Оригинальная статья/Original article

УДК 004.056

DOI: http://doi.org/10.20914/2310-1202-2017-4-90-96

Экспериментальный метод определения вероятностно-временных характеристик систем защиты информации от несанкционированного доступа в автоматизированных информационных системах

Алексей В. Скрыпников [1] skrypnikovvsafe@mail.ru
Антон Д. Попов [2] anton.holmes@mail.ru
Евгений А. Рогозин [2] evgenirogozin@yandex.ru
Виктор А. Хвостов [1] hvahva1@mail.ru

[1] Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия
[2] Воронежский институт МВД России, пр. Патриотов, 53, г. Воронеж, 394065, Россия

Реферат. Статья посвящена методу экспериментальной оценке параметров функционирования типовых систем защиты информации от несанкционированного доступа, сертифицированных, широко используемых в организациях, эксплуатирующих автоматизированные информационные системы. В ходе эксперимента оценивались статистические данные в динамике функционирования систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. Регистрация параметров времени выполнения защитных функций защиты осуществлялась при помощи специальной утилиты "ProcessMonitor" из состава комплекта утилит компании "Sysinternals", используемой для фильтрации процессов и потоков. Загрузка процессора и оперативной памяти ЭВМ с использованием специального программного обеспечения, специально разработанного для выполнения экспериментальных исследований, имитирует работу СЗИ в условиях реальной работы по прямому назначению. Специальное программное обеспечение имитации работы системы с высокой загрузкой разработано в "VisualStudio 2015" в рамках "ConsoleApplication".При этом обеспечивается загрузка процессора на уровне порядка 50-70 % и оперативной памяти 60-80%. Полученные значения времени реализации защитных функций в условиях высокой загрузки ресурсов средства вычислительной техники по прямому назначению позволят оценить конфликтные и динамические свойства СЗИ. В дальнейшем полученные экспериментальные оценки могут быть использованы при разработке модели защиты информации в автоматизированных информационных системах, а также при формировании требований к качеству (ресурсоемкости, времени реакции на запрос пользователя, коэффициенту готовности и. т.п.). Также результаты вычислительного эксперимента в дальнейшем могут быть использованы для разработки программного комплекса оценки динамического показателя эффективности систем защиты информации от несанкционированного доступа в автоматизированных информационных системах.

Ключевые слова: защита информации, автоматизированная система, система защиты информации, несанкционированный доступ, информационная безопасность, органы внутренних дел

Computational experiment for the purpose of determining the probabilistic and temporal characteristics of information security systems against unauthorized access in automated information systems

Aleksei V. Skrypnikov [1] skrypnikovvsafe@mail.ru
Anton D. Popov [2] anton.holmes@mail.ru
Evgenii A. Rogozin [2] evgenirogozin@yandex.ru
Victor A. Khvostov [1] hvahva1@mail.ru

[1] Voronezh state university of engineering technologies, Revolution Av., 19 Voronezh, 394036, Russia
[2] Voronezh Institute of the Ministry of the Interior of Russia, Patriotov av., 53 Voronezh, 394065, Russia

Summary.The article is devoted to the method of experimental estimation of parameters of functioning of standard information protection systems from unauthorized access, certified, widely used in organizations operating automated information systems. In the course of the experiment, statistical data were evaluated in the dynamics of the functioning of information security systems against unauthorized access in automated information systems. Registration of the parameters for the execution time of protective protection functions was carried out using a special utility called ProcessMonitor from the Sysinternals suite of utilities used to filter processes and threads. The loading of the processor and main memory of the computer with the use of special software, specially designed for performing experimental research, simulates the operation of GIS in real-world work for its intended purpose. A special software for simulating the work of a system with high load is developed in "VisualStudio 2015" within the framework of "ConsoleApplication". At the same time, the processor is loaded at a level of 50-70% and 60-80% of the operative memory. The obtained values of the time of implementation of protective functions in conditions of high utilization of resources of computer facilities for their intended purpose will allow us to assess the conflict and dynamic properties of the GIS. In the future, the obtained experimental estimates can be used to develop a model of information security in automated information systems, as well as in the formation of quality requirements (resource intensity, response time to the user's request, availability, etc.). Also, the results of the computational experiment in the future can be used to develop a software package for assessing the dynamic performance of information security systems against unauthorized access in automated information systems

Keywords:information security; automated system; information security system; system effectiveness; unauthorized access; information security; internal affairs agencies

Для цитирования

Скрыпников А.В., Попов А.Д., Рогозин Е.А., Хвостов В.А. Экспериментальный метод определения вероятностно-временных характеристик систем защиты информации от несанкционированного доступа в автоматизированных информационных системах // Вестник ВГУИТ. 2017. Т. 79. № 4. С. 90–96. doi:10.20914/2310-1202-2017-4-90-96

For citation

Skrypnikov A.V., Popov A.D., Rogozin E.A., Khvostov V.A. Computational experiment for the purpose of determining the probabilistic and temporal characteristics of information security systems against unauthorized access in automated information systems. *Vestnik VGUIT* [Proceedings of VSUET]. 2017. vol. 79. no. 4. pp. 90–96. (in Russian). doi:10.20914/2310-1202-2017-4-90-96

Введение

В настоящее время требования к системам защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных информационных системах (АИС) осуществляются на основе нормативной документации Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [1], а также нормативных документов [2]. Общим недостатком существующих нормативных документов является то, что требования к СЗИ от НСД формируются в виде функционала, основанного на определенном классе защищенности АИС, не учитывающего свойств СЗИ от НСД связанных с повышенной ресурсоемкостью. При этом ресурсоемкость системы защиты влечет за собой увеличение времени отклика АИС на пользовательские запросы. В целом это приводит к затруднению функционирования АИС по своему прямому предназначению [2–4]. В связи с этим необходим учет реальных динамических свойств процессов защиты информации, позволяющий найти компромисс между эффективностью по прямому предназначению и ее защищенностью. С этой целью для разработки программного комплекса оценки динамического показателя эффективности СЗИ от НСД в АИС необходимо экспериментально оценить вероятностно-временные характеристики (ВВХ).

Теоретический анализ

В качестве объекта исследования, при проведении вычислительного эксперимента выберем широко используемую, сертифицированную по 3 классу защищенности средств вычислительной техники и по 2 уровню контроля отсутствия недокументированных возможностей типовую СЗИ от НСД «Страж NT» [3].

Сложность структуры АИС, разнообразность и специфичность протекающих в ней информационных процессов приводит к необходимости исследования организации защиты информации при проектировании СЗИ от НСД с целью определения ее характеристик при разных условиях функционирования. Как сказано выше, ранее проведенные исследования [5] позволили разработать основные этапы и задачи проектирования СЗИ от НСД в АИС ОВД. В рамках данного алгоритма этап «Программно-техническая разработка, адаптация и тестирование СЗИ от НСД в АИС ОВД» подразумевает проведение вычислительного эксперимента для определения ее ВВХ.

Первоочередным при разработке СЗИ от НСД должны быть заложены и обоснованы на этапе «Формирование требований к СЗИ от НСД в АИС» [5] требования в части определения ВВХ. Данные требования относятся к функциональным и позиционируются нормативными документами как одни из важнейший на стадии проектирования программных продуктов [8, 9]. Они в свою очередь описывают широкий спектр функциональных характеристик системы такие как: обработку данных, способы и методы проводимых вычислений и т. д. Одной из особенностей функциональных требований является, то что к поведению системы относится не только то, что система должна делать, но и то, что она не должна делать [9, 10]. Применительно к СЗИ от НСД это недопущение превышения интервала времени с момента обращения к защищаемой функции до окончания выполнения функции, относительно максимального времени выполнения функции, установленного в технической документации [7]. Данное требование исходит из доступности требуемых вычислительных ресурсов, таких как вычислительные возможности и объема памяти АИС.

Относительно АИС в защищенном исполнении функциональные требования определены в ГОСТР ИСО/МЭК 15408-2-2013 как функциональные требования безопасности. Данный стандарт также включает в себя каталог функций, отвечающих общим требованиям к функциональным возможностям безопасности [11]. Функциональные требования безопасности объединены в классы, семейства и компоненты. Вероятностно-временные характеристики СЗИ от НСД в АИС ОВД можно отнести к классу «FRU: Использование ресурсов». Данный класс содержит 3 семейства:

- FRU_FLT Отказоустойчивость;
- FRU_PRS Приоритет обслуживания;
- FRU_RSA Распределение ресурсов.

Определение ВВХ СЗИ от НСД в АИС ОВД в частном случае можно отнести к семейству «FRU_RSA Распределение ресурсов», но с дополнением. Предложение заключается в том, чтобы при проектировании АИС в защищенном исполнении найти компромисс между ее функционированием по прямому назначению (обработка, хранение и передача информации) и ресурсов, отвлекаемых самой СЗИ от НСД.

Для проверки реализации всех предъявляемых требований к проектируемой АИС проводятся различные методы тестирования [8]. Перспективным считается метод «потоков динамических тестов в реальном времени». При попытке реализации такого метода относительно типовой СЗИ от НСД в АИС доступ к ряду функций был ограничен, потому что они выполняются на уровне ядра. А разработка программного обеспечения на низком уровне для получения ВВХ СЗИ от НСД, представляется значительным привлечением людских ресурсов. Поэтому с учетом данных особенностей разработаем проведения вычислительного эксперимента.

Вычислительный эксперимент

Вычислительный эксперимент направлен на ресурсы АИС (оперативную память и процессорное время) в результате воздействия на которые деструктивного воздействия получим ВВХ компонентов СЗИ от НСД. Получение ВВХ необходимо для дальнейшей разработки программного комплекса оценки динамического показателя эффективности СЗИ от НСД в АИС. Так как эксперимент направлен на ресурсы АИС для СЗИ от НСД, необязательным является рассмотрение других сценариев реализации эксперимента, потому что мы рассмотрим вариант загрузки ресурсов с учетом того, что СЗИ от НСД в АИС ОВД останется возможность реализовывать свои функции по прямому предназначению, целью которого является получение ВВХ.

При НСД основным фактором реализации угроз является человеческий, а именно неграмотные действия пользователей (операторов). Довольно частыми являются случаи, когда носители информации используются не только при работе с СЗИ от НСД, но и на не аттестованных рабочих местах, что может привести к деструктивным воздействиям со стороны злоумышленника. Этому подтверждение исследования российских ученых и статистические данные ведущих антивирусных компаний. В работе [12] проведены исследования комплексной оценки угроз, в которой рассмотрены следующие факторы: ошибки пользователя, программные ошибки, отказ в обслуживания, перегрузка трафика, люки, логические бомбы, троянские кони, аппаратные сбои, аппаратные ошибки, ошибки передачи данных полученные результаты показали, что около 60–70% всех потерь информации исходят из некорректных действий пользователей (операторов). Согласно статистической информации только в результате ошибок пользователей и обслуживающего персонала происходит до 65% случаев нарушения информационной безопасности [13]. Это обосновывается тем предполагаемому нарушителю физический доступ к реальной АИС ограничен, а каналы связи имеют место быть, когда необходимо реализовать связь между операторами, но в основном такого рода АИС автономны. Из вышесказанного определимся, что сценарий вычислительного эксперимента будет основываться на пользовательских ошибках, и его реализация основана на одной из них.

На рисунке 1 представлена структурная схема (сценарий) вычислительного эксперимента для определения времени работы компонентов СЗИ от НСД в АИС.

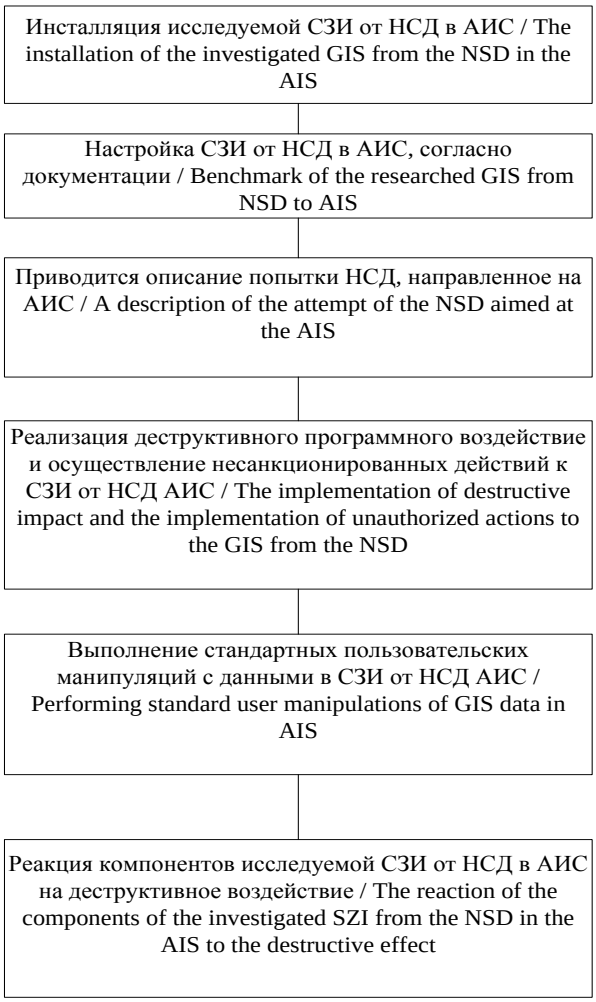


Рисунок 1. Алгоритм проведения вычислительного эксперимента над СЗИ от НСД в АИС

Figure 1. Algorithm for carrying out a computational experiment on the system for protecting information from unauthorized access in automated information systems

1. Инсталляция СЗИ от НСД «Страж NT» основывалась на рекомендациях разработчика. При этом была развернута полная версия СЗИ от НСД на автоматизированном рабочем месте с следующими характеристиками: процессор Pentium(R) Dual-Core с таковой частотой 2.6 GHz, оперативная память 2 ГБ, 32 разрядная операционная система. Совместно с СЗИ от НСД было установлено прикладное программное обеспечение в виде пакета «Office» и антивируса «Kaspersky».

2. В рамках вычислительного эксперимента произведена настройка СЗИ от НСД согласно документации [3]. Если рассматривать СЗИ от НСД различных типов, то их этапы настройки принципиально не отличается.

3. Принцип деструктивного воздействия заключается в следующем. Пользователь, пренебрегает своими должностными обязанностями и использует зарегистрированный в СЗИ от НСД флэш-накопитель не по назначению, а именно с другими устройствами. Подобная ситуация даёт

возможность злоумышленникам, используя вредоносное программное обеспечение, осуществить несанкционированное проникновение сначала на флэш-накопитель в виде скрытых файлов «autorun.inf» и «nagruz.exe», а в последующем и в АИС.

Пользователь начинает работать с файлами на флэш-накопителе, подключая его к защищенной АИС тем самым активируя вредоносную программу. Разработанный нарушителем код копируется на жесткий диск компьютера и запускается, попадая в автозагрузку, а при последующей перезагрузки начинает свое воздействие на ресурсы АИС. Снижение объема ресурсов АИС позволит определить ВВХ СЗИ от НСД при деструктивном воздействии, визуально определить, как работает АИС и СЗИ от НСД по прямому предназначению при подобных экстренных ситуациях.

4. На данном этапе реализуем практическую составляющую деструктивного воздействия на АИС, посредством специально разработанного вредоносного программного обеспечения рисунках 2 и3, которое разработано в «Visual Studio 2015» в рамках «Console Application».

Разработанное вредоносное программное обеспечение работает на АИС с различной мощностью процессора и объемом оперативной памяти, подсчитывает свободное количество ресурсов и исходя из этого определяет степень воздействия. Также реализована многопоточность, для каждого ядра создается отдельный поток, бесконечно перемножающий матрицы, использование оперативной памяти достигается при помощи загрузки в нее пустых байтов с определенным промежутком времени. Работа вредоносного программного обеспечения представлена на рисунке 3. Скрытное воздействие на ресурсы позволило заметно снизить быстродействие АИС ОВД, но в тоже время оставляя ей возможность выполнять свои функции по прямому предназначению. Вредоносное программное обеспечение распоряжается ресурсами системы в виде 50% от оперативной памяти и процессорного времени, общая нагрузка на систему будет составлять 70–90% в сумме с процессами, которые работают по умолчанию и вызываются пользователем. Программа была протестирована на нескольких системах и показала положительные результаты.

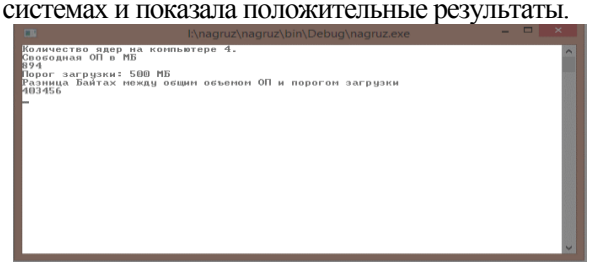


Рисунок 2. Подсчет ресурсов АИС

Figure 2. Counting Resourcesautomated information system

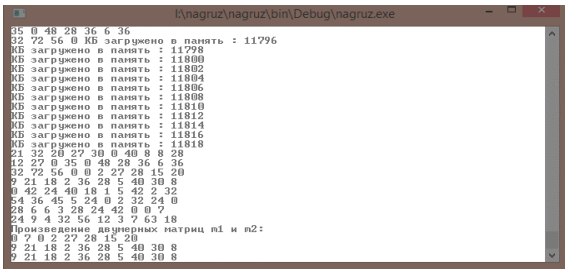


Рисунок 3. Деструктивное воздействие на АИС

Figure 3. Destructive impact on automated information system

5. Деструктивное воздействие реализовано после этого имитируем работу пользователя, осуществив стандартные манипуляции с файлами и папками СЗИ от НСД в АИС. Эти действия необходимы для того, чтобы задействовать все механизмы защиты и впоследствии зафиксировать их выполнения. Можно заметить, что при деструктивном воздействии существенно увеличилось время отклика прикладного программного обеспечения.

6. С целью определения статистических данных будем основываться на ранее разработанной графой модели [5]. Временные характеристики подсистемы «Вход в систему» зафиксированы при помощи программного продукта «Process Monitor», который предназначен для мониторинга всех процессов в оперативной памяти в реальном времени, а также для мониторинга файловой системы и системного реестра. Сбор информации при помощи «ProcessMonitor» осуществлялся при помощи фильтрации процессов и потоков. Он разработан компанией «Sysinternals» для наблюдения в масштабе реального времени за действиями различных процессов в операционных системах семейства «Windows». «Process Monitor» включает в себя несколько подпрограмм: мониторинга обращений к реестру «Regmon» и мониторинга обращений к файловой системе «Filemon», а также дополнительно, позволяет получать более подробную информацию о взаимодействии процессов, операциях ввода-вывода, сетевой активности и использовании ресурсов. Данный программный продукт не требует установки, однако работа ее возможна только с правами администратора.

Для своей работы, «ProcessMonitor» устанавливает в системе собственный драйвер «Procmon20.sys», при помощи которого осуществляется перехват контролируемых монитором системных функций и сбор данных подлежащих мониторингу. Наблюдение выполняется для следующих классов операций:

- обращения к файловой системе (filesystem);
- обращение к реестру (Registry);
- работа с сетью (Network);
- активность процессов (Process).

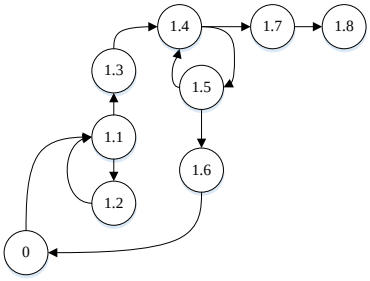
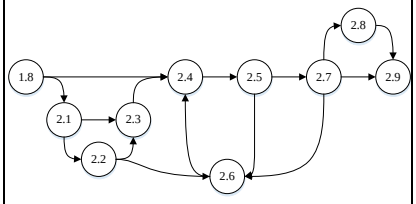
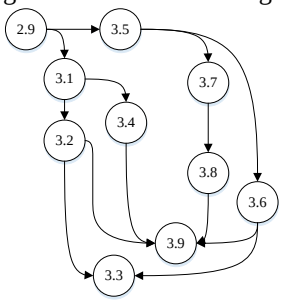
Результаты экспериментальной оценки динамических функций СЗИ «Страж NT» представлены в таблице 1.

Таблица 1.

Реакция СЗИ от НСД на деструктивное воздействие

Table 1.

The reaction of the information protection system against unauthorized access to destructive impact

Наименование подсистемы и граф состояний СЗИ от НСД	Функции, выполняемые СЗИ от НСД	Время с.
1. Вход в систему / Login to the system 	0 Включение автоматизированного рабочего места (АРМ) (Прекращение выполнения функций АРМ)/ Enabling the automated workstation (AWP) (Terminating the functions of the workstation) 1.1 Предъявление идентификатора/ Presentation of the identifier 1.2 Прекращение работы идентификатора, но в случае новой попытки его нужно заново ввести / Termination of the identifier, but in the case of a new attempt it must be re-entered 1.3 Допуск к вводу пароля / Authorization to enter a password 1.4 Ввод пароля / Enter password 1.5 Повторный ввод пароля / Retype password 1.6 Блокировка входа в систему при трехразовом неправильном вводе пароля / Blocking the logon with a three-time wrong password entry 1.7 Аутентификация субъекта системы / Authentication of the subject of the system 1.8 Вход систему / Login to the system	10 с. 1 с. 6 с. 1 с. 5 с. 5 с. 1 с. 1 с. 5 с.
2. Разграничение доступа и взаимодействие с внешними носителями / Access delimitation and interaction with external media 	2.1 Сопоставлениеидентификационнойинформациивнешнегоносителяипользователя / Comparison of the identification information of the external medium and the user 2.2 Контроль устройств (если устройство не принадлежит пользователю, срабатывает данный механизм) / Control of devices (if the device does not belong to the user, this mechanism works) 2.3 Доступ к внешнему носителю / Access to external media 2.4 Обращение объекту / Accessing an object 2.5 Сопоставление меток конфиденциальности пользователя и ресурса (в СЗИ реализуется на основе мандатного принципа контроля доступа) / Comparison of the labels of the user's privacy and the resource (in the GIS is implemented on the basis of the mandatory principle of access control) 2.6 Блокировка доступа к объекту / Blocking access to an object 2.7 Проверка полномочий доступа пользователя (в СЗИ реализуется на основе дискреционного принципа контроля доступа) / Verification of user access authority (in the GIS is implemented on the basis of the discretionary principle of access control) 2.8 Преобразование информации на носителе при помощи шифрования (в СЗИ применяется метод гаммирования) / Transformation of information on the medium by means of encryption (GIS method is applied in GIS) 2.9 Допуск субъекта к защищаемому объекту / Admission of the subject to the protected object	0.2 с 0.01 с 0.01 с 0.1 с. 0.09 с. 0.03 с. 0.08 с. 0.7 с. 2 с.
3. Механизмы контроля целостности регистрации и учета / Mechanisms to control the integrity of registration and accounting 	3.1 Запроснапреобразованиеобъекта/ Request to convert an object 3.2 Блокировкапреобразованияобъекта/ Block an object conversion 3.3 РегистрациянарушенийработысСЗИ / Registration of violations of work with GIS 3.4 Пересчетпараметровцелостностифайла / Conversion of file integrity parameters 3.5 Запроснаудаление / Requestfordeletion 3.6 Блокировкаудаления / DeletionBlocking 3.7 Преобразованиеобъектапередудалением / Convertinganobjectbeforedeleting 3.8 Удаление объекта / Delete an object 3.9 Завершение работы с объектом / Finishing work with the object	0.009 с. 0.003 с. 0.02 с. 0.6 с. 0.009 с. 0.004 с. 2 с. 0.05 с. 0.002 с.

Заключение

В статье представлены результаты вычислительного эксперимента по исследованию ВВХ (времени реакции) на деструктивное воздействие, которые совместно с алгоритмом оценки динамического показателя эффективности СЗИ от НСД являются основой для разработки программного комплекса анализа, моделирования и оценки динамического показателя эффективности СЗИ от НСД в АИС с целью исследования вероятностно-временных характеристик процессов защиты.

ЛИТЕРАТУРА

1 ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 (дата обращения: 03.12.2017).

2 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". URL: http:// http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 29.11.2017).

3 СЗИ «Страж NT». Руководство администратора. URL: http://www.guardnt.ru/download/ doc/admin_guide_nt_3_0.pdf (дата обращения: 03.11.2017).

4 Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/ opis30.pdf (дата обращения: 04.11.2017).

5 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.

6 Рогозин Е. А., Попов А. Д. Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД // Вестник Воронежского института МВД России. 2016. № 4. С. 122—131.

7 Макаров О.Ю., Хвостов В.А., Хвостова Н.В. Методика нормирования требований к информационной безопасности автоматизированных систем // Вестник Воронежского государственного технического университета. 2010. Т. 6. № 11. С. 47 – 511

8 Липаев В.В. Тестирование компонентов и комплексов программ. М.: СИНТЕГ, 2010. 400 с.

9 Куликов С.С. Тестирование программного обеспечения. Базовый курс. «Четыре четверти», Минск, 2015. 296 с. URL: http://svyatoslav.biz/ software_testing_book/ (дата обращения: 11.11.2017).

10 Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.

11 ГОСТР ИСО/МЭК 15408-2—2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

12 Рогозин Е.А. и др. Методологические основы безопасности использования информационных технологий в системах электронного документооборота: монография. Воронеж: Научная книга, 2011. 252 с.

13 Saltzer J.H., Schroeder M.D. The protection of information in computer systems // Proceedings of the IEEE. 1975. V. 63. № 9.

14 Zequ Yang; Peng Cheng; Jiming Chen Differential-privacy preserving optimal power flow in smart grid // IET Generation, Transmission & Distribution. 2017. V. 11. № 15. P. 3853 – 3861.

15 Jun Yang, Chunjie Zhou, Shuanghua Yang, Haizhou Xu et al. Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems // IEEE Transactions on Industrial Electronics Year. 2017. V. PP. № 99. P. 1 – 1.

16 Hwaiyu Geng A Single platform approach for the management of emergency in complex environments such as large events, digital cities, and networked regions // Internet of Things and Data Analytics. 2017.

17 Sghaier Guizani Internet-of-things (IoT) feasibility applications in information Centric Networking System // 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017. P. 2192 – 2197.

18 Семененко В.А. Информационная безопасность. М.: МГУИТ, 2010. 277 с.

REFERENCES

1 FSTEK RF. Rukovodyaschiy dokument. Kontseptsiya zaschityi sredstv vyichislitelnoy tehniki i avtomatizirovannyih system ot nesanktsionirovan-no godostupa k informatsii [Guidance document. The concept of protecting computer facilities and automated systems from unauthorized access to information] Available at: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 (in Russian).

2 PostanovleniePravitelstva RF ot 01.11.2012 N 1119 "Ob utverzhdeniitrebovaniy k zaschitepersonalnyihdannyihpriihobrabotke v informatsionnyihsistemahpersonalnyihdan-nyih". [Decree of the Government of the Russian Federation of 01.11.2012 N 1119 "On the approval of the requirements for the protection of personal data when processing them in information systems of personal data] Available at: http:// http://www.consultant.ru/document/cons_doc_LAW_137356/ (in Russian).

3 SZI «Strazh NT». Rukovodstvoadmini-stratora: [Administrator's Guide] Available at: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (in Russian).

4 Sistema zaschityiinformatsiiotnesanktsi-onirovannogodostupa «Strazh NT». Opisaniepri-meneniya: [The system of protection of information from unauthorized access] Available at: http://www.rubinteh.ru/public/opis30.pdf (in Russian).

5 Rogozin E. A., Popov A. D., Shagirov T. V. Designing systems to protect information from unauthorized access in automated systems of internal affairs bodies. *VestnikVoronezhskogoinstituta MVD Rossii* [Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia] 2016. no. 2. pp. 174—183. (in Russian)

6 Rogozin E. A., Popov A. D. The model of the functioning of a standard system for protecting information from unauthorized access in automated information systems ATS. *Vestnik Voronezhskogo instituta MVD Rossii* [Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia] 2016. no. 4. no. 122—131. (in Russian)

7 Makarov O.Yu., Hvostov V.A., Hvostova N.V. Methodology of rationing requirements for information security of automated systems. *VestnikVoronezhskogo gosu-darstvennogo tehnicheskogo universiteta* [Proceedings of Voronezh State Technical University] 2010. vol.6. no.11 pp. 47 – 511 (in Russian)

8 Lipaev V.V. Testirovaniekomponentovikompleksovprogramm [Testing components and software packages] Moscow, SINTEG, 2010. 400 p. (in Russian)

9 Kulikov S.S. Testirovanie programmnogo obespecheniya. Bazovyiykurs. «Chetyire chetverti» [Software testing. Basic course. Four quarters,] 2015. 296 p. Available at: http://svyatoslav.biz/software_testing_book/ (in Russian)

10 Markov A.S., Tsirlov V.L., Barabanov A.V. Metodyiotsenkinesootvetstviyasredstvzaschityiinformatsii [Methods for assessing the discrepancy between information protection means] Moscow, Radio I svyaz, 2012. 192 p. (in Russian)

11 GOSTR ISO/MEK 15408-2—201 3Informatsionnaya tehnologiya. Metodyiisred-stva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnyi htehnologiy. Chast 2. Funktsi onalnyie komponentyi bezopasnosti [Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 2. Functional safety components]. (in Russian)

12 Rogozin E.A. et al. Metodologicheskie osnovy bezopasnosti ispolzovaniya informatsionnyih tehnologiy v si-stemahelektronnogo dokumento oborota: monogra-fiya [Methodological fundamentals of the safety of using information technologies in electronic document management systems: monograph] Voronezh, Voronezh: IPTs «Nauchnaya kniga», 2011. 252 p. (in Russian)

13 Saltzer J.H., Schroeder M.D. The protection of information in computer systems Proceedings of the IEEE. 1975. vol. 63. no. 9.

14 Zequ Yang; Peng Cheng; Jiming Chen Differential-privacy preserving optimal power flow in smart grid. IET Generation, Transmission & Distribution. 2017. vol. 11. no. 15. pp. 3853 – 3861.

15 Jun Yang, Chunjie Zhou, Shuanghua Yang, Haizhou Xu et al. Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Electronics Year. 2017. vol. PP. no. 99. pp. 1 – 1.

16 Hwaiyu Geng A Single platform approach for the management of emergency in complex environments such as large events, digital cities, and networked regions. Internet of Things and Data Analytics. 2017.

17 Sghaier Guizani Internet-of-things (IoT) feasibility applications in information Centric Networking System. 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017. pp. 2192 – 2197.

18 Semenenko V.A. Informatsionnaya bezopasnost [Information Security] Moscow, MGUIT, 2010. 277 p. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

Алексей В. Скрыпников д.т.н., профессор, кафедра информационной безопаснсоти, Воронежский государственный институт инженерных технологий, проспект Революции 19, г. Воронеж, 394000, Россия, skrypnikovvsafe@mail.ru

Антон Д. Попов адъюнкт, кафедра автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России, пр. Патриотов, 53, г. Воронеж, 394065, Россия, anton.holmes@mail.ru

Евгений А. Рогозин д.т.н., профессор, кафедра автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России, пр. Патриотов, 53, г. Воронеж, 394065, Россия, evgenirogozin@yandex.ru

Виктор А. Хвостов к.т.н., доцент, кафедра информационной безопасности, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394000, Россия, hvahva1@mail.ru

КРИТЕРИЙ АВТОРСТВА

Все авторы в равной степени принимали участие в написании рукописи и несут ответственность за плагиат

КОНФЛИКТ ИНТЕРЕСОВ

Авторы заявляют об отсутствии конфликта интересов.

ПОСТУПИЛА 04.10.2017
ПРИНЯТА В ПЕЧАТЬ 08.12.2017

INFORMATION ABOUT AUTHORS

Aleksei V. Skrypnikov Dr. Sci. (Engin.), professor , Information security affairs department, Voronezh state university of engineering technogies, Revolution Av. 19, Voronezh, 394000, Russia, skrypnikovvsafe@mail.ru

Anton D. Popov post-graduate cadet, automated information systems in interior affairs de-partment, Voronezh Institute of the Ministry of Interior, Patriotov av., 53, Voronezh, 394086, Russia, anton.holmes@mail.ru

Evgenii A. Rogozin Dr. Sci. (Engin.), professor, automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior, Patriotov av., 53, Voronezh, 394086, Russia, evgenirogozin@yandex.ru

Victor A. Khvostov Cand. Sci. (Engin.), associate professor, Information security affairs department, Voronezh state university of engineering technolo-gies, Revolution av., 19 Voronezh, 394000, Russia, hvahva1@mail.ru

CONTRIBUTION

All authors equally participated in writing the manuscript and responsible for the plagiarism

CONFLICT OF INTEREST

The authors declare no conflict of interest.

RECEIVED 10.4.2017
ACCEPTED 12.8.2017