Михаил Б. Абросимов, Ихаб А. Камил
СГУ имени Н.Г.Чернышевского,
ул. Астраханская, 83, г. Саратов, 410012, Россия
e-mail: mic@rambler.ru, https://orcid.org/0000-0002-4473-8790
e-mail: kamil.iehab@mail.ru, https://orcid.org/0000-0003-1100-5635

РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И СИСТЕМЫ ОТКАЗОУСТОЙЧИВОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.06

Аннотация. Одной из первых угроз побудивших создание систем предотвращения вторжений считают «червь Морриса», который поразил компьютеры в конце 1988г. Системы предотвращения вторжений развивались, и со временем стали полноценной системой, включающей в себя специальные проактивные методы предотвращения атак, рассчитанные для защиты от различного рода угроз. Среди проактивных систем предотвращения вторжений можно выделить следующие: поведенческий анализатор процессов для анализа поведения запущенных в системе процессов, системы устранение возможностей попадания инфекции на компьютер, системы блокировка портов, системы блокировки DoS-атак.

В статье описывается разработанная система предотвращения вторжений. Цель работы раскрыть возможности использования параллельных потоков для улучшения работы систем предотвращения вторжений. Эффективность разрабатываемой системы достигается за счет организации предотвращение атак на уровне конкретного узла, путем контроля всех системных вызовов. Система служит посредником между открытой и защищенной средой. Для повышения скорости передачи/приема информации в системе была использована технология отказоустойчивости. Актуальность темы определяется ростом бесчисленного количества разнообразных вредоносных программ, и возрастающей необходимости в защите корпоративной информации.

Ключевые слова: системы предотвращения вторжений, безопасное соединение, отказоустойчивость, параллельное программирование, вирусы, технология виртуализации, вредоносный трафик.

Для цитирования. ***АБРОСИМОВ, Михаил Б.; КАМИЛ, Ихаб А.*** *РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И СИСТЕМЫ ОТКАЗОУСТОЙЧИВОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 65-73, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1094>. Дата доступа: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.06.*

Mikhail B. Abrosimov, Iehab A. Kamil
Saratov state University named after N. G. Chernyshevskogo,
St. Astrakhanskaya, 83, Saratov, 410012, Russia
e-mail: mic@rambler.ru, https://orcid.org/0000-0002-4473-8790
e-mail: kamil.iehab@mail.ru, https://orcid.org/0000-0003-1100-5635

Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology

DOI: http://dx.doi.org/10.26583/bit.2018.1.06

Abstract. One of the first threats that prompted the creation of intrusion prevention systems is considered to be the "Morris worm", which hit computers in late 1988. Intrusion prevention systems evolved, and eventually became a full-fledged system incorporating special proactive methods to prevent attacks, designed to protect against various kinds of threats. Among the proactive intrusion prevention systems are the following: a behavioral process analyzer for

analyzing the behavior of processes running in the system, eliminating the possibility of infection on the computer, locking the ports, blocking the DoS attacks.
In article the developed system of prevention of invasions is described. It is more effective to develop and use the systems of prevention of invasions as separate means of protection which will serve as the intermediary between the protected and opened networks. It is more expedient to organize prevention of the attacks at the level of concrete knot, by control of all system calls. Special attention in article is paid to use of technologies of parallel programming in the developed system. The main advantages of system of fault tolerance and the used algorithms for realization of technology of prevention of invasions are described.
Keywords: the intrusion prevention system, secure communication, fault tolerance, parallel programming, viruses, virtualization, malicious traffic.
For citation. ***ABROSIMOV, Mikhail B.; KAMIL, Iehab A.*** *Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology. IT Security (Russia), [S.l.], v. 25, n. 1, p. 65-73, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1094>. Date accessed: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.06.*

Введение

Системы предотвращения вторжений – это современные технологии защиты, построенные на анализе поведения. Решения, которые раньше помогали, становятся неэффективными против некоторых видов угроз. Многие вирусы умеют адаптироваться, изменять размер, имена файлов, процессов и служб [1]. Процесс обнаружения и предотвращения атак на уязвимости, как таковой, подразумевает анализ и реакции на события: нарушения политик безопасности, политик использования ресурсов, политик стандартизации. Инциденты могут иметь любую природу, например, вредоносный код, неавторизованный доступ или попытки получения дополнительных прав. Системы предотвращения вторжения умеют непосредственно воздействовать на такие компоненты атаки, как тело атаки, например, обрыв соединения; среда безопасности, например, переконфигурирование для запрета сетевого доступа в сегмент; содержимое атаки, или удаление вредного аттачмента. Если нельзя обнаружить потенциальную опасность файла по внешним признакам, можно определить его вредоносную природу по поведению. Именно поведенческим анализом занимается система предотвращения вторжений.

IPS-системы корпорации Cisco

Cisco предоставляет решения по управлению IPS для развертываний любого размера, от небольших организаций до крупных предприятий. Cisco IPS Manager Express представляет собой полнофункциональное приложение для управления системами IPS и формирования отчетов по этим системам, поддерживающее до 10 устройств. Cisco Security Manager представляет собой решение управления безопасностью корпоративного класса с тысячами реальных развертываний. Кроме того, имеется полнофункциональный локальный интерфейс командной строки.

Cisco IPS Manager Express и Cisco Security Manager поддерживают устройства Cisco IPS серии 4500, а также другие сенсоры Cisco IPS. Cisco Security Manager 4.x предоставляет следующие функции:

- Гибкие процессы для поэтапной поставки новых и обновленных сигнатур, а также создания политик для IPS относительно этих сигнатур с последующим распространением политик на другие устройства;
- Поддержка расширенной отчетности и управления событиями для новейших функций IPS Cisco, включая глобальную корреляцию;
- Контроль доступа на основе ролей и рабочие процессы для обеспечения безошибочных, тразвертываний и соответствия установленным требованиям.

Cisco IPS Manager Express предоставляет следующие функции:

- Подготовку, мониторинг и устранение неполадок
- Перетаскиваемые устройства панели мониторинга для простоты настройки

– Персонализированные области просмотра, которые запоминают параметры пользователя, чтобы минимизировать время настройки и управления
– Гибкое средство создания отчетов, которое позволяет создавать настраиваемые отчеты и отчеты по соответствию нормативным требованиям в течение секунд
– Предварительно определенные шаблоны настройки, привязанные к объекту.

Системы защиты от Cisco на сегодняшний день являются лидерами во многих странах мира, в том числе и в России. Несмотря на все преимущества данной системы, существует главный недостаток – это большие финансовые затраты при внедрении.

Интегрированная система предотвращения вторжений

Существует два типа IPS: отдельные (или специальные) и интегрированные. Cisco IPS Manager Express относится к первому типу систем. Отдельные IPS обеспечивают:

– дополнительный уровень сетевой защиты от вторжений;
– возможность установки посредством выделенного специализированного оборудования.

Интегрированные IPS предлагают:

– комплексную систему защиты от вторжений по всей инфраструктуре безопасности;
– возможность интеграции в существующие узлы безопасности, как правило, в межсетевые экраны.

Разрабатываемая система относится к интегрированным системам предотвращения вторжений – что требует минимальных затрат на внедрение защиты. Система базируется на операционной системе Linux, что позволяет использовать встроенные средства штатного пакетного фильтра операционной системы Linux для подключения которого используются библиотеки netlink-queue и libnfnetlink. Они позволяют наблюдать за файлами, процессами и службами при поиске подозрительной активности. В случае подозрительной активности происходит блокировка вредоносных программ по критерию опасного выполнения кода – это позволяет поддерживать оптимальную безопасность системы без необходимости обновления баз [2, с.8]. Система позволяет управлять входящим и исходящим трафиком, основываясь на наборах правил, а также запуском и работой процессов на основании выполняемых изменений в компьютере согласно правилам контроля. Выделим основные сигнатуры угроз, определенные в системе (рис.1).

Для аудита системы ведется системный журнал – в котором регистрируются нетипичные поведения системы, которые распознаются благодаря заранее определенным сценариям вторжений (известные шаблоны атак). Например, при атаке TearDrop по типу «отказ в обслуживании» (Denial of Service, DoS) рассылаемые пакеты фрагментированы таким образом, что это вызывает крах атакуемой системы. На основе журнала формируется черный список IP-адресов, что позволяет предотвратить подключение к ботнетам, источникам спама и другим вредоносным IP-адресам.

Благодаря комбинации правил IPS с учетом уязвимостей, пользовательских правил, интеллектуального механизма анализа IP-адресов и возможностей оценки файлов интегрированная система имеет в своем распоряжении более широкий арсенал средств для защиты своих систем, и низкую – стоимость внедрения [3].

Разработанная система:

– анализирует входной трафик;
– принимает решения о блокировке трафика, для обеспечения надежного удаленного управления системой.
– помещает данные об угрозах в журнал;
– присваивает угрозе индекс вредоносного поведения;
– осуществляет соединение по параллельным каналам.

Средства конфигурирования должны быть удобны конечным пользователям, с этой целью была добавлена возможность определения правил обнаружения угроз

пользователями. Эта функция доступна в режиме online. Она позволяет, пропуская трафик через себя, не изменяя скорость работы системы [4, с.119]. Помимо проверки входных данных система обеспечивает сборку и передаваемых пакетов, анализируя данные пакетов для обнаружения следов опасной активности.

```
// создание нового потока для организации сигнатурного способа защиты
void * pthread_capture_tcp(void *arg);
```

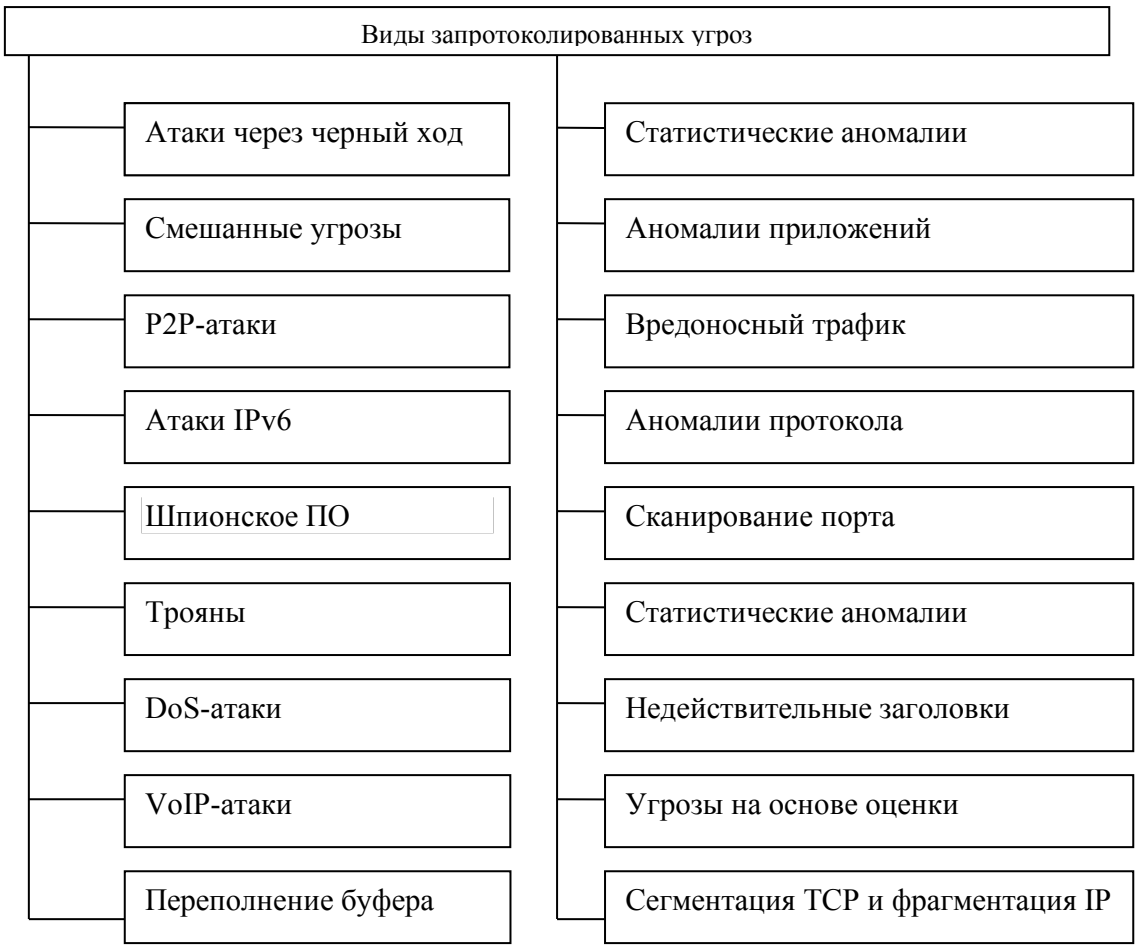

Рис. 1. Виды запротоколированных угроз
(Fig.1. Types of logged threats)

При передачи данных система устанавливает начальное число последовательности пакетов, и ряд других переменных, связанных с этим соединением. Числа последовательностей выбираются случайно на обоих сторонах. Клиентом выбирается случайное число X и отправляет SYN-пакет, который может также содержать дополнительные флаги TCP и значения опций. Сервером определяется случайное число Y, которое прибавляет 1 к значению X и отправляется ответ. В итоге завершение обмена данными происходит после прибавления 1 к значениям X и Y и отправления ACK-пакета [5].

В случае выявления подозрительных действий вредоносной программой или злоумышленником, система заблокирует данную активность (рис. 2).

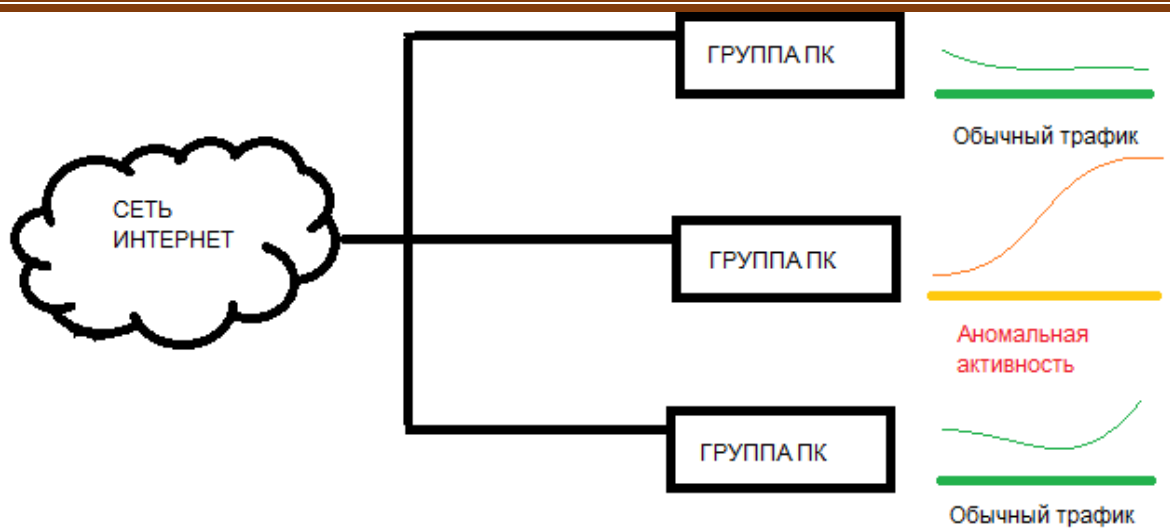

Рис. 2. Технология обнаружение уязвимостей
(Fig.2. Technology detection of vulnerabilities)

После обнаружения опасной уязвимости система реагирует на сетевую активность эксплойтов, которые используют данную уязвимость. Система предотвращения вторжений, заблокирует такой трафик заблаговременно, до достижения, им атакуемого сервера или рабочей станции [6, с.312]. Если запрос в базу не позволяет установить диспозицию файла, то она отправляется в хранилище, где производится подробный анализ: определяется его способность к сохранению после перезагрузки, проверяется трафик, генерируемый приложением, а также создаваемые процессы, записи реестра и техники скрытия процессов. В результате анализа присваивается индекс вредоносного поведения.

Разработанная система позволит отследить следующие действия:

- передачу управления другими установленными программами;
- внесение изменений в записи системного реестра;
- несанкционированное отключение программ;
- организацию межпроцессорного доступа к памяти, который позволяет внедрять вредоносный код в доверительную программу;
- а также изменения, выполняемые другими программами [7, с.63].

При использовании для защиты технологии предотвращения вторжений, контролируя параметры сессии (IP, номер порта, состояние связей), можно изучить пакет, анализируя передаваемые и получаемые данные [8, с.105].

```
if (setsockopt(raw_socket, IPPROTO_IP, IP_HDRINCL, &optval, sizeof(optval)) < 0)
{
  cerr << "Error: setsockopt(...IP_HDRINCL...)." << endl;
  exit(EXIT_FAILURE);
 }
 // Добавление сокета IP_DONTFRAG как отдельный фрагмент флага
 if (setsockopt(raw_socket, IPPROTO_IP, IP_MTU_DISCOVER, &frag, sizeof(frag)) <
0) {
  cerr << "Error: setsockopt(...IP_DONTFRAG...)." << endl;
  exit(EXIT_FAILURE);
 }
```

В разработанной системе осуществляется более глубокая проработка алгоритма функционирования прикладных протоколов (контроль состояния сеансов) (рис.3).

Рис. 3. Основные угрозы и методы их решения
(Fig.3. The main threats and methods for solving them)

Добавление профилирования трафика, и организация централизованного управления системой предотвращения вторжений, позволяют улучшить точность обнаружения вторжений [9, с.240].

Данную технологию можно использовать для организации безопасной системы, что и было использовано в разработанной системе [10, с.107].

Параллельные потоки в интегрированной системе IPS

Развитие технологий параллельного программирования привело к эффективному использованию вычислительных ресурсов многопроцессорных систем и их вычислительных ресурсов [11, с.89]. Использование технологии параллельного программирования в работе приложения, позволило реализовать дополнительные механизмы защиты. С помощью генерации параллельных потоков данных выявляются возможные аномалии, например, при организации механизма отслеживания многократного введения паролей для входа в систему [12, с.49].

```
// создаем новый поток
if (pthread_create(&thread,
NULL, // создание потока со стандартными атрибутами
pthread_capture_tcp,
NULL (!= 0) {
cerr << "Error: pthread_create().\n" << endl;
exit(status);
}
```

Используя данные из потока, системой создаются счетчики, сохраняющиеся для последующего использования.

Параллельно организованные потоки позволяют быстро подключать нужные элементы для захвата, декодирования, анализа и обработки пакетов. Это позволяет не снижать скорость приема/передачи данных, а также увеличивать пропускную способность системы.

Решение проблемы отказоустойчивости в системах предотвращения вторжений является одной из приоритетных, потому что в случае выхода из строя системы, в канале образуется затор, и трафик не доходит до адресата [13, с.50].

В разработанной системе для бесперебойного доступа созданы параллельные процессы. Процесс отправляет устройству heartbeat-пакеты, это позволяет не терять соединения в случае обрыва канала [14]. При возникновении сбоя работы встроенного приложения, система автоматически направит трафик в обход отказавшего устройства. Параллельно с этим происходит восстановление состояния системы до ближайшей

контрольной точки состояния вычислений. Данные для восстановления хранятся в специальных репозиториях.

Адаптивный подход, реализованный в системе позволяет продолжить вычисления на оставшихся работоспособных узлах без аварийного завершения работы системы. Это происходит благодаря трансляции найденных локальных значений соседним узлам. То есть на каждом узле хранится локальный экземпляр списка сохраненных задач, который сохраняет все подзадачи данного узла и пересылает их на другие соседние узлы. После завершения работы системы отчет отправляется на родительский узел, и удаляется из списка сохраненных.

Реализованный подход позволяет определять все сбои и вычислять необходимые подзадачи для отказоустойчивости системы. Совместное использование методов параллельного программирования и основных принципов отказоустойчивости позволяет перейти к реализации концепции локальной синхронизации и корректной завершаемости вычислительных приложений.

Тестирование системы

Для тестирования созданной системы использовался программный пакет BreakingPoint Virtual Edition фирмы IXIA. С его помощью искусственно было увеличено количество SYN-запросов до 12000 в секунду и произведены атаки IP-адреса с постоянной скоростью 6000 SYN в секунду. На следующем этапе было возвращено исходное значение в 12000 (достаточно для имитации DDoS-защиты, для обнаружения SYN-флуд-атаку). Для одиночных серверов был установлен порог срабатывания 3000 чтобы обеспечить то, что одиночные сервера не получат DDoS атаку при превышении лимита для всей платформы в 30000.

По результатам теста были сделаны следующие выводы:

- Система уменьшает скорость срабатывания защиты с 50 минут вначале тестов до 5 минут.
- Нет перебоев в работе, при обнаружении атаки.
- Необходимо около 15 секунд в тесте чтобы определить атаку
- Необходимо заранее подготовить персонал к действиям в случае атаки.
- При повторном тестировании система сократила время реагирования до 15 минут.

Заключение

Таким образом, системы предотвращения вторжений являются важным элементом многоуровневой защиты. Для оптимальной и эффективной работы IPS пользователь должен обладать определенными знаниями и квалификацией. Разработанная система предотвращения вторжений, имея достаточные полномочия, позволяет прекращать активность вредоносной программы. Если для остановки работы опасной программы требуется подтверждение пользователя, эффективность системы мала. Система предотвращения вторжений включает в себя определенный набор правил, который может применить пользователь. Правильное администрирование системы позволяет избежать появления конфликтов программного обеспечения и системы.

Увеличение пропускной способности сети привело к увеличению скорости обмена данными, снижению стоимости Интернет трафика. Разработанная система позволяет, используя систему предотвращения вторжений и технологию параллельного программирования организовать эффективную работу по организации безопасности системы.

СПИСОК ЛИТЕРАТУРЫ:

1 Спатулас Г.П., Катсикас С.К. Методы пост-обработки оповещений при обнаружении вторжений: опрос. Международный журнал информатики безопасности №2, 2013. с. 64-80. URL: http://www.ijiss.org/ijiss/index.php/ijiss/article/view/50/pdf_8. (Дата обращения: 10.12.2017).
2 Annual Security Report URL: http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html (дата обращения: 20.11.2017).
3 James P. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Co., 1980.
4 Denning D. An intrusion detection model. Proc. of IEEE Symposium on Security and Privacy, 1987, pp.118–131.
5 Глебов М., Селищев И. Системы предотвращения вторжений «из коробки». Тест-драйв. URL: https://habrahabr.ru/company/it/blog/209714/. (дата обращения: 12.12.2017).
6 Правиков Д. И., Закляков П. В. Использование виртуальных ловушек для обнаружения телекоммуникационных атак. Проблемы управления безопасностью сложных систем: Труды международной конференции. Москва, декабрь 2011 г./ Под ред. Архиповой Н. И. и Кульбы В. В. Часть 1. М.: РГГУ - Издательский дом МПА-Пресс. 342 с., с 310-314.
7 Брюховецкий А.А., Сосоновский Ю.В., Милюков В.В. Фундаментальное исследование в области методов построения систем обнаружения и предотвращения сетевых вторжений. Вестник СЕВНТУ. 2014. № 154.С. 60-63.
8 Баччелли Ф., Рыбко Н.А., Шлосман С.Б. Сети массового обслуживания с подвижными приборами – предел среднего поля. Проблемы передачи информации. 2016, том 52:2, 86–110.
9 Пузырьков Д.В., Подрыга О.П., Поляков С.В. Параллельная обработка и визуализация для результатов моделирования методом молекулярной динамики Труды Института системного программирования РАН. Том 28, №2, 2016 г. С. 221-242.
10 Taheri S. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications. 22, June 2015, Pages 99-112 URL: https://doi.org/10.1016/j.jisa.2014.09.003 (дата обращения: 12.12.2017).
11 Taheri S. Hartung S. Anonymous group-based routing in MANETs. Journal of Information Security and Applications. Volume 22, June 2015, Pages 87-98. https://doi.org/10.1016/j.jisa.2014.09.002 (дата обращения: 12.12.2017).
12 Вьюкова Н.И., Галатенко В.А., Сумборский С.В. Поддержка параллельного и конкурентного программировнаия в языке C++. Журнал «Программирование». 2017. № 5 С. 48-59
13 Хорошилов А.В., Щепетков И.В. ADV_SPM — Формальные модели политики безопасности на практике Труды Института системного программирования РАН. Том 29, № 3, 2017 г. С. 43-56.
14 Fua Y., Koné O. Model based security verification of protocol implementation. Journal of Information Security and Applications. 22, June 2015, Pages 17-27 URL: https://doi.org/10.1016/j.jisa.2014.08.002 (дата обращения: 12.12.2017).

REFERENCES:

[1] Spatulas G.P., Katsikas S.K. Methods of post-processing of alerts in intrusion detection: a survey. International journal of safety Informatics №2, 2013. p.64-80. URL: http://www.ijiss.org/ijiss/index.php/ijiss/article/view/50/pdf_8. (Data obrashhenija: 10.12.2017). (in Russian).
[2] Annual Security Report URL: http://www.cisco.som /c/m/en_us/offers/ sc04/2016- annual- security -report/ index .html (data obrashhenija: 20.11.2017).
[3] James P. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Co., 1980.
[4] Denning D. An intrusion detection model. Proc. of IEEE Symposium on Security and Privacy, 1987, pp.118–131.
[5] Glebov M., Selishhev I. Intrusion prevention systems "out of the box". Test-drive. URL: https://habrahabr.ru/ company/it/blog /209714/. (data obrashhenija: 12.12.2017). (in Russian).
[6] Pravikov D. I., Zakljakov P. V. The use of virtual traps for detection of telecommunication attacks. Security management problems of complex systems: Proceedings of the international conference. Moskva, dekabr' 2011 g. Pod red. Arhipovoj N. I. i Kul'by V. V. Chast' 1. M.: RGGU - Izdatel'skij dom MPA-Press. 342 p., p 310-314. (in Russian).
[7] Brjuhoveckij A.A., Sosonovskij Ju.V., Miljukov V.V. Fundamental research in the field of methods of construction of detection systems and network intrusion prevention. Vestnik SEVNTU. 2014. № 154.P. 60-63. (in Russian).
[8] Bachchelli F., Rybko N.A., Shlosman S.B. Queueing networks with mobile devices-the limit of the average field. Problems of information transmission. 2016, tom 52:2, p86–110. (in Russian).

[9] Puzyr'kov D.V., Podryga O.P., Poljakov S.V. Parallel processing and visualization to simulation results by the molecular dynamics method Proceedings of Institute for system programming Russian Academy of Sciences. Tom 28, №2, 2016 g. P. 221-242. (in Russian).

[10] Taheri S. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications. 22, June 2015, Pages 99-112 URL:https://doi.org/10.1016/j.jisa.2014.09.003 (data obrashhenija: 12.12.2017).

[11] Taheri S. Hartung S. Anonymous group-based routing in MANETs. Journal of Information Security and Applications. Volume 22, June 2015, Pages 87-98. https://doi.org/10.1016/j.jisa.2014.09.002 (data obrashhenija: 12.12.2017).

[12] V'jukova N.I., Galatenko V.A., Sumborskij S.V. Support for parallel and competitive programming in C++. The Journal "Programming". 2017. № 5 P. 48-59. (in Russian).

[13] Horoshilov A.V., Shhepetkov I.V. ADV_SPM — Formal models of security policy in practice the Proceedings of the Institute for system programming Russian Academy of Sciences. Tom 29, № 3, 2017 g. P. 43-56. (in Russian).

[14] Fua Y., Koné O. Model based security verification of protocol implementation. Journal of Information Security and Applications. 22, June 2015, Pages 17-27 URL: https://doi.org/10.1016/j.jisa.2014.08.002 (data obrashhenija: 12.12.2017).

Поступила в редакцию – 18 декабря 2017 г. Окончательный вариант –08 февраля 2018 г.
Received – December 18, 2017. The final version – February 08, 2018.