Для цитирования: *Дровникова И.Г., Змеев А.А., Попов А.Д., Рогозин Е.А. Методика исследования вероятностно-временных характеристик реализации сетевых атак в программной среде имитационного моделирования. Вестник Дагестанского государственного технического университета. Технические науки. 2017;44 (4):99-113. DOI:10.21822/2073-6185-2017-44-4-99-113*

For citation: *Drovnikova I.G., Zmeev A.A., Popov A.D., Rogozin E.A. Methodology for investigating the probability-time characteristics of network attacks in the simulation modelling software environment. Herald of Daghestan State Technical University. Technical Sciences. 2017; 44 (4):99-113. (In Russ.) DOI:10.21822/2073-6185-2017-44-4-99-113*

ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056
DOI:10.21822/2073-6185-2017-44-4-99-113

МЕТОДИКА ИССЛЕДОВАНИЯ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В ПРОГРАММНОЙ СРЕДЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Дровникова И.Г.[1], Змеев А.А.[2], Попов А.Д.[3], Рогозин Е.А.[4]
[1,3,4]Воронежский институт МВД России,
[1,3,4]394065, г. Воронеж, пр. Патриотов,53, Россия,
[2]Военная академия воздушно-космической обороны имени Маршала Советского Союза Г.К. Жукова,
[2]170022, г. Тверь, ул. Жигарева, 50, Россия,
[1]e-mail: idrovnikova@mail.ru, [2] e-mail: tzmeev@yandex.ru,
[3] e-mail: anton.holmes@mail.ru, [4] e-mail: evgenirogozin@yandex.ru

Резюме. Цель. *Проведён анализ открытых литературных источников и нормативных документов по проблеме защиты информации в автоматизированных системах, который показал отсутствие в этих документах количественных параметров вероятностно-временных характеристик реализации сетевых атак к информационному ресурсу автоматизированных систем. К ним можно отнести среднее время нахождения сетевой атаки в одном из ее состояний, реализующие деструктивные воздействия с целью разработки эффективной модели противодействия реализуемых в системах и средствах информационной безопасности угрозам.* ***Метод.*** *Одним из методов решения этой проблемы является натурный эксперимент. При реализации его на практике возникает много трудностей, а именно определение вероятностно-временных характеристик сетевых атак (если время значительно меньше секунды). Применены новые информационные технологии, к которым можно отнести и программную среду имитационного моделирования «CPNTools».* ***Результат.*** *Разработана методика определения вероятностно-временных характеристик реализации сетевых атак к информационному ресурсу автоматизированных систем (количественные величины времен реализации сетевых атак во всех состояниях формальной модели их функционирования). Предложена классификация сетевых угроз несанкционированного доступа в автоматизированных системах на основе имеющегося у Федеральной службы по техническому и экспортному контролю России банка данных.* ***Вывод.*** *Выходными данными разработанной методики являются вероятностно-временные характеристики сетевых атак к информационному ресурсу автоматизированных систем, полученные в ходе имитационного моделирования в программной среде «CPNTools» в виде времени нахождения в одном из состояний реализации этих деструктивных воздействий в автоматизированных системах. Определены перспективы применения полученных результатов, связанные с повышением реальной защищенности существующих, а также разрабатываемых автоматизированных систем.*

Ключевые слова: *автоматизированная система, несанкционированный доступ, вероятностно-временные характеристики, система защиты информации от несанкционированного доступа, угроза, сетевая атака*

TECHNICAL SCIENCE
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

METHODOLOGY FOR INVESTIGATING THE PROBABILITY-TIME CHARACTERISTICS OF NETWORK ATTACKS IN THE SIMULATION MODELLING SOFTWARE ENVIRONMENT

Irina G. Drovnikova[1], Anatoly A.Zmeev [2], Anton D. Popov[3], Evgenii A. Rogozin[4]
[1,3,4] Voronezh Institute of the Ministry of the Interior of Russia,
[1,3,4]53 Patriotov Ave., Voronezh 394065, Russia,
[2]Zhukov Air and Space Defense Academy,
[2]50 Zhigareva Str., Tver 170022, Russia,
[1]e-mail: idrovnikova@mail.ru, [2] e-mail: tzmeev@yandex.ru,
[3] e-mail: anton.holmes@mail.ru, [4] e-mail: evgenirogozin@yandex.ru

Abstract. Objectives *An analysis of open access literature sources and normative documents on the problem of information protection in automated systems was carried out. This showed the absence in these documents of quantitative parameters of the probability-time characteristics of network attacks carried out on information resource of automated systems. To such parameters one can attribute the average time of a network attack in one of its states, realising destructive impacts, in order to develop an effective model for countering threats implemented in systems and information security products.* ***Methods*** *One of the methods for solving this problem is a full-scale experiment; however, in practice many difficulties arise during its implementation, namely the determination of the probability-time characteristics of network attacks (if the time is much less than a second). To solve this complex problem, it is necessary to use new information technologies, which include the CPNTools simulation modelling software environment.* ***Results*** *The methodology for determining the probability-time characteristics of network attacks carried out on the information resource of automated systems (the quantitative values of the times of the network attack at all states of the formal model of their operation) is developed. A classification of network threats comprising unauthorised access in automated systems based on the data bank of the Federal Service for Technical and Export Control of Russian Federation is proposed.* ***Conclusion*** *The output data of the methodology developed in the article are the probability-time characteristics of network attacks carried out on the information resource of automated systems. This data was obtained during the simulation using CPNTools software environment in the form of the residence time (realisation) in one of the realisation states of these destructive effects in automated systems. The main aspects of the obtained results are analysed and prospects for their future use, connected with the increase of real security of existing, as well as developed, automated systems, are outlined.*

Keywords: *automated system, unauthorised access, probability-time characteristics, system of information protection from unauthorised access, threat, network attack.*

Введение. В настоящее время при эксплуатации автоматизированных систем (АС) на первый план выходят вопросы, связанные с повышением надѐжности их функционирования как существующих, так и перспективных (разрабатываемых) АС. В качестве одного из основных негативных факторов, влияющего на функционирование этих систем можно назвать факт, связанный с несанкционированным доступом (НСД) злоумышленника к информационному ресурсу АС, который в целом непосредственно влияет на уровень защищѐнности [1]. Поэтому вопросы, связанные с научными исследованиями в области защиты информационного ресурса АС являются весьма актуальными.

Анализ нормативных документов Федеральной службы по техническому и экспортному контролю России (ФСТЭК) показал [2-10], что вопросы, связанные сполучением количественных характеристик времени реализации угроз в АС проработаны в недостаточном объеме. Данные характеристики в частности необходимы:

– при разработке АС в защищѐнном исполнении;

– при сертификации систем защиты информации (СЗИ) от НСД (нормативные документы при сертификации СЗИ);

– при формировании требований средствам и системам информационной безопасности (ИБ) в АС.

Постановка задачи. Для исследований реализаций угроз НСД, с целью получения вероятностно-временных характеристик (ВВХ) в АС, необходимо разработать соответствующую методику. Для этого необходимо:

1. Провести классификацию угроз НСД в АС;

2. Выбрать типовые, наиболее распространѐнные атаки к информационному ресурсу АС, которые способствуют реализации угроз НСД;

3. Разработать вербальные (описательные) модели реализации сетевых атак на информационный ресурс АС, для создания формальной модели функционирования дестабилизирующих воздействий в виде ориентированного графа;

4. Используя программную среду CPNTools необходимо запрограммировать каждую графовую модель реализации сетевых атак в АС и провести имитационное моделирование.

5. По результатам имитационного моделирования в программной среде имитационного моделирования CPNTools представить результирующие таблицы каждой из сетевых атак.

6. Привести в качестве практического примера использование полученных результатов в виде ВВХ сетевых атак к информационному ресурсу АС, которые станут основой для формирования требований к СЗИ от НСД при использовании генетического алгоритма (ГА) [8]. Используя возможности пакета прикладных программ Matlab 2013, который содержит в своем составе библиотеку со встроенными ГА.

Метод исследования. Для исследования необходимо провести классификацию угроз НСД к информационному ресурсу АС, связанные непосредственно с человеческим фактором, к которым можно отнести и сетевые атаки. Анализ [9] позволил представить классификационную схему угроз НСД к информационному ресурсу АС в виде, показанном на рис.1.

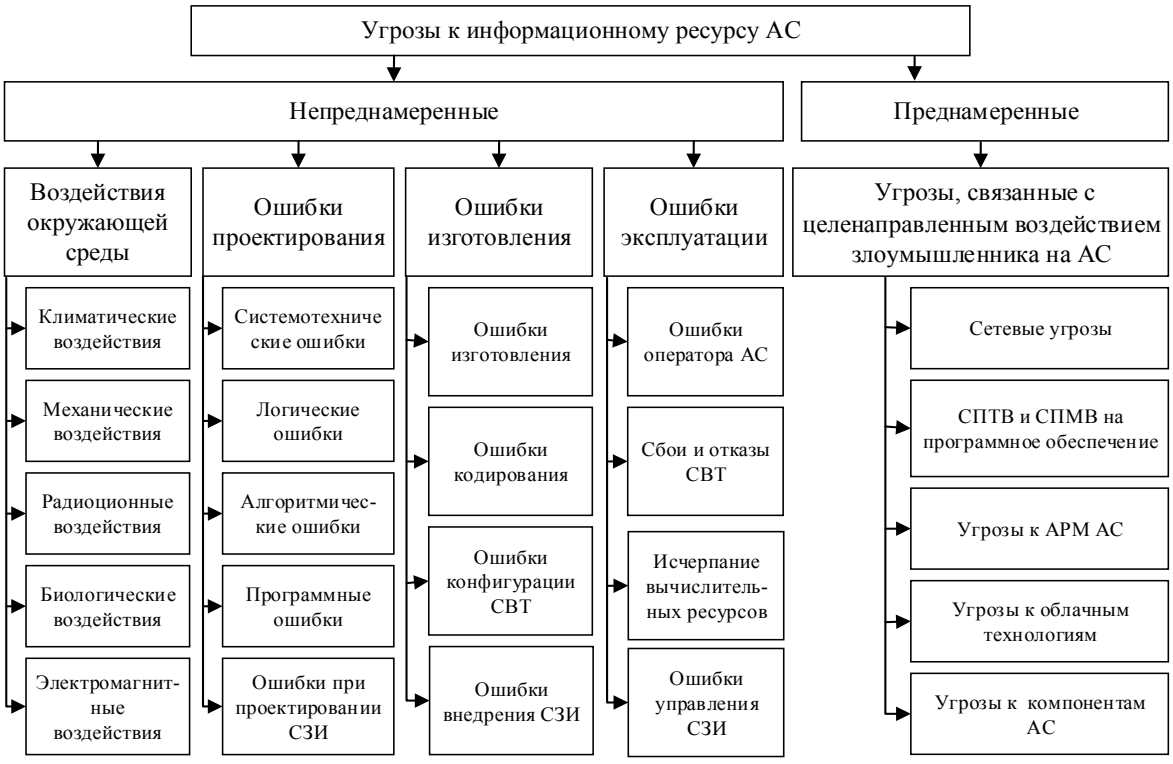

Рис.1 Классификационная схема угроз НСД к информационному ресурсу АС
Fig. 1 Classification scheme of threats to the information resource AS

Непреднамеренные угрозы представляют собой ошибки, обусловленные человеческим фактором, а также к ним можно отнести и влияние окружающей среды. Преднамеренные угрозы непосредственно реализуются злоумышленниками и нацелены на совершение противоправных (незаконных) действий к информационному ресурсу АС, целью которых является нарушение таких свойств информации, как конфиденциальность, целостность и доступность, а также нарушение надежности функционирования АС в целом.

Преднамеренные угрозы довольно полно представлены в банке данных главного законодателя страны в области ИБ ФСТЭК России по адресу bdu.fstec.ru [11].

Следует отметить, что существующий банк данных постоянно пополняется; сотрудники ФСТЭК исследуют как альтернативные базы, так и ресурсы крупных компаний производителей. Можно сказать, что данный перечень угроз представляет собой более полную картину относительно имеющихся классификаций, и охватывает все актуальные аспекты в области ИБ АС. В исследуемом банке данных на данный момент имеется 207 угроз НСД. Анализ имеющейся информации по угрозам в банке данных показал, что более одной трети от общего количества угроз, а именно 74, занимают угрозы, связанные с сетевым воздействием на информационные ресурсы АС, что требует наиболее тщательного исследования. Данный вид угроз ИБ в АС направлен на следующие объекты воздействия: сетевой трафик; системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение; виртуальная машина; информационная система; микропрограммное обеспечение; объекты файловой системы; сетевой узел; аппаратное обеспечение; рабочая станция.

Сетевые угрозы реализуются злоумышленниками в виде сетевых атак на информационные ресурсы АС. Данным деструктивным воздействиям подвержены различные организации, эксплуатирующие АС, такие как коммерческие, государственные, военные и другие структуры. Поэтому проблема защиты информационного ресурса АС принимает федеральный уровень.

Злоумышленники используют все более изощренные методы воздействия на информационные ресурсы, тем самым подвергая предприятия, эксплуатирующие АС, например, к финансовым потерям. Поэтому в соответствии в [2] необходимо на начальных стадиях разработки АС предусмотреть возможную реализацию сетевых атак.

К основным ВВХ сетевых атак можно отнести среднее время нахождения в одном из состояний графовой модели, формально описывающую их реализацию в АС.

С целью получения количественных значений ВВХ сетевых атак в АС необходимо использовать программную среду имитационного моделирования «CPNTools», которая представляет собой мощный инструмент для анализа и моделирования сетей различного уровня сложности, к которым можно отнести цветные сетей Петри и временные сетей Петри [12-14].

Деструктивные воздействия могут реализовываться разными способами, основными этапами которых являются сбор информации, реализация атаки и ее завершение, заключающиеся в уничтожении следов.

Обсуждение результатов. Рассмотрим типовые, наиболее распространенные сетевые атаки.

«Сниффинг пакетов». Данный вид атаки, относится к пассивным и часто используется при подготовке к активным сетевым атакам, которые возможны в том случае, если в сети установлены концентраторы, при использовании которых пакеты внутри сети рассылаются широковещательным способом, а компьютер, при получении пакета, принимает решение о его принадлежности.

В случае если злоумышленнику удается получить доступ к машине, находящейся в такой сети, то ему станет доступна абсолютно вся передаваемая информация. Ему будет достаточно перевести сетевую карту в «неразборчивый режим», в котором компьютер принимает все приходящие пакеты, вне зависимости принадлежат они ему или нет.

Данный вид атак может быть реализован при помощи специального программного обеспечения – пакетного сниффера, который захватывает все сетевые пакеты, на которые направлена атака. В дальнейшем полученные сниффером данные могут быть использованы для НСД к информационному ресурсу АС. На рис. 2 приведена графовая модель, показывающая основные

этапы реализации сетевой атаки «сниффинг пакетов» на информационный ресурс АС [15-16].

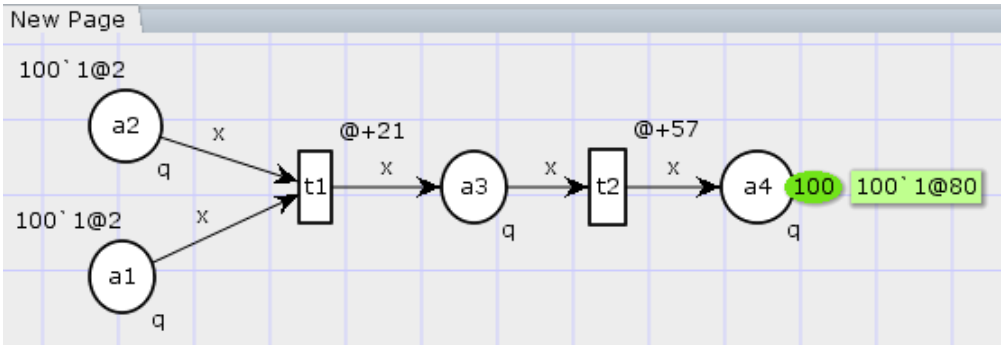

Рис.2. Графовая модель сетевой атаки «сниффинг пакетов»
Fig.2. Graph model of network attack «packet sniffing»

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.1.

Соотношение машинного времени к реальному времени во всех графовых моделях будет представлено, как 1 ед. = 0,001 с.

Результирующие таблицы, полученные при помощи программной среды CPNTools, имеют следующие поля: Name – имя позиции, Count – счетчик проходов по графу, начиная с 0, Sum – суммарное количество попадания маркера в конкретную позицию, Avrg – среднее значение, но в контексте данной имитационной задачи, так как маркер в сети один, будет являться вероятностью попадания маркера в позицию, Min – минимальное количество маркеров в позиции, Max – максимальное количество маркеров в позиции,TimeAvrg – среднее время пребывания маркера в позиции.

Таблица 1. Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «сниффинг пакетов»
Table 1. Results of simulation simulation in the CPNTools network environment «packet sniffing»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	102	8.695652	0	100	2
Marking_size_New_Page'a2_1	102	8.695652	0	100	2
Marking_size_New_Page'a3_1	202	91.304348	0	100	21
Marking_size_New_Page'a4_1	102	0.000000	0	100	57

Атака «сканирование сети» выполняется в разведывательных целях.

С ее помощью злоумышленнику становится известна информация о структуре сети и сервисах, имеющихся в данной сети. Для ее реализации необходимо просканировать сеть при помощи специального программного обеспечения, предназначенного для сбора информации. Первоочередным необходимо установить параметры сканирования и произвести последовательный опрос всех хостов в указанном диапазоне IP-адресов в многопоточном режиме при помощи ICMP-эхо-запросов. При рассылке недопустимых ICMP или TCP пакетов, злоумышленник сможет определить тип операционной системы и программное обеспечение, установленное на целевых компьютерах. В результате чего будет получен доступ к информации о размещенных в сканируемой сети сервисов и хостов [14].

На рис. 3 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «сканирование сети» на информационный ресурс АС [14,17-18].

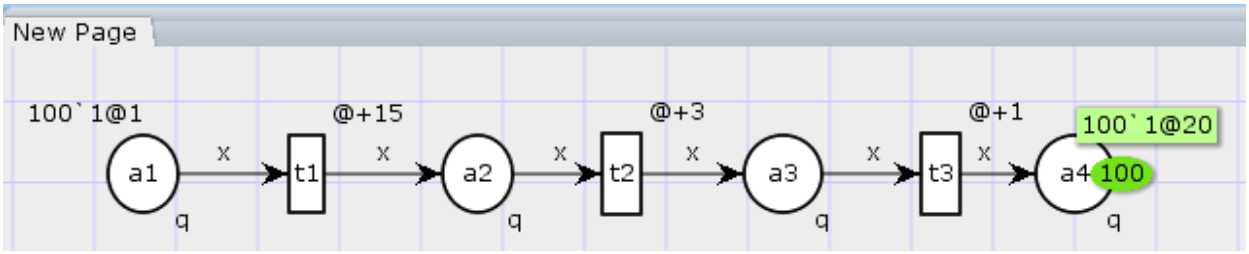

Рис.3. Графовая модель сетевой атаки «сканирование сети»
Fig.3. The graph model of network attack «network scanning»

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.2.

Таблица 2. Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «сканирование сети»
Table 2. Results of simulation simulation in the CPNTools network attack environment «network scanning»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a2_1	202	45.833333	0	100	16
Marking_size_New_Page'a3_1	202	45.833333	0	100	3
Marking_size_New_Page'a4_1	202	54.166667	0	100	1

Сетевая атака «отказ в обслуживании», известна, как SYN- или TCP-flood, и DoS атаки. Основной задачей такой атаки является отказ в обслуживании.

Злоумышленник начинает одновременно посылать огромное количество SYN-пакетов с разных IP-адресов на целевой хост. Атакуемая цель при получении такого пакета формирует ответ и одновременно резервирует место в буфере для еще одного пакета, задача которого завершить соединение.

В результате, через некоторый промежуток времени, буфер переполняется, а реальные пользователи получают отказ при попытке подключиться к такому хосту, что, в конечном счете, может привести к нарушению одного из свойств информации (доступности).

На рис. 4 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «отказ в обслуживании» на информационный ресурс АС [14,17-18].

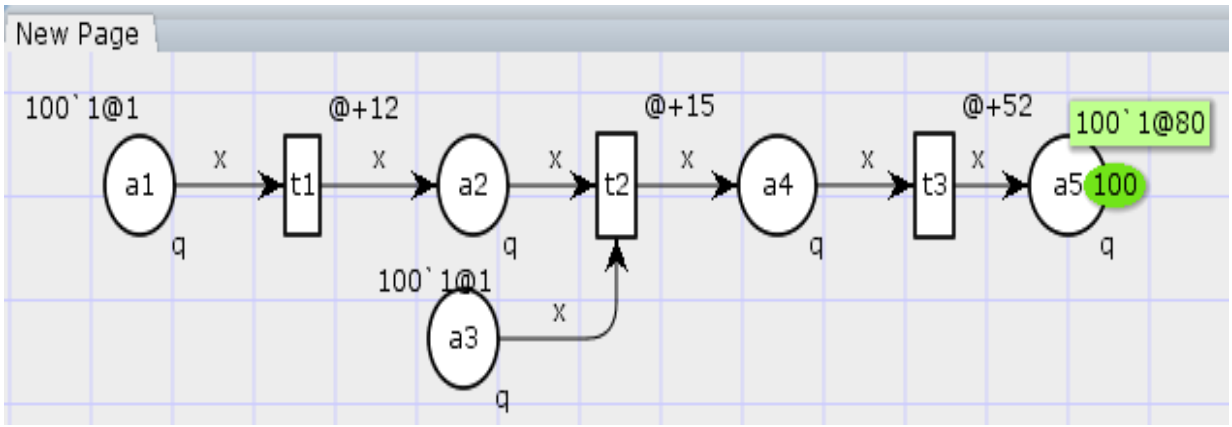

Рис.4. Графовая модель сетевой атаки «отказ в обслуживании»
Fig.4. The graph model of network attack «denial of service»

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.3.

Таблица 3.Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «отказ в обслуживании»
Table 3. Results of simulation simulation in the CPNTools software environment of the network denial-of-service attack

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	102	3.571429	0	100	1
Marking_size_New_Page'a2_1	202	42.857143	0	100	12
Marking_size_New_Page'a3_1	102	46.428571	0	100	1
Marking_size_New_Page'a4_1	202	53.571429	0	100	15
Marking_size_New_Page'a5_1	102	0.000000	0	100	52

«ARP-spoofing». Для осуществления данного типа атаки, злоумышленник должен получить доступ к компьютеру, подключенному к сети, а также к специальному программному обеспечению. Проводится необходимая настройка программного обеспечения для сканирования сети с целью выявления соответствия MAC-адресов с IP-адресами хостов. Затем происходит перехват трафика между целевыми хостами с последующей подменой таблиц MAC-адресов и ожидание подключения к удаленному хосту для получения имени пользователя и пароля. На рис.5 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «ARP-spoofing» на информационный ресурс АС [14,19].

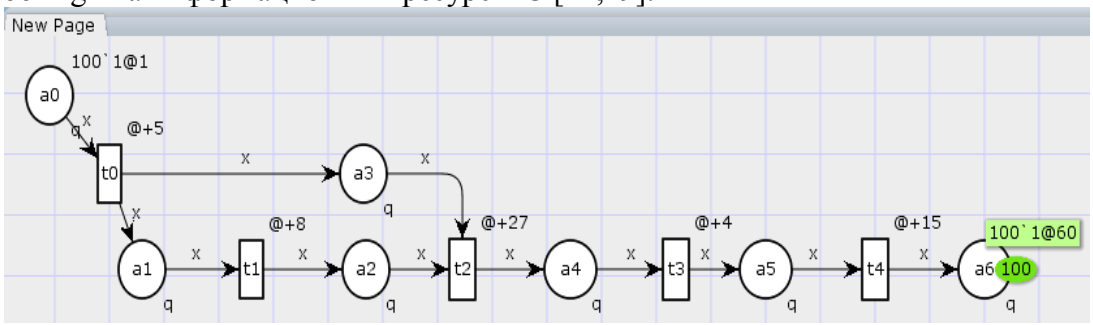

Рис.5. Графовая модель сетевой атаки «ARP-spoofing»
Fig.5. The graph model of the network attack «ARP-spoofing»

Результаты имитационного моделирования данной атаки представлены в табл.4.

Таблица 4. Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «ARP-spoofing»
Table 4. Results of simulation in the software environment CPNTools network attack «ARP-spoofing»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	202	11.111111	0	100	6
Marking_size_New_Page'a2_1	202	17.777778	0	100	8
Marking_size_New_Page'a3_1	202	28.888889	0	100	6
Marking_size_New_Page'a4_1	202	60.000000	0	100	27
Marking_size_New_Page'a5_1	202	8.888889	0	100	4
Marking_size_New_Page'a6_1	102	0.000000	0	100	15

Сетевая атака «подмена доверенного объекта сети» (IP-spoofing).

Для реализации данной атаки злоумышленнику необходимо сформировать пакеты с ложным обратным адресом. Он отправляет такой пакет атакуемому хосту, таким образом переключая на свой компьютер соединение, установленное с другим компьютером, сохраняя при этом право доступа того пользователя, соединение с которым было разорвано.

Знание конкретной реализации набора протоколов TCP/IP позволяет предсказать значение поля-счетчика, предназначенного для идентификации сообщения. Так, с помощью посылки нескольких десятков пакетов с последующим их анализом, можно определить алгоритм, используемый для установки значения счетчиков. На рис. 6 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «IP-spoofing» на информационный ресурс АС [14,19].

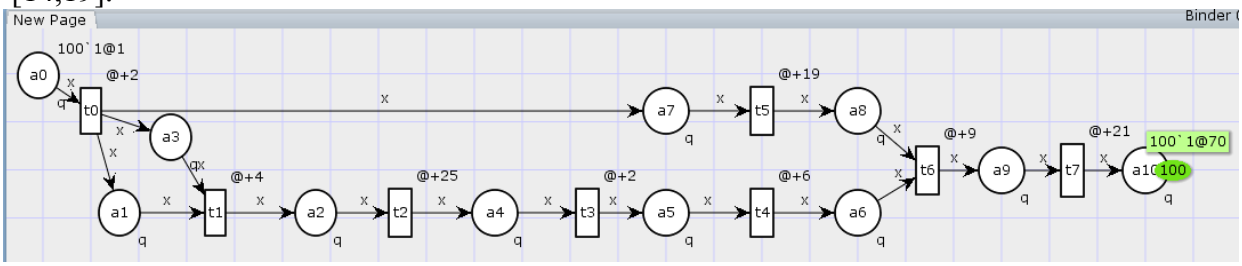

Рис.6. Графовая модель сетевой атаки «IP-spoofing»
Fig.6. The graph model of the network attack "IP-spoofing"

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.5.

Таблица 5. Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «IP-spoofing»
Table 5. Results of simulation simulation in the CPNTools software environment «IP-spoofing»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	202	4.081633	0	100	3
Marking_size_New_Page'a2_1	202	8.163265	0	100	4
Marking_size_New_Page'a3_1	202	4.081633	0	100	3
Marking_size_New_Page'a4_1	202	51.020408	0	100	25
Marking_size_New_Page'a5_1	202	4.081633	0	100	2
Marking_size_New_Page'a6_1	202	12.500000	0	100	6
Marking_size_New_Page'a7_1	202	4.081633	0	100	3
Marking_size_New_Page'a8_1	202	77.083333	0	100	19
Marking_size_New_Page'a9_1	202	18.750000	0	100	9
Marking_size_New_Page'a10_1	102	0.000000	0	100	21

Сетевая атака «перехват TCP-сессии» (IP-hijacking). Реализация данного типа атаки возможна, если у злоумышленника имеется доступ к машине, находящейся на пути сетевого потока, а также при обладании достаточными правами для генерации и перехвата пакетов.

При передаче пакетов, всегда используются два 32-битных поля-счетчика, значение которых проверяются и сервером, и клиентом. Имеется возможность ввести соединение в состояние, при котором, значения счетчиков, отправляемых сервером, не будут соответствовать значениям, которые ожидает клиент и наоборот. В таком случае становится связующим звеном

между сервером и клиентом. Такое положение дает ему возможность обхода СЗИ от НСД с одноразовыми паролями.

На рис.7 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «IP-hijacking» на информационный ресурс АС [14,19].

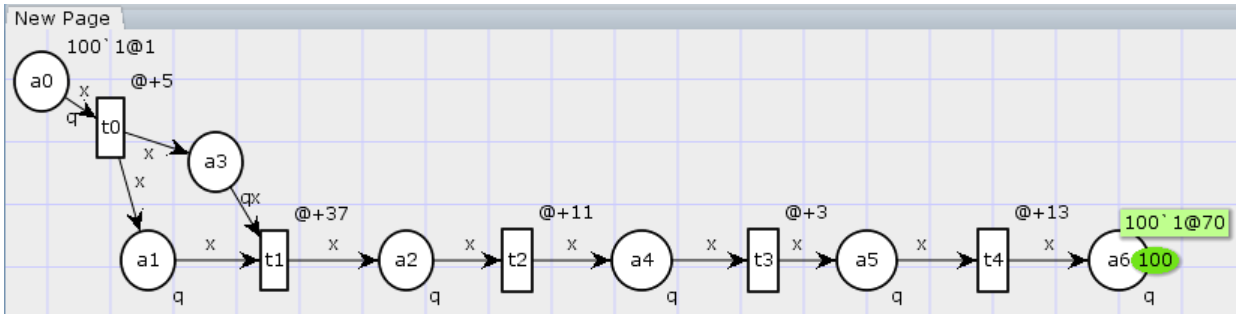

Рис.7. Графовая модель сетевой атаки «IP-hijacking»
Fig.7. Graph model of network attack «IP-hijacking»

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.6.

Таблица 6.Результаты имитационного моделирования в программной среде CPNToolscетевой атаки «IP-hijacking»
Table 6. Results of simulation simulation in the CPNTools network environment «IP-hijacking» software environment

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	202	8.928571	0	100	6
Marking_size_New_Page'a2_1	202	66.071429	0	100	37
Marking_size_New_Page'a3_1	202	8.928571	0	100	6
Marking_size_New_Page'a4_1	202	19.642857	0	100	11
Marking_size_New_Page'a5_1	202	5.357143	0	100	3
Marking_size_New_Page'a6_1	102	0.000000	0	100	13

Сетевая атака «Внедрение в сеть ложного объекта путем навязывания ложного маршрута».

Для реализации данной атаки следует подготовить ICMPRedirectHost сообщение, с указанием конечного IP-адреса и IP-адреса ложного маршрутизатора. Затем это сообщение отправляется атакуемому от имени маршрутизатора при помощи указания в поле адреса отправителя IP-адрес маршрутизатора. Имеются два варианта проведения данной удаленной атаки.

В первом случае злоумышленник находится в той же сети, что и атакуемый. Так, атакующий имеет возможность изменить маршрут передачи пакетов, что позволит получить доступ к передаваемой информации. Далее, полученная информация анализируется злоумышленником, а пакеты передаются дальше.

Во втором случае злоумышленник и атакуемый находятся в разных сетях. При такой разновидности атаки, злоумышленнику не удастся получить доступ к передаваемой информации, но у него получится нарушить работоспособность атакуемого хоста, так как связь между данным хостом и указанным в ICMP-сообщении сервером будет нарушена.

На рис.8 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «Внедрение в сеть ложного объекта путем навязывания ложного маршрута» на информационный ресурс АС [14,19].

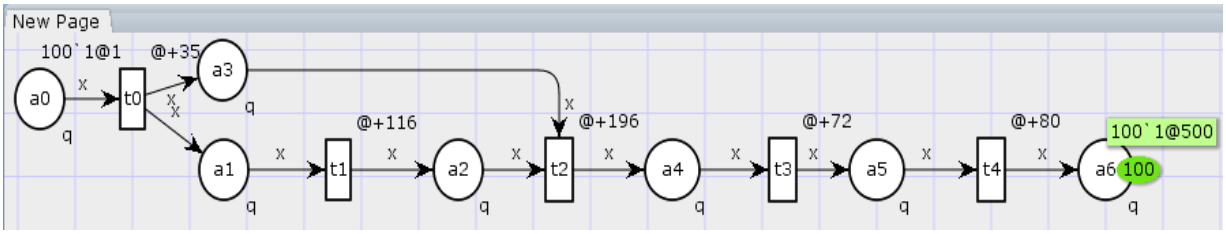

Рис.8. Графовая модель сетевой атаки «Внедрение в сеть ложного объекта путем навязывания ложного маршрута»
Fig.8. The graph model of the network attack «The introduction of a false object into the network by imposing a false route»

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.7.

Таблица 7. Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «Внедрение в сеть ложного объекта путем навязывания ложного маршрута»
Table 7. Results of simulation simulation in the CPNTools software environment of the network attack «Introduction of a false object into the network by imposing a false route»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	202	8.333333	0	100	36
Marking_size_New_Page'a2_1	202	27.619048	0	100	116
Marking_size_New_Page'a3_1	202	35.952381	0	100	36
Marking_size_New_Page'a4_1	202	46.666667	0	100	196
Marking_size_New_Page'a5_1	202	17.142857	0	100	72
Marking_size_New_Page'a6_1	102	0.000000	0	100	80

Сетевая атака «Межсегментное внедрение ложного DNS-сервера».

При реализации этой атаки злоумышленник не имеет возможности получать запрос атакуемого хоста к подлинному DNS-серверу. При реализации данной атаки необходимо определить номер порта, с которого посылается запрос, с последующим подбором идентификатора запроса.

На рис. 9 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «Внедрение в сеть ложного объекта путем навязывания ложного маршрута» на информационный ресурс АС [14].

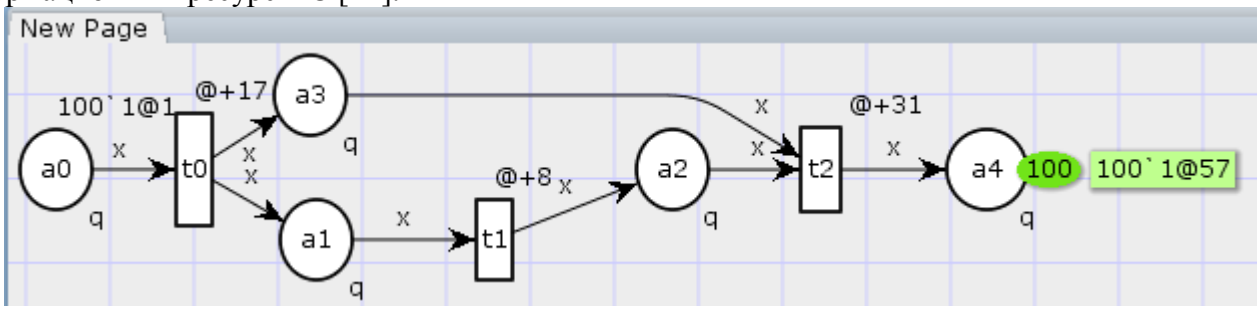

Рис.9. Графовая модель сетевой атаки «Межсегментное внедрение ложного DNS-сервера»
Fig.9. The graph model of the network attack «Intersegment implementation of a false DNS server»

При использовании программной среды CPNTools проведено имитационное моделирование данной атаки, результаты которого представлены в табл.8.

Таблица 8. Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «Межсегментное внедрение ложного DNS-сервера»
Table 8. Results of simulation simulation in the CPNTools software environment of the network attack «Intersegment implementation of a false DNS server»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	202	65.384615	0	100	18
Marking_size_New_Page'a2_1	202	30.769231	0	100	8
Marking_size_New_Page'a3_1	202	96.153846	0	100	18
Marking_size_New_Page'a4_1	102	0.000000	0	100	31

Сетевая атака «Внедрение ложного DNS-сервера».

При осуществлении данной атаки, злоумышленником перехватывается запрос атакуемого хоста к подлинному DNS-серверу. Так может быть решена задача по определению номера порта, с которого был отправлен запрос. Остается только определить идентификатор запроса, путем отправки нескольких ответов с разными идентификаторами после чего сетевая атака может быть реализована. На рис. 10 приведена графовая модель, показывающая основные этапы реализации сетевой атаки «Внедрение ложного DNS-сервера» на информационный ресурс АС [14].

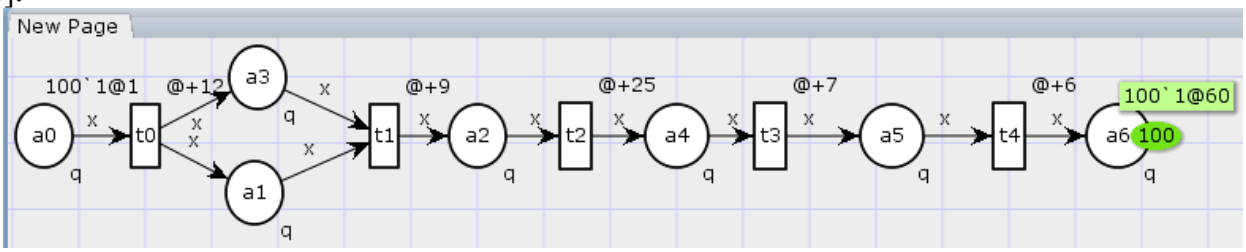

Рис.10. Графовая модель сетевой атаки «Внедрение ложного DNS-сервера»
Fig.10. The graph model of the network attack «Deployment of a false DNS server»

При использовании программной среды CPNTools проведем имитационное моделирование данной атаки, результаты которого представлены в табл.9.

Таблица 9.Результаты имитационного моделирования в программной среде CPNTools сетевой атаки «Внедрение ложного DNS-сервера»
Table 9. Results of simulation simulation in the CPNTools software environment of the network attack «Deployment of a false DNS server»

Timedstatistics					
Name	**Count**	**Avrg**	**Min**	**Max**	**TimeAvrg**
Marking_size_New_Page'a1_1	202	22.222222	0	100	13
Marking_size_New_Page'a2_1	202	16.666667	0	100	9
Marking_size_New_Page'a3_1	202	22.222222	0	100	13
Marking_size_New_Page'a4_1	202	46.296296	0	100	25
Marking_size_New_Page'a5_1	202	12.962963	0	100	7
Marking_size_New_Page'a6_1	102	0.000000	0	100	6

В качестве примера использования данной методики при решении прикладной задачи для формирования количественных требований к СЗИ от НСД воспользуемся возможностью пакета прикладных программ Matlab-2013 (где имеются встроенные генетические алгоритмы).

Исходными данными для генетического алгоритма являются ВВХ сетевых атак, представленные в результирующих таблицах CPNTools.

При эволюционном моделировании использовались следующие параметры ГА:

1) значение популяции – 100 %;
2) рулеточный отбор новой популяции;
3) мутационная допустимость – 0,5 %;
4) допустимость кроссинговера – (80 – 95) %.

Численный эксперимент ГА осуществлялся по формированию требований к СЗИ от НСД и был остановлен в связи с окончанием роста функции приспособленности (функции оптимизации) [8].

Результаты формирования требований к СЗИ от НСД при использовании эволюционных методов моделирования (генетического алгоритма, встроенного в пакет прикладных программ Matlab 2013) представлены в табл.10. В ней приведены результаты нормирования количественных требований к СЗИ от НСД вАС (показателей ν_i^j и λ_i^j результирующей марковской модели) [8].

Таблица 10. Результаты формирования требований к СЗИ от НСД при использовании эволюционных методов моделирования (генетического алгоритма, встроенного в пакет прикладных программ Matlab 2013)

Table 10. The results of the formation of requirements for GIS from NSD using the evolutionary modeling methods (the genetic algorithm built into the Matlab 2013 application package)

№ п.п.	Наименование атаки	Вид параметров модели защиты	Параметр времени реализации ν_i^j	Интенсивность реализации λ_i^j
Сбор информации о топологии и принципах функционирования информационной системы (Probes)				
1	Сканирование сети	$\nu_1^1 \lambda_1^1$	0.02	2e-6
2	Сниффинг пакетов в сети без коммутаторов	$\nu_1^2 \lambda_1^2$	0.08	1,3e-5
Непосредственное проникновение в информационную систему (RemotetoLocalUserAttacks)				
3	Внедрение в сеть ложного объекта на основе недостатков алгоритмов удаленного поиска (ARP-spoofing)	$\nu_2^1 \lambda_2^1$	0.06	9,1e-3
4	Внедрение в сеть ложного объекта путем навязывания ложного маршрута	$\nu_2^2 \lambda_2^2$	0.5	5,2e-3
5	Подмена доверенного объекта сети (IP-spoofing)	$\nu_2^3 \lambda_2^3$	0.07	7,4e-4
6	Перехват TCP-сессии (IP-hijacking)	$\nu_2^4 \lambda_2^4$	0.07	5,2e-7
7	Внедрение ложногоDNS-сервера	$\nu_2^5 \lambda_2^5$	0.06	1,22e-5
8	Межсегментное внедрение ложного DNS-сервера	$\nu_2^6 \lambda_2^6$	0.057	2,41e-6
Установление контроля над информационной системой (UsertoRootAttacks)				
9	«Отказ в обслуживании» (SYN-flood)	$\nu_3^1 \lambda_3^1$	0.08	1,5e-3

Вывод. В настоящее время получение количественных значений ВВХ, связанных с сетевыми атаками, являются довольно сложной проблемой. Это вызвано тем, что в открытой печати по конкретным результатам реализации угроз отсутствует реальная статистика, которая необходима при решении прикладных задач в области информационной безопасности. Результаты и статистические данные, полученные с помощью программной среды имитационного моделирования CPNTools позволяют решать широкий спектр выше упомянутых задач.

В данной статье разработана методика исследования ВВХ реализации сетевых атак в программной среде имитационного моделирования CPNTools, ценность которой состоит в получении количественных значений ВВХ сетевых атак к информационному ресурсу АС. Они позволяют решать широкий спектр прикладных задач, связанных с защитой информации в АС, к которым можно отнести:

1) Проектирование СЗИ от НСД в АС на основе оценки их эффективности функционирования;

2) Разработка перспективных и доработка существующих АС, функционирующих в защищенном исполнении;

3) Сертификация объектов информатизации;

4) Разработка методики вычислительного эксперимента с целью исследования ВВХ СЗИ от НСД в АС при их создании и модификации.

5) Формирование требований к СЗИ от НСД в АС.

Библиографический список:

1. ФСТЭК РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. [Электронный ресурс]. URL:http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3.
2. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении. [Электронный ресурс]. – URL:http://docs.cntd.ru/document/1200108858.
3. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. [Электронный ресурс]. –URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g.
4. ГОСТ 34.601-90. Автоматизированные системы. Стадии создания. [Электронный ресурс]. – URL:http://www.insapov.ru/gost-34-601-90.html.
5. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Воениздат, 1992.
6. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.[Электронный ресурс]. – URL:http://fstec.ru/component/attachments/download/299.
7. Приказ МВД России от 14.03.2012 №169. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года. [Электронный ресурс]. – URL: http://policemagazine.ru/forum/showthread.php?t=3663.
8. Методы и средства эволюционного моделирования при обосновании требований к программным систем защиты информации: монография / Змеев А.А., Мачтаков С.Г., Мещерякова Т.В, Никулина Е.Ю., Рогозин Е.А., Стукалов В.В., Хвостов В.А.; под ред. Е.А. проф. Рогозина. Воронеж: Воронежский институт МВД России, 2014. 74 с.
9. Рогозин Е.А., Попов А.Д., Шагиров Т.В. Проектирование систем защита информации от несанкционированного доступа в автоматизированных системах органов внутренних дел//Вестник Воронежского института МВД России. 2016. № 2. С. 174 183.
10. Дровникова И. Г., Мещерякова Т. В., Попов А. Д, Рогозин Е. А., Ситник С.М. Математическая модель оценки эффективности систем защиты информации с использованием преобразования Лапласа и численного метода Гивенса // Труды СПИИРАН. 2017. № 3 (52). С. 234258. DOI 10.15622/sp.52.11
11. Банк данных угроз ФСТЭК РФ. [Электронный ресурс]. – URL: http://bdu.fstec.ru/threat.
12. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students'book. – Odessa: ONAT, 2006. 60 p.
13. Kurt Jensen, Lars M. Kristensen. Coloured Petri Nets. Modelling and Validation of Concurrent Systems // Springer-Verlag Berlin Heidelberg. 2009. 384 p.
14. Wil van der Aalst; Christian Stahl.Modeling Business Processes - A Petri Net-Oriented Approach // Massachusetts Institute of Technology. 2011. 400 p.
15. Радько Н.М., Язов Ю.К., Корнеева Н.Н. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа : учеб.пособие – Воронеж : ФГБОУ ВПО «Воронежский государственный технический университет», 2013. 263 с.
16. Sheng Ding, Na Xia, Peipei Wang, Shaojie Li, Yuanxiao Ou, "Optimization Algorithm Based on SPSA in Multi-channel Multi-radio Wireless Monitoring Network", Cyber-Enabled Distributed Computing and Knowledge Discov-

ery (CyberC) 2015. International Conference on, pp. 517-524, 2015.

17. Masoud Hasanifard, Behrouz Tork Ladani. "DoS and port scan attack detection in high speed networks", Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on, pp. 61-66, 2014.
18. Muniyandi A.P., et al., " Network Anomaly Detection by Cascading KMeans Clustering and C4.5 Decision Tree algorithm, " Procedia Engineering, vol. 30, pp. 174-182, 2012.
19. Pengfei Zhang, Sai Ganesh Nagarajan, Ido Nevat, "Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things" IEEE Internet of Things Journal, vol. 4, Issue: 6, pp 2199-2206, 2017.

References:

1. FSTEK RF. Rukovodyashchii dokument. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya. [Elektronnyiresurs]. URL1: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3. [FSTEC of the Russian Federation. Guidance document. Protection against unauthorized access to information. Terms and Definitions. [Electronic resource] URL1: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3. (In Russ.)]
2. GOST R 51583-2014. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii [Elektronnyiresurs]. URL: http://docs.cntd.ru/document/1200108858. [GOST R 51583-2014. The order of creation of the automated systems in the protected execution [Electronic resource]. URL: http://docs.cntd.ru/document/1200108858. (In Russ.)]
3. FSTEK RF. Rukovodyashchii dokument. Sredstva vychislitel'noi tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii [Elektronnyiresurs]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g. [FSTEC of the Russian Federation. Guidance document. Means of computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information [Electronic resource]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g. (In Russ.)]
4. GOST 34.601-90. Avtomatizirovannye sistemy. Stadii sozdaniya. [Elektronnyiresurs]. URL:http://www.insapov.ru/gost-34-601-90.html. [GOST 34.601-90. Automated systems. Stages of creation. [Electronic resource]. URL:http://www.insapov.ru/gost-34-601-90.html. (In Russ.)]
5. FSTEK RF. Rukovodyashchii dokument. Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. M.: Voenizdat, 1992. [FSTEC of the Russian Federation. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information security. Moscow: Voenizdat, 1992. (in Russ.)]
6. FSTEK RF. Rukovodyashchii dokument. Kontseptsiya zashchity sredstv vychislitel'noi tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii [Elektronnyiresurs]. URL: http: //fstec.ru/component/attachments/download/299. [FSTEC of the Russian Federation. Guidance document. The concept of protecting computer facilities and automated systems from unauthorized access to information [Electronic resource]. URL: http: //fstec.ru/component/attachments/download/299. (In Russ.)]
7. Prikaz MVD Rossiiot 14.03.2012 №169. Ob utverzhdenii Kontseptsii obespecheniya informatsionnoi bezopasnosti organov vnutrennikh del Rossiiskoi Federatsii do 2020 goda. [Elektronnyiresurs]. URL: http://policemagazine.ru/forum/showthread.php?t=3663. [Order of the Ministry of Internal Affairs of Russia from 14.03.2012 №169. About the statement of the Concept of maintenance of information security of law-enforcement bodies of the Russian Federation till 2020. [Electronic resource]. URL: http://policemagazine.ru/forum/showthread.php?t=3663. (in Russ.)]
8. Zmeev A.A., Machtakov S.G., Meshcheryakova T.V, NikulinaE.Yu., Rogozin E.A., Stukalov V.V., Khvostov V.A. Metody i sredstva evolyutsionnogo modelirovaniya pri obosnovanii trebovanii k programmnym sistem zashchity informatsii. Monografiya (pod red. E.A. Rogozina). Voronezh: Voronezhskii institut MVD Rossii; 2014. 74 s. [Zmeev A.A., Machtakov S.G., Meshcheryakova T.V, NikulinaE. Yu., Rogozin E.A., Stukalov V.V., Khvostov V.A. Methods and means of evolutionary modeling in substantiating the requirements for software information security systems. Monograph (edited by E.A. Rogozin). Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russian Federation; 2014. 74 p. (in Russ.)]
9. Rogozin E.A., Popov A.D., Shagirov T.V. Proektirovanie sistem zashchity informatsii ot nesanktsionirovannogo

dostupa v avtomatizirovannykh sistemakh organov vnutrennikh del. VestnikVoronezhskogo instituta MVD Rossii. 2016; 2:174-183. [Rogozin E.A., Popov A.D., Shagirov T.V. Designing of information security systems against unauthorized access in automated systems of internal affairs bodies. Vestnik of Voronezh Institute of the Ministry of the Interior of Russia. 2016; 2:174-183. (In Russ.)]

10. Drovnikova I.G., Meshcheryakova T.V., Popov A.D, Rogozin E.A., Sitnik S.M. Matematicheskaya model' otsenki effektivnosti sistem zashchity informatsii s ispol'zovaniem preobrazovaniya Laplasa i chislennogo metoda Givensa. Trudy SPIIRAN. 2017; 3(52):234-258. DOI 10.15622/sp.52. [Drovnikova I.G., Meshcheryakova T.V., Popov A.D, Rogozin E.A., Sitnik S.M. A mathematical model for evaluating the effectiveness of information security systems using the Laplace transform and the Givens numerical method. Proceedingsof SPIIRAN. 2017; 3(52):234-258. DOI 10.15622/sp.52. (In Russ.)]
11. Bank dannykhugroz FSTEK RF. [Elektronnyiresurs]. URL: http://bdu.fstec.ru/threat. [FSTEC RF Database of Threats [Electronic resource]. URL: http://bdu.fstec.ru/threat. (In Russ.)]
12. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students'book. Odessa: ONAT; 2006. 60 p.
13. Jensen K., Kristensen L.M. Coloured Petri Nets. Modelling and Validation of Concurrent Systems. Springer-Verlag Berlin Heidelberg; 2009. 384 p.
14. Van der Aalst W., Stahl C. Modeling Business Processes - A Petri Net-Oriented Approach. MassachusettsInstituteofTechnology; 2011. 400 p.
15. Rad'ko N.M., YazovYu.K., Korneeva N.N. Proniknoveniya v operatsionnuyu sredu komp'yutera: model i zloumyshlennogo udalennogo dostupa: ucheb.posobie. Voronezh: FGBOU VPO «Voronezhskii gosudarstvennyi tekhnicheskii universitet»; 2013. 263 s. [Rad'ko N.M., YazovYu.K., Korneeva N.N. Penetrations into the operating environment of the computer: malicious remote access models: tutorial. Voronezh: Voronezh State Technical University; 2013. 263 p. (In Russ.)]
16. Ding S., Xia N., Wang P., Li S., Ou Y. Optimization Algorithm Based on SPSA in Multi-channel Multi-radio Wireless Monitoring Network. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) International Conference. 2015. P. 517-524.
17. Hasanifard M., Ladani B.T. DoS and port scan attack detection in high speed networks. Information Security and Cryptology (ISCISC) 11th International ISC Conference. 2014. P. 61-66.
18. Muniyandi A.P. et al. Network Anomaly Detection by Cascading KMeans Clustering and C4.5 Decision Tree algorithm. Procedia Engineering. 2012;30:174-182.
19. Zhang P., Nagarajan S.G., Nevat I. Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things. IEEE Internet of Things Journal. 2017;4(6):2199-2206.

Сведения об авторах:

Дровникова Ирина Григорьевна – доктор технических наук, доцент, кафедра автоматизированных информационных систем органов внутренних дел.

Змеев Анатолий Анатольевич – соискатель.

Попов Антон Дмитриевич – адъюнкт.

Рогозин Евгений Алексеевич – доктор технических наук, профессор, кафедра автоматизированных информационных систем органов внутренних дел.

Information about the authors:

Irina G. Drovnikova – Dr. Sci. (Technical), Assoc. Prof., Department of Automated Information Systems.

Anatoly A.Zmeev – Doctoral candidate.

Anton D. Popov – Adjunct.

Evgenii A. Rogozin – Dr. Sci. (Technical), Prof., Department of Automated Information Systems .

Конфликт интересов. **Conflict of interest**.

Авторы заявляет об отсутствии конфликта интересов. The authors declare no conflict of interest.

Поступила в редакцию 15.09.2017. **Received** 15.09.2017.

Принята в печать 20.11.2017. **Accepted for publication** 20.11.2017.