверенного объекта сети»
Fig. 4. A graph describing the mechanism for implementing a network attack «Substitution of a trusted network object»

Ссостояние 4.10 соответствует реализации атаки «Подмена доверенного объекта сети». В табл. 4 приведено описание ее вредоносных функций.

Таблица 4. Сетевая атака «Подмена доверенного объекта сети»
Table 4. Network attack «Spoofing a trusted network object»

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
4.1	Атакуемый хост готов The attacked host is ready	$e_{4.1}$	$(v_{4.1},v_{4.3})$
4.2	Хост злоумышленника готов к проведению атаки SYN-flood и ожидает перезагрузки атакуемого хоста The attacker's host is ready for a SYN-flood attack and is waiting for the attacked host to reboot	$e_{4.2}$	$(v_{4.2},v_{4.3})$
4.3	Перезагрузка атакуемого хоста (в результате атаки SYN-flood или самопроизвольная), атакуемый хост недоступен Reboot of the attacked host (as a result of a SYN-flood attack or spontaneous), the attacked host is unavailable	$e_{4.3}$	$(v_{4.3},v_{4.4})$
4.4	Отправка C-SYN и обработка его сервером Sending C-SYN and processing it by the server	$e_{4.4}$	$(v_{4.4},v_{4.5})$
4.5	Прием S-SYN хостом злоумышленника Reception of S-SYN by the attacker's host	$e_{4.5}$	$(v_{4.5},v_{4.6})$
4.6	Отправка C-SYN2 от имени атакуемого хоста и обработка его сервером Sending C-SYN2 on behalf of the attacked host and processing it by the server	$e_{4.6}$	$(v_{4.6},v_{4.9})$
4.7	Хост злоумышленника готов к подбору S-ACK2 Attacker host ready to brute-force S-ACK2	$e_{4.7}$	$(v_{4.7},v_{4.8})$
4.8	Подбор S-ACK2 хостом злоумышленника Hacking S-ACK2 by the attacker's host	$e_{4.8}$	$(v_{4.8},v_{4.9})$
4.9	Отправка подходящего S-ACK2 и его принятие, установка соединения с правами атакуемого хоста Sending a suitable S-ACK2 and accepting it, establishing a connection with the rights of the attacked host	$e_{4.9}$	$(v_{4.9},v_{4.10})$
4.10	Отправка данных, результат – выполнение сервером команды злоумышленника Sending data, the result is the execution of the attacker's command by the server	$e_{4.10}$	

Графовая модель, описывающая основные этапы процесса реализации сетевой атаки «Навязывание ложного маршрута» на информационный ресурс автоматизированной системы ОВД, представлена на рис. 5, а описание ее вредоносных функций – в табл. 5.

Рис. 5 показывает, что в состоянии 5.6 происходит реализация сетевой атаки «Навязывание ложного маршрута».

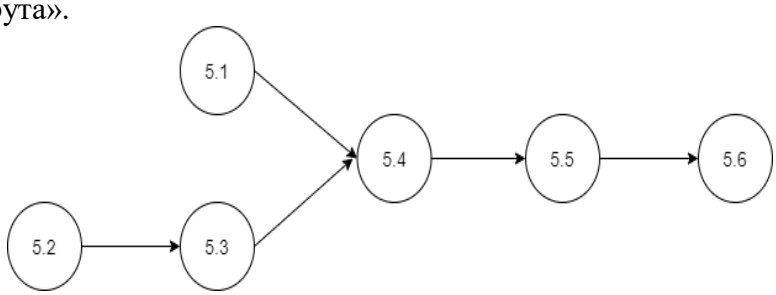

Рис. 5. Граф, описывающий механизм реализации сетевой атаки «Навязывание ложного маршрута»
Fig. 5. A graph describing the mechanism for implementing a network attack «Imposing a false route»

Таблица 5. Сетевая атака «Навязывание ложного маршрута»
Table 5. False route imposition network attack

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
5.1	Атакуемый хост готов The attacked host is ready	$e_{5.1}$	$(v_{5.1},v_{5.4})$
5.2	Злоумышленник активен The attacker is active	$e_{5.2}$	$(v_{5.2},v_{5.3})$
5.3	Настройка программы Program setting	$e_{5.3}$	$(v_{5.3},v_{5.4})$
5.4	Передача на атакуемый хост и принятие им ложных ICMP-redirect-сообщений Sending and receiving false ICMP-redirect messages to the attacked host	$e_{5.4}$	$(v_{5.4},v_{5.5})$
5.5	Изменение таблицы маршрутизации атакуемого хоста Modifying the routing table of the attacked host	$e_{5.5}$	$(v_{5.5},v_{5.6})$
5.6	Перехват и анализ трафика атакуемого хоста (для внутрисегментной атаки). Нарушение маршрутизации атакуемого хоста (для межсегментной атаки) Interception and analysis of the attacked host's traffic (for intra-segment attacks). Violation of routing of the attacked host (for cross-segment attack)	$e_{5.6}$	

На рис. 6 представлена графовая модель, описывающая основные этапы процесса реализации сетевой атаки «Внедрение ложного объекта сети» (ARP-spoofing).

В табл. 6 приведено описание ее вредоносных функций.

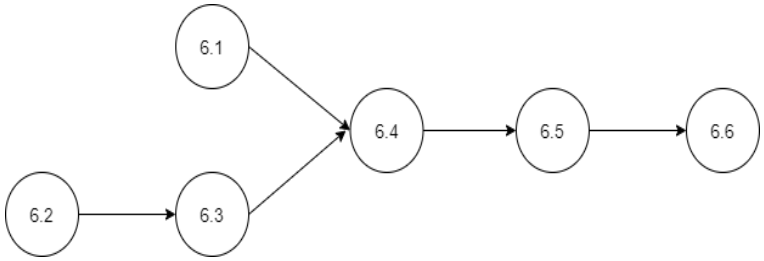

Рис. 6. Граф, описывающий механизм реализации сетевой атаки

«Внедрение ложного объекта сети»
Fig. 6. A graph describing the mechanism for implementing a network attack
«Injection of a false network object»

Таблица 6. Сетевая атака «Внедрение ложного объекта сети»
Table 6. Network attack «Injection of a false network object»

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
6.1	Атакуемый хост формирует широковещательный ARP-запрос The attacked host generates a broadcast ARP request	$e_{6.1}$	$(v_{6.1},v_{6.4})$
6.2	Хост злоумышленника находится внутри сегмента сети атакуемого хоста The attacker's host is inside the attacked host's network segment	$e_{6.2}$	$(v_{6.2},v_{6.3})$
6.3	Подготовка хоста злоумышленника к проведению атаки (сканирование MAC-адресов хостов сети и настройка программы) Preparing an attacker host for an attack (scanning the MAC addresses of network hosts and configuring programs)	$e_{6.3}$	$(v_{6.3},v_{6.4})$
6.4	Отправка ложного ARP-ответа и принятие его атакуемым хостом Sending a bogus ARP response and accepting it by the attacked host	$e_{6.4}$	$(v_{6.4},v_{6.5})$
6.5	Изменение ARP-таблицы атакуемого хоста Modifying the ARP table of the attacked host	$e_{6.5}$	$(v_{6.5},v_{6.6})$
6.6	Перехват и анализ трафика атакуемого хоста Interception and analysis of the traffic of the attacked host	$e_{6.6}$	

Рис. 7. показывает, что в состоянии 7.5 происходит реализация сетевой атаки «Отказ в обслуживании». Описание ее вредоносных функций – в табл. 7.

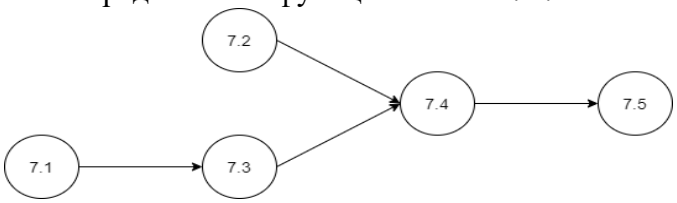

Рис.7. Граф, описывающий механизм реализации сетевой атаки «Отказ в обслуживании»
Fig. 7. Graph describing the mechanism for implementing a network denial of service attack

Таблица 7. Сетевая атака «Отказ в обслуживании»
Table 7. Network attack «Denial of service»

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
7.1	Хост злоумышленника готов The attacker host is ready	$e_{7.1}$	$(v_{7.1},v_{7.3})$
7.2	Атакуемый хост готов принять SYN-пакеты с несуществующим обратным адресом в очередь неоткрытых соединений The attacked host is ready to accept SYN packets with a non-existent return address in the queue of unopened connections	$e_{7.2}$	$(v_{7.2},v_{7.4})$
7.3	Запуск и настройка программы для SYN-flood Launching and configuring the SYN-flood program	$e_{7.3}$	$(v_{7.3},v_{7.4})$
7.4	Отправка SYN-пакетов и постановка их в очередь атакуемому хосту Sending SYN packets and queuing them to the attacked host	$e_{7.4}$	$(v_{7.4},v_{7.5})$
7.5	Переполнение очереди атакуемого хоста, он не в состоянии обрабатывать другие запросы The target host's queue is overflowing, it is unable to process other request	$e_{7.5}$	

На рис. 8. представлена графовая модель, описывающая основные этапы процесса реализации сетевой атаки «Удаленный запуск приложений» (IP-hijacking), а в табл.8 приведено описание ее вредоносных функций. Состояние 8.8 соответствует реализации сетевой атаки «Удаленный запуск приложений».

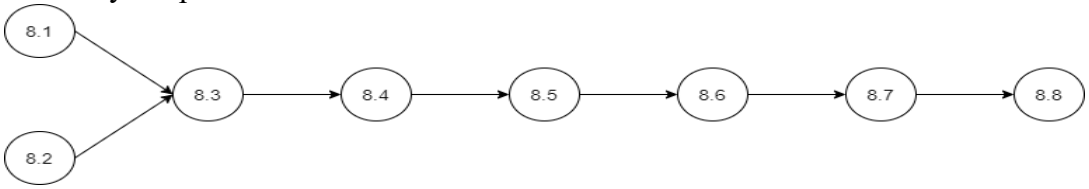

Рис. 8. Граф, описывающий механизм реализации сетевой атаки «Удаленный запуск приложений»
Fig. 8. Graph describing the mechanism for implementing a network attack «Remote Application Launch»

Таблица 8. Сетевая атака «Удаленный запуск приложений»
Table 8. Remote Application Launch Network Attack

№ Состояния No. Fortunes	Вредоносные функции, выполняемые сетевой атакой Malicious functions performed by a network attack	e_k	(v_i,v_j)
8.1	Атакуемые хосты готовы The attacked hosts are ready	$e_{8.1}$	$(v_{8.1},v_{8.3})$
8.2	Хост злоумышленника готов к перехвату трафика Attacker host is ready to intercept traffic	$e_{8.2}$	$(v_{8.2},v_{8.3})$
8.3	Обмен пакетами между атакуемыми хостами для установления соединения, перехват S-SYN и C-ACK Exchange of packets between attacked hosts to establish a connection, interception of S-SYN and C-ACK	$e_{8.3}$	$(v_{8.3},v_{8.4})$
8.4	Отправка RST от имени второго атакуемого хоста, закрытие соединения между атакуемыми хостами для первого из них Sending RST on behalf of the second attacked host, closing the connection between the attacked hosts for the first of them	$e_{8.4}$	$(v_{8.4},v_{8.5})$
8.5	Отправка первым атакуемым хостом S-SYN2 для второго хоста, перехват S-SYN2, обработка первым атакуемым хостом C-SYN2 The first attacked host sends S-SYN2 for the second host, intercepts S-SYN2, and is processed by the first attacked host C-SYN2	$e_{8.5}$	$(v_{8.5},v_{8.6})$
8.6	Отправка C-SYN2 от имени второго атакуемого хоста, перехват S-SYN2, возникновение ACK-бури между атакуемыми хостами Sending C-SYN2 on behalf of the second attacked host, intercepting S-SYN2, occurrence of an ACK storm between the attacked hosts	$e_{8.6}$	$(v_{8.6},v_{8.7})$
8.7	Отправка S-ACK2 от имени второго атакуемого хоста, принятие S-ACK2, установка соединения с правами второго атакуемого хоста Sending S-ACK2 on behalf of the second attacked host, accepting S-ACK2, establishing a connection with the rights of the second attacked host	$e_{8.7}$	$(v_{8.7},v_{8.8})$
8.8	Обмен модифицированными данными со вторым атакуемым хостом по ACK, с первым – по ACK-2 Exchange of modified data with the second attacked host via ACK, with the first via ACK-2	$e_{4.8}$	

Вывод. В статье разработаны графовые модели динамики реализации типовых сетевых атак на информационный ресурс современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД.

Выделены ключевые элементы и функциональные компоненты моделей, что позволяет наглядно представить процесс реализации их основных вредоносных функций и учесть предполагаемые действия злоумышленника.

На основе представленных графовых моделей и их элементов, полностью идентичных типовым сетевым атакам, реально воздействующим на информационный ресурс защищенных АС ОВД, могут быть разработаны динамические модели их реализации с помощью сети Петри-Маркова, а также имитационные модели в программной среде CPN Tools с целью получения вероятностно-временных характеристик в виде времен выполнения каждой атакой вредоносных функций.

В дальнейших исследованиях предложенные модели рассмотренных типовых сетевых атак планируется использовать в качестве основы для анализа и разработки моделей противодействия угрозам удаленного НСД к информационному ресурсу защищенных АС ОВД, а также для проведения количественной оценки опасности реализации сетевых атак на конфиденциальный информационный ресурс и количественной оценки эффективности функционирования программных средств и систем ИБ в защищенных АС на объектах информатизации ОВД в соответствии с требованиями действующей нормативной документации [1, 2, 18-21].

Полученные результаты могут быть использованы для формирования частной модели актуальных атак для конкретной АС ОВД и обоснования количественных требований к перспективным СЗИ от НСД при их эксплуатации на объектах информатизации ОВД в рамках концепции обеспечения ИБ ОВД РФ[2].

Библиографический список:

1. ФСТЭК России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс]. Режим до-

ступа: https://fstec.ru/component/ attachments/download/299. (Дата обращения: 15.05.2020).
2. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169 [Электронный ресурс]. Режим доступа: http://policemagazine.ru/forum/ showthread.php?t =3663. (Дата обращения: 15.05.2020).
3. Рогозин Е.А. Проблемы и пути их решения при проектировании систем защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД / Е.А. Рогозин, А.Д. Попов, Т.В. Мещерякова // Информационные технологии, связь и защита информации МВД России. 2017. Ч. 1. С. 115-118.
4. Butusov I.V. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure / I.V. Butusov, A.A. Romanov [Электронный ресурс]. с Режим доступа: http://fcyberrus.com/wp-content/uploads/2018/05/02-10-125-18_1.Butusov. pd. (Дата обращения: 17.05.2020).
5. Дровникова И.Г. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронежского университета МВД России. 2019. № 4. С. 51-63.
6. Sher A. Simulation of Attacks in a Wireless Sensor Networkusing NS2 / A. Sher // The School of Engineering & Computing Sciences. Texas A&M University-Corpus Christi. Spring 2015. 49 p.
7. Yuanshun Y. Automated Crowdturfing Attacks and Defenses in Online Review Systems / Y. Yuanshun [etc.] // arXiv:1708.08151v2 [cs.CR]. 8 Sep. 2017. 16 p. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/view/ (Дата обращения: 17.05.2020).
8. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. 2015. pp. 100-112.
9. Effectiveness Evaluation on Cyberspace Security Defense System / L. Yun [etc.] // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. pp. 576-579.
10. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М: РадиоСофт, 2010. 232 с.
11. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронеж. госуд. технич. ун-т, 2013. 265 с.
12. ФСТЭК России. Банк данных угроз безопасности информации. Режим доступа: https://bdu.fstec.ru/threat. (Дата обращения: 16.05.2020).
13. Овчинникова Е.С. Анализ и классификация основных угроз информационной безопасности автоматизированных систем на объектах информатизации органов внутренних дел / А.В. Бацких, И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Безопасность информационных технологий = IT Security. Т. 27. № 1. 2020. С. 40-50.
14. Овчинникова Е.С. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел / И.Г. Дровникова, Е.С. Овчинникова, В.В. Конобеевских //Вестник Дагестанского государственного технического университета. Технические науки. Т. 47. № 1. 2020. С. 72-85.
15. Свами М. Графы, сети и алгоритмы: пер. с англ. / М. Свами, К. Тхуласираман. Москва: Мир, 1984. 455 с.
16. Дистель Р. Теория графов / Р. Дистель. Новосибирск: изд-во ин-та математики, 2002. 336 с.
17. Sudakov B. Graph Theory/B. Sudakov. 18.08.2016 [Электронный ресурс]. Режим доступа: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii. (Дата обращения: 15.05.2020).
18. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 19.12.2016) (с изм. и доп., вступ. в силу с 13.12.2019) [Электронный ресурс]. Режим доступа: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii. (Дата обращения: 17.05.2020).
19. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016, №646 [Электронный ресурс]. Режим доступа: (Дата обращения: 18.05.2020): http://publication.pravo.gov.ru/Document/View/0001201612060002.
20. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ 1200108858. (Дата обращения: 18.05.2020).
21. ФСТЭК России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники [Электронный сурс]. Режим доступа: http://docs.cntd.ru/ document/901817221. (Дата обращения: 18.05.2020).

References:

1. FSTEK Rossii. Rukovodyashchiy dokument. Kontseptsiya zashchity sredstv vychislitel'noy tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii [Elektronnyy resurs]. [FSTEC of

Russia. Guidance document. The concept of protection of computer technology and automated systems from unauthorized access to information [Electronic resource]. Access mode: https://fstec.ru/component/ attachments / download / 299. - (Date of treatment: 05/15/2020). (In Russ)]

2. Ob utverzhdenii Kontseptsii obespecheniya informatsionnoy bezopasnosti organov vnutrennikh del Rossiyskoy Federatsii do 2020 goda: prikaz MVD Rossii ot 14.03.2012 № 169 [Elektronnyy resurs]. [On the approval of the Concept for ensuring information security of the internal affairs bodies of the Russian Federation until 2020: order of the Ministry of Internal Affairs of Russia dated March 14, 2012 No. 169 [Electronic resource]. Access mode: http://policemagazine.ru/forum/showthread.php?t = 3663. (Date of treatment: 05/15/2020). (In Russ)]
3. Rogozin Ye.A. Problemy i puti ikh resheniya pri proyektirovanii sistem zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh informatsionnykh sistemakh OVD / Ye.A. Rogozin, A.D. Popov, T.V. Meshcheryakova // Informatsionnyye tekhnologii, svyaz' i zashchita informatsii MVD Rossii. 2017. CH. 1. S. 115-118. [Rogozin E.A. Problems and ways to solve them in the design of information protection systems from unauthorized access in automated information systems of the internal affairs department / E.A. Rogozin, A.D. Popov, T.V. Meshcheryakova // Information technologies, communication and information protection of the Ministry of Internal Affairs of Russia. 2017. Part 1. pp. 115-118. (In Russ)]
4. Butusov I.V. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure / I.V. Butusov, A.A. Romanov [Electronic resource]. Access mode: http://fcyberrus.com/wp-content/uploads/2018/05/02-10-125-18_1. Butusov. pd. (Date of treatment: 05/17/2020).
5. Drovnikova I.G. Analiz sushchestvuyushchikh sposobov i protsedur otsenki opasnosti realizatsii setevykh atak v avtomatizirovannykh sistemakh organov vnutrennikh del i aspekty ikh sovershenstvovaniya / I.G. Drovnikova, Ye.S. Ovchinnikova, Ye.A. Rogozin // Vestnik Voronezh. in-ta MVD Rossii. 2019. № 4. S. 51-63. [Drovnikova I.G. Analysis of existing methods and procedures for assessing the danger of implementing network attacks in automated systems of internal affairs bodies and aspects of their improvement / I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin // Bulletin Voronezh. Institute of the Ministry of Internal Affairs of Russia. 2019.No. 4.pp. 51-63. (In Russ)]
6. Sher A. Simulation of Attacks in a Wireless Sensor Network using NS2 / A. Sher // The School of Engineering & Computing Sciences. –Texas A&M University-Corpus Christi. Spring 2015. 49 p.
7. Yuanshun Y. Automated Crowdturfing Attacks and Defenses in Online Review Systems / Y. Yuanshun [etc.] // arXiv:1708.08151v2 [cs.CR]. 8 Sep. 2017. 16 p. [Elektronnyy resurs]. [Yuanshun Y. Automated Crowdturfing Attacks and Defenses in Online Review Systems / Y. Yuanshun [etc.] // arXiv: 1708.08151v2 [cs.CR]. 8 Sep. 2017.16 p. [Electronic resource]. Access mode: https://docviewer.yandex.ru/view/ (Date of access: 17.05.2020). (In Russ)]
8. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. 2015. 100-112.
9. Effectiveness Evaluation on Cyberspace Security Defense System / L. Yun [etc.] // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. 576-579.
10. Rad'ko N.M. Risk-modeli informatsionno-telekommunikatsionnykh sistem pri realizatsii ugroz udalennogo i neposredstvennogo dostupa / N.M. Rad'ko, I.O. Skobelev. M: RadioSoft, 2010. 232 s. [Radko N.M. Risk-models of information and telecommunication systems in the implementation of threats of remote and direct access / N.M. Radko, I.O. Skobelev. M: RadioSoft, 2010.232 p. (In Russ)]
11. Rad'ko N.M. Proniknoveniya v operatsionnuyu sredu komp'yutera: modeli zloumyshlennogo udalennogo dostupa / N.M. Rad'ko, YU.K. YAzov, N.N. Korneyeva. Voronezh: Voronezh. gosud. tekhnich. un-t, 2013. 265 s. [Radko N.M. Penetration into the operating environment of a computer: models of malicious remote access / N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh. state technical un-t, 2013. 265 p. (In Russ)]
12. FSTEK Rossii. Bank dannykh ugroz bezopasnosti informatsii. Rezhim dostupa: https://bdu.fstec.ru/threat. (Data obrashcheniya: 16.05.2020). [FSTEC of Russia. Databank of information security threats. Access mode: https://bdu.fstec.ru/threat. (Date of treatment: 16.05.2020). (In Russ)]
13. Ovchinnikova Ye.S. Analiz i klassifikatsiya osnovnykh ugroz informatsionnoy bezopasnosti avtomatizirovannykh sistem na ob"yektakh informatizatsii organov vnutrennikh del / A.V. Batskikh, I.G. Drovnikova, Ye.S. Ovchinnikova, Ye.A. Rogozin // Bezopasnost' informatsionnykh tekhnologiy = IT Security. T. 27. № 1. 2020. S. 40-50. [Ovchinnikova E.S. Analysis and classification of the main threats to the information security of automated systems at the objects of informatization of the internal affairs bodies / A.V. Batskikh, I. G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin // Security of information technologies = IT Security. T. 27.No. 1. 2020.pp. 40-50. (In Russ)]
14. Ovchinnikova Ye.S. Analiz tipovykh setevykh atak na avtomatizirovannyye sistemy organov vnutrennikh del / I.G. Drovnikova, Ye.S. Ovchinnikova, V.V. Konobeyevskikh //Vestnik Dagestanskogo gosud. tekhnich. universiteta. Tekhnicheskiye nauki. T. 47. № 1. 2020. S. 72-85. [Ovchinnikova E.S. Analysis of typical network attacks on automated systems of internal affairs bodies / I.G. Drovnikova, E.S. Ovchinnikova, V.V. Konobeevskikh // Herald of the Daghestan State Technical University. Technical Science. T. 47. No. 1. 2020. pp. 72-85. (In Russ)]

15. Svami M. Grafy, seti i algoritmy: per. s angl. / M. Svami, K. Tkhulasiraman. Moskva: Mir, 1984. 455 s. [Swami M. Graphs, networks and algorithms: trans. from English / M. Swami, K. Thulasiraman. Moscow: Mir, 1984 455 p. (In Russ)]
16. Distel' R. Teoriya grafov / R. Distel'. Novosibirsk: izd-vo in-ta matematiki, 2002. 336 s. [Distel R. Graph Theory / R. Distel. Novosibirsk: publishing house of the Institute of Mathematics, 2002.336 p. (In Russ)]
17. Sudakov B. Graph Theory / B. Sudakov. 08/18/2016 [Electronic resource]. Access mode: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii. (Date of access: 15.05.2020).
18. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: federal'nyy zakon ot 27.07.2006 № 149-FZ (v red. ot 19.12.2016) (s izm. i dop., vstup. v silu s 13.12.2019) [Elektronnyy resurs]. – Rezhim dostupa: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii. – (Data obrash-cheniya: 17.05.2020). [On information, information technologies and information protection: Federal Law No. 149-FZ of July 27, 2006 (as amended on December 19, 2016) (as amended and supplemented, entered into force on December 13, 2019) [Electronic resource]. Access mode: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii. (Date of treatment: 05/17/2020). (In Russ)]
19. Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii: ukaz Prezidenta RF ot 05.12.2016, №646 [Elektronnyy resurs]. [On the approval of the Doctrine of information security of the Russian Federation: decree of the President of the R.ussian Federation of 05.12.2016 No. 646 [Electronic resource]. Access mode: http://publication.pravo.gov.ru/Document/View/0001201612060002. (Date of access: 05/18/2020). (In Russ)]
20. GOST R 51583-2014. Natsional'nyy standart Rossiyskoy Federatsii. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchiye polozheniya [Elektronnyy resurs] [GOST R 51583-2014. National standard of the Russian Federation. Protection of information. The procedure for creating automated systems in a protected design. General provisions [Electronic resource]. Access mode: http://docs.cntd.ru/document/1200108858. (Date of access: 05/18/2020). (In Russ)]
21. FSTEK Rossii Rukovodyashchiy dokument. Vremennoye polozheniye po organizatsii razrabotki, izgotovleniya i ekspluatatsii programmnykh i tekhnicheskikh sredstv zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh sistemakh i sredstvakh vychislitel'noy tekhniki [FSTEC of Russia. Guidance document. Temporary regulations on the organization of development, manufacture and operation of software and technical means of protecting information from unauthorized access in automated systems and computer facilities [Electronic resource] (In Russ)]

Сведения об авторе:

Овчинникова Елена Сергеевна, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел; e-mail.ru:yelena_ovchinnikova1@mail.ru

Information about authors:

Elena S. Ovchinnikova, Adjunct, Department of Automated Information Systems of the Internal Affairs Bodies; e-mail.ru:yelena_ovchinnikova1@mail.ru

Конфликт интересов.
Автор заявляет об отсутствии конфликта интересов.
Поступила в редакцию 01.12.2020.
Принята в печать 15.01.2021.

Conflict of interest.
The author declare no conflict of interest.
Received 01.12. 2020.
Accepted for publication 15.01.2021.