7. IEEE 802.1Q-2018 – IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks. URL: https://standards.ieee.org/standard/802_1Q-2018.html (accessed: 15.02.2021).
8. IEEE 802.1D – MAC bridge. URL: shttps://www.ieee802.org/1/pages/802.1D.html (accessed: 15.02.2021).
9. Time-Sensitive Networking. URL: https://en.wikipedia.org/wiki/Time-Sensitive_Networking (accessed: 15.02.2021).
10. Ivanov I.V. OPC UA – new round of revolution. *Avtomatizatsija v promyshlennosti*, 2017, no. 2, pp. 7–9. (In Russ.)
11. Bina Sh., Brukner D., Vasina A.S. OPC UA TSN as a technology for communication at all levels of automation. *Avtomatizatsija v promyshlennosti*, 2019, no. 2, pp. 26–34. (In Russ.)
12. Tejlor A., Zapke M. TSN: converged networks for better performance IIoT. *Besprovodnye tehnologii*, 2018, no. 1, pp. 46–49. (In Russ.)
13. Testbed TSN (Time-Sensitive Networking). URL: https://lni40.de/lni40-content/uploads/2019/08/LNI_Use-Case_TESTBED-TSN-TIME-SENSITIVE-NETWORKING.pdf (accessed: 15.02.2021).
14. Quan W. et al. OpenTSN: an open-source project for time-sensitive networking system development. *CCF Transactions on Networking*, 2020, vol. 3, pp. 51–65.
15. Bruckner D. et al. OPC UA TSN. A new Solution for Industrial Communication. URL: https://www.moxa.com/Moxa/files/66/6669d232-4227-440a-9ddf-477e70b11780.pdf (accessed: 15.02.2021).

Received 15.02.2021

УДК 004

ЭЛЕКТРОННЫЕ КЛЮЧИ КАК МЕТОД ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ

Василенко К.А.[1], Золкин А.Л.[2], Ляпунов В.Н.[1], Семейкин В.А.[3]
[1] Владивостокский государственный институт экономики и сервиса, Владивосток, РФ
[2] Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
[3] Морской государственный университет адм. Г.И. Невельского, Владивосток, РФ
E-mail: k2857@mail.ru, alzolkin@list.ru, liapunov_vitalii_nikolaevich@vvsu.ru, vlad_6653496@mail.ru

В статье описываются принципы работы, виды технической реализации и способы применения электронных ключей. Также были рассмотрены основные российские производители электронных ключей, и выявлены особенности их продуктов. При обеспечении должным образом информационной безопасности компании необходимо учитывать правильную настройку и поддержку аппаратных и программных средств защиты информации во избежание убытков, с целью ликвидации рисков получения электронного ключа злоумышленником. Учитывая, что электронные ключи чаще всего относят к аппаратным способам защиты программ от взлома, при этом имеются улучшенные кроссплатформенные аппаратно-программные решения. Их существование обусловлено тем, что разработчики, проектирующие электронные ключи, также предоставляют и комплект разработчика программного обеспечения (SDK) к ним. Компании в своих собственных программных продуктах имеют возможность реализации с помощью SDK всех средств защиты электронных ключей, таких как средства разработки, защита фрагментов кода программы, разработка инструментов автоматической защиты и многое другое.

Ключевые слова: *электронные ключи, смарт-карты, методы защиты информации, программное обеспечение, несанкционированный доступ, злоумышленник, сервер, зашифрованный код, ключи активации, идентификация*

Введение

Защита программного обеспечения и электронных документов с использованием электронных ключей существует уже много лет, и она до сих пор показывает свою эффективность. Электронный ключ (аппаратный ключ, донгл) – это аппаратное средство, в основе которой лежит специальная микросхема, защищающая программное обеспечение и документы от незаконного копирования, использования и распространения третьими лицами.

История аппаратных ключей берет начало в начале 1980-х годов. К их появлению привела одна причина [1; 2]. Наличие защиты программ-

ного обеспечения от нелицензионного пользования в готовом продукте снижает риски и значительно увеличивает доход разработчиков. Раньше программисты добивались защищенности программного обеспечения (ПО) путем добавления в программы серийных номеров и ключей активации. В итоге злоумышленники нашли способ обходить эти средства защиты с помощью реверс-инжиниринга, патчей, эмуляторов ключа и кейгенов, что и привело к созданию электронных ключей.

Особенности конструкции электронных ключей с позиции обеспечения информационной безопасности

Ключи могут отличаться по технической реализации: интерфейс подключения устройства, форм-фактор, наличие криптопроцессора, объем памяти и т. д. Как правило, чаще всего ключи делают в формате флеш-устройств, которые подключаются через USB-порт. Хотя существуют и другие реализации, основанные на PCMCIA и LPT-интерфейсах.

Существуют также и беспроводные аппаратные ключи. Например, Everykey – это Bluetooth-устройство, которое позволяет хранить ключи и пароли, используя множество технологий защиты ПО [2; 3]. Everykey использует четыре уровня шифрования: AES 128-bit, AES 256-bit и RSA 4096-bit – и обладает возможностью удаленно заморозить устройство, что не даст другим использовать Everykey в случае его утери или кражи. Каждый раз, когда Everykey передает зашифрованное сообщение, его содержимое зашифровывается и изменяется, не давая злоумышленнику подделать Everykey-ключ. Пароли устройств также никогда не хранятся на серверах Everykey. Все эти особенности вместе делают Everykey безопасным и защищенным.

Аппаратные ключи также способны работать в пределах локальной сети, а не только одной рабочей станции. Защищенное программное обеспечение может самостоятельно определить и обратиться к ключу по внутренней сети. Таким образом, не обязательно покупать электронные ключи для каждого пользователя, чтобы, например, лицензировать защищенные приложения или открыть доступ к документам рабочей группы.

Электронные ключи имеют множество применений. Они используются для подтверждения отсутствия изменений в файлах. Ключи можно применять для хранения электронных денег на смарт-карте или собственной электронной подписи. Без них не обойтись, когда требуется зафиксировать состояние файла с момента его подписания. С помощью USB-донглов можно реализовать лицензирование программного обеспечения, идентификацию владельца [4–6].

Принцип работы электронных ключей основывается на электронной цифровой подписи, которая находится внутри ключа в защищенном виде. Если пользователь потеряет свой ключ, то он сможет это оперативно заметить и отозвать подпись.

Для обеспечения еще большей надежности существуют смарт-карты. Смарт-карты представляют собой пластиковые карты со встроенной микросхемой. Они обладают множеством плюсов, таких как: отказоустойчивость, невозможность подделки, аутентификация пользователя на рабочей станции, что исключает возможность утечки данных. Единственным недостатком можно считать только наличие карт-ридера для использования смарт-карт.

Иногда разработчики реализуют в смарт-картах двухфакторную аутентификацию. Для того чтобы использовать такой ключ, необходимо также знать и PIN-код, что повышает надежность хранения информации в разы.

Как правило, аппаратные ключи используются следующим образом. Сначала через специальный интерфейс ключ подключается к компьютеру. В это время программа загружается в оперативную память и через драйвер посылает ключу запрос, который он должен обработать. Аппаратный ключ формирует код с помощью встроенного микропроцессора и отправляет его обратно в компьютер. Если ответ электронного ключа не совпал со значением в программе, то она выполнит действия по защите от несанкционированного доступа, которые предварительно задал программист. Как правило, это переход в режим демонстрации, который блокирует доступ к данным или определенным функциям программы. Если же ответ оказался правильным, то программа продолжает свою работу.

Запросы также бывают нескольких типов в зависимости от задачи. Они могут включать в себя просто проверку наличия ключа в интерфейсе компьютера или считывание с электронного ключа нужной программе информации в качестве параметра запуска. В электронный ключ можно встроить внутренний таймер и с его помощью выполнять запросы приложения.

Программа может выполнить запрос на расшифровку предварительно зашифрованного кода или информации, которые нужны для работы

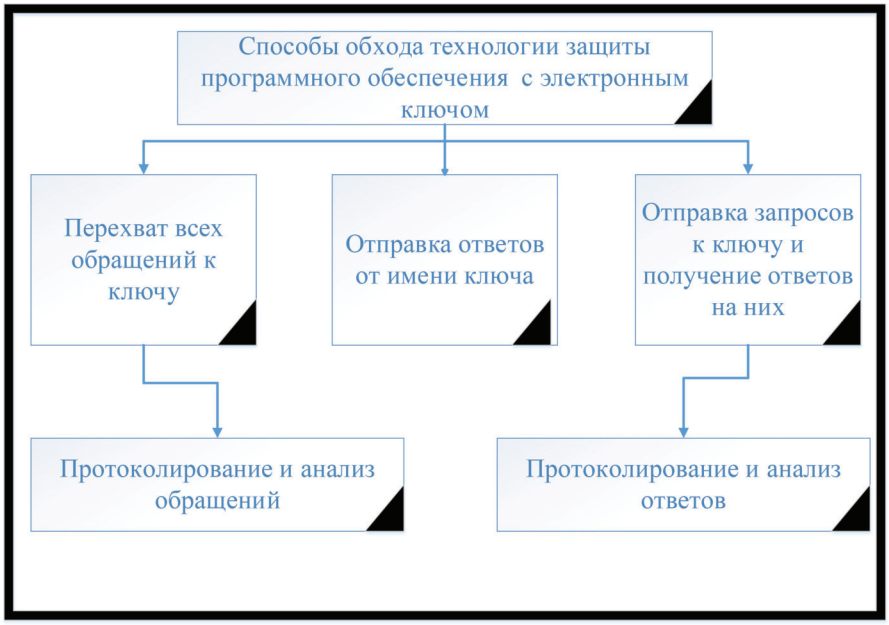

Рисунок 1. Способы обхода технологии защиты программного обеспечения с электронным ключом

программного обеспечения. Если аппаратный ключ не сможет этого сделать, то программа запустит зашифрованный код, который приведет к ошибке [7].

Также можно защитить программу путем высчитывания контрольной суммы. Приложение проверяет целостность кода сравнением контрольной суммы, посчитанной на микропроцессоре ключа, с контрольной суммой самой программы. Это можно сделать, например, на основе выполнения электронной цифровой подписи кода и проверки этой подписи уже внутри программы (см. рисунок 1).

В свою очередь хакеры придумали множество способов обхода защиты, но главная их задача была в том, чтобы заставить программу работать без настоящего электронного ключа. Чтобы программа правильно работала и считала, что работает с ключом, необходимо либо эмулировать наличие ключа, либо взломать и переписать код самой программы.

Несмотря на то что электронные ключи считаются аппаратным способом защиты программ от взлома, тем не менее существуют и кроссплатформенные аппаратно-программные решения. Они существуют, потому что разработчики, проектирующие электронные ключи, также предоставляют и комплект разработчика программного обеспечения (SDK) к ним. С помощью SDK все средства защиты электронных ключей возможно реализовывать и в собственных программных продуктах компаний [8]. Например, средства разработки, защита фрагментов кода программы, разработка инструментов автоматической защиты и многое другое.

Анализ отечественных разработок электронных ключей и технологий защиты ПО от нелегального копирования

Созданием электронных ключей в России занимается множество компаний. Наиболее значимые из них – это «Аладдин Р.Д.» и «Актив».

Компания «Актив» – это один из самых крупных разработчиков электронных ключей и других средств информационной безопасности. Основными проектами компании «Актив» являются Guardant, Рутокен. Guardant – это пакет программно-аппаратных разработок для лицензирования и защиты ПО от нелегального копирования. Он дает возможность получить разработчикам достойные продажи с их программного продукта. В Guardant входят следующие решения: аппаратные ключи, инструменты для защиты исходного кода и средства лицензирования программ.

Уникальной чертой Guardant является возможность программисту создавать и хранить во внутренней памяти ключа собственные алгоритмы шифрования и отдельные части исходного кода программы, под который создается электронный ключ. В Guardant также встроен собственный криптопроцессор, позволяющий безопасно исполнять код в самом ключе, не используя для этого процессор компьютера [9; 10].

Этот подход к проектированию защиты сильно осложняет работу взломщикам и помогает защитить исходный код программы от реверс-инжиниринга другими компаниями-конкурентами. Тем не менее разработчики также должны иметь

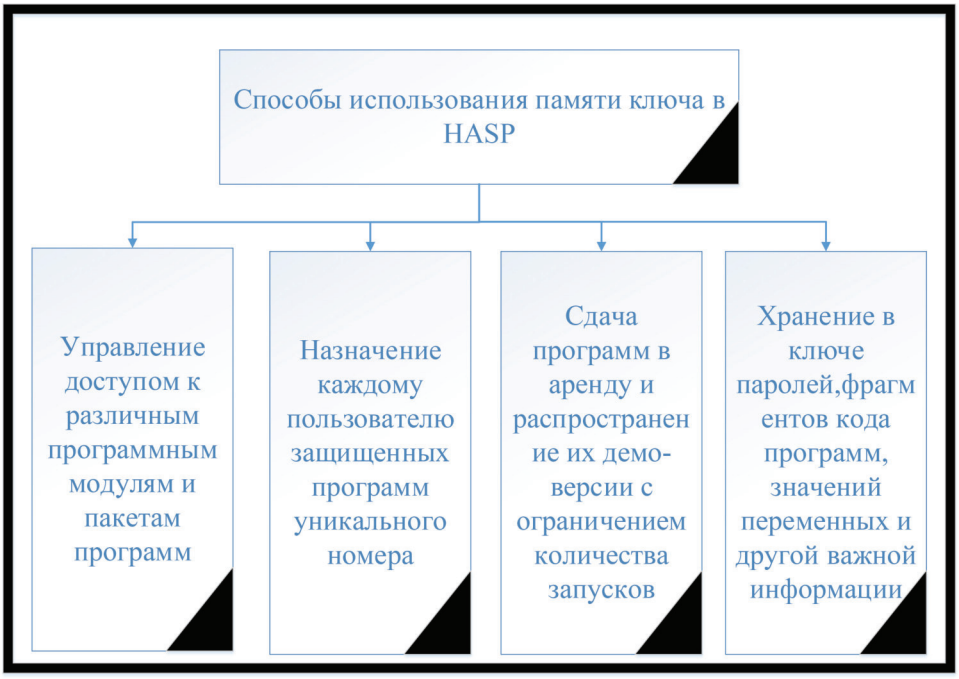

Рисунок 2. Способы использования памяти ключа в HASP

в виду, что опытный злоумышленник может легко провести криптоанализ и взломать защиту, если программисты реализовали излишне простой алгоритм шифрования.

Рутокен – это серия аппаратных ключей, которые можно использовать для создания электронной подписи и аутентификации. Эти ключи представляют собой личные устройства доступа к информационным ресурсам. Форм-факты электронных ключей могут быть различны: от обычных USB-донглов до беспроводных Bluetooth-устройств и смарт-карт.

«Аладдин Р.Д.» – это отечественная компания, разрабатывающая различные системы защиты данных от злоумышленников и аутентификации пользователей. Наиболее известными продуктами этой компании являются HASP и eToken.

HASP представляет собой комплекс программ и устройств, необходимых для защиты файлов и ПО от несанкционированного использования [11; 12]. Аббревиатура HASP расшифровывается как Hardware Against Software Piracy (аппаратные средства против программного пиратства) и включает в себя сам электронный ключ HASP, программу для «привязки» к этому ключу и методы защиты и контроля целостности программного кода программ (см. рисунок 2).

В основу успеха этой технологии легла микросхема ASIC, которая имеет индивидуальный алгоритм работы для каждого аппаратного ключа, что обеспечивает повышенную безопасность и надежность.

Микросхема имеет собственную внутреннюю память, через которую разработчик может устанавливать каждому пользователю свой идентификатор, управлять доступом к различному программному обеспечению и хранить пароли или другие важные данные.

eToken – это линейка персональных устройств проверки подлинности, представленных в форм-факторе USB-ключей. «Аладдин Р.Д.» разработали технологию, благодаря которой стало возможно применять USB-донглы как полноценный аналог смарт-карт и не тратить деньги на дорогие устройства считывания [13–15]. Для применения этой технологии необходимо только специальное ПО eToken PKI Client, которое обеспечивает работу с eToken и USB-порт.

Заключение

Таким образом, особенностью персональных устройств проверки подлинности eToken является их надежность и функциональность. Они имеют энергонезависимую память и микропроцессор, что позволяет хранить в них множество данных и выполнять вычисления прямо в ключе. Они отличаются малым размером, позволяющим постоянно носить их с собой. eToken выполнен в крепком корпусе, который защищает его от механических повреждений и воды.

Аппаратно-программные средства защиты информации необходимо не просто приобретать, но и правильно настраивать и поддерживать. В противном случае если электронный ключ, который хранит в себе все пароли пользователя, получит злоумышленник, то ему достаточно будет подобрать всего один пароль, чтобы получить полный

доступ к этому ключу. Это приведет к огромным убыткам компании, и это надо иметь в виду при проектировании систем защиты с использованием электронных ключей.

Литература

1. HASP // Википедия – свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/HASP (дата обращения: 19.05.2020).
2. Конявская С. Защита информации с USB-интерфейсом // Журнал сетевых решений LAN. 2007. № 11. URL: http://www.osp.ru/lan/2007/11/4592946 (дата обращения: 10.06.2020).
3. Оценка эффективности систем защиты программного обеспечения // CIT Forum. URL: http://citforum.ru/security/software/sereda1 (дата обращения: 29.09.2020)
4. Скляров Д.В. Аппаратные ключи защиты // Искусство защиты и взлома информации. СПб.: БХВ-Петербург. 2020. 288 с.
5. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника. 2019. 384 с.
6. Платонов В.В. Программно-аппаратные средства защиты информации. М.: Академия, 2013. 336 с.
7. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. 173 с.
8. Основы криптографии / А.П. Алферов [и др.]. М.: Гелиос АРВ, 2002. 480 с.
9. Касперский К. Техника внедрения кода в PE-файлы и методы его удаления // Хакер. 2004. № 7. 81 с.
10. Фергюсон Н., Шнайер Б. Практическая криптография. М.: Диалектика, 2018. 432 с.
11. Digitalization peculiarities of organizations – A case study / V.L. Vasilev [et al.] // Entrep. Sustain. 2020. № 7. P. 3173–3190.
12. Дудукалов Е.В. Государственное регулирование развития национального сегмента интернета в России // Государственное и муниципальное управление. Ученые записки СКАГС. 2008. № 3. С. 155–164.
13. Дудукалов Е.В. Технологические парки в системе национальных приоритетов постиндустриального развития экономики // Экономические и гуманитарные науки. 2014. № 5 (268). С. 112–118.
14. Assessment of Modern Global Trends in Digital Trade and Finance / T. Ignatova [et al.] // Advances in Economics, Business and Management Research. 2020. Vol. 139. P. 363–366.
15. Игнатова Т.В., Дудукалов Е.В., Черкасова Т.П. Знаниевые экосистемы и рейтинги цифровизации национальных экономик // Цифровая экосистема экономики: Материалы VII Международной научно-практической видеоконференции. Ростов-на-Дону: ЮФУ, 2020. С. 391–397.

Получено 20.12.2020

Василенко Константин Александрович, преподаватель высшей категории Колледжа сервиса и дизайна Владивостокского государственного университета экономики и сервиса (ВГУЭС). 690092, Российская Федерация, г. Владивосток, ул. Добровольского, 20. Тел. +7 964 453-06-36. E-mail: k2857@mail.ru

Золкин Александр Леонидович, к.т.н., доцент кафедры информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики. 443010, Российская Федерация, г. Самара, ул. Льва Толстого, 23. Тел. +7 960 825-68-49. E-mail: alzolkin@list.ru

Ляпунов Виталий Николаевич, преподаватель Колледжа сервиса и дизайна ВГУЭС. 690092, Российская Федерация, г. Владивосток, ул. Добровольского, 20. Тел. +7 924 327-19-37. E-mail: liapunov_vitalii_nikolaevich@vvsu.ru

Семейкин Владислав Андреевич, студент Морского государственного университета им. адм. Г.И. Невельского. 690003, г. Владивосток. ул. Верхнепортовая, 50а. Тел. +7 914 665-34-96. E-mail: vlad_6653496@mail.ru

ELECTRONIC KEYS AS A METHOD OF SOFTWARE PROTECTION FROM UNAUTHORIZED USE

Vasilenko K.A.[1], Zolkin A.L.[2], Lyapunov V.N.[1], Semeikin V.A.[3]
[1] Vladivostok State University of Economics and Service, Vladivostok, Russian Federation
[2] Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
[3] Maritime State University named after G.I. Nevelskoy, Vladivostok, Russian Federation
E-mail: k2857@mail.ru, alzolkin@list.ru,
liapunov_vitalii_nikolaevich@vvsu.ru, vlad_6653496@mail.ru

The article describes the principles of operation, types of technical implementation and methods of use of electronic keys. The main Russian manufacturers of electronic keys have been considered and the features of their products have been identified. It is necessary to take into account the correct configuration and support of hardware and software for protection of information while ensuring proper information security of the company, in order to avoid losses, in order to eliminate the risks of obtaining an electronic key by an intruder. Taking into account the fact that electronic keys are mostly referred to hardware methods of software protection from hacking, there are improved cross-platform hardware and software solutions. Their existence is driven by the fact that the developers who design electronic keys also provide a software development kit (SDK) for them. Companies have the ability to implement all means of protecting electronic keys in their own software products using the SDK (such as development tools, protection of software code fragments, development of automatic protection tools, and more).

Keywords: *electronic keys, smart cards, information protection methods, software, unauthorized access, intruder, server, encrypted code, activation keys, identification*

DOI: 10.18469/ikt.2021.19.2.08

Vasilenko Konstantin Alexandrovich, Service and Design College of the Vladivostok State University of Economics and Service, 20, Dobrovolskogo Street, Vladivostok, 690092, Russian Federation; Highest Category Lecturer. Tel. +7 964 453-06-36. E-mail: k2857@mail.ru

Zolkin Alexander Leonidovich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstogo Street, Samara, 443010, Russian Federation; Associate Professor of Computer Science and Computer Engineering Department, PhD in Technical Science. Tel. +7 960 825-68-49. E-mail: alzolkin@list.ru

Lyapunov Vitaliy Nikolaevich, Service and Design College of the Vladivostok State University of Economics and Service, 20, Dobrovolskogo Street, Vladivostok, 690092, Russian Federation; Lecturer. Tel. +7 924 327-19-37. E-mail: liapunov_vitalii_nikolaevich@vvsu.ru

Semeykin Vladislav Andreevich, Maritime State University named after G.I. Nevelskoy, 50a, Verkhneportovaya Street, Vladivostok, 690003, Russian Federation; Student. Tel. +7 914 665-34-96. E-mail: vlad_6653496@mail.ru

References

1. HASP. Wikipedia – the free encyclopedia. URL: https://ru.wikipedia.org/wiki/HASP (accessed: 19.05.2020). (In Russ.)
2. Konjavskaja S. Data protection with USB interface. *Zhurnal setevyh reshenij LAN*, 2007, no. 11, URL: http://www.osp.ru/lan/2007/11/4592946 (accessed: 10.06.2020). (In Russ.)
3. Evaluation of the effectiveness of software protection systems. CIT Forum. URL: http://citforum.ru/security/software/sereda1 (accessed: 29.09.2020). (In Russ.)
4. Skljarov D.V. Hardware security keys. *Iskusstvo zaschity i vzloma informatsii*. SPb.: BHV-Peterburg, 2020, 288 p. (In Russ.)

5. Scheglov A.Yu. *Protection of computer information from unauthorized access*. Saint Petersburg: Nauka i Tehnika, 2019, 384 p. (In Russ.)
6. Platonov V.V. *Information security software and hardware*. Moscow: Akademija, 2013, 336 p. (In Russ.)
7. Rjabko B.Ya., Fionov A.N. *Fundamentals of Modern Cryptography for Information Technology Professionals*. Moscow: Nauchnyj mir, 2004, 173 p. (In Russ.)
8. Alferov A.P. et al. *Fundamentals of Cryptography*. Moscow: Gelios ARV, 2002, 480 p. (In Russ.)
9. Kasperskij K. Technique for embedding code in PE files and methods for removing it. *Haker*, 2004, no. 7, 81 p. (In Russ.)
10. Fergjuson N., Shnajer B. *Practical Cryptography*. Moscow: Dialektika, 2018, 432 p. (In Russ.)
11. Vasilev V.L. et al. Digitalization peculiarities of organizations – A case study. *Entrep. Sustain*, 2020, no. 7, pp. 3173–3190.
12. Dudukalov E.V. State regulation of the development of the national segment of the Internet in Russia. *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski SKAGS*, 2008, no. 3, pp. 155-164. (In Russ.)
13. Dudukalov E.V. Technological parks in the system of national priorities of post-industrial development of the economy. *Ekonomicheskie i gumanitarnye nauki*, 2014, no. 5 (268), pp. 112–118. (In Russ.)
14. Ignatova T. et al. Assessment of Modern Global Trends in Digital Trade and Finance. *Advances in Economics, Business and Management Research*, 2020, vol. 139, pp. 363–366.
15. Ignatova T.V., Dudukalov E.V., Cherkasova T.P. Knowledge ecosystems and digitalization ratings of national economies. *Tsifrovaja ekosistema ekonomiki*: Materialy VII Mezhdunarodnoj nauchno-prakticheskoj videokonferentsii. Rostov-na-Donu: YuFU, 2020, pp. 391–397. (In Russ.)

Received 20.12.2020

УДК 004.4

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ ДЛЯ ИССЛЕДОВАНИЯ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Ряполова Е.И., Студянникова М.А.
Оренбургский филиал Поволжского государственного университета телекоммуникаций и информатики, Оренбург, РФ
E-mail: studyannikovam@mail.ru

Представлена разработка имитационной модели для исследования поведения пользователя в распределённых информационно-вычислительных системах, разработка языковой модели описания поведения пользователя, описаны права доступа, выявлена ключевая информация для составления профиля нормального поведения пользователя, разработана структурная схема и математическая модель по методу анализа аномального поведения пользователя на основе автоматной модели, которая создается на базе правил несанкционированных действий пользователя и содержит сигнатуры аномального поведения пользователя, описано формальное представление таблицы переходов и последовательности действий пользователя, разработана автоматная модель поведения пользователя, представлена обобщенная модель поведения пользователя как цифрового автомата, а также схема алгоритма действий пользователя. Использованы методы теории информационной безопасности, теории автоматов, теории распознавания образов и теории проектирования вычислительных систем.

Ключевые слова: *аномальное поведение пользователей, мониторинг поведения пользователей, системы информационной безопасности, распределённая информационная система, автоматная модель, сигнатурный подход, имитационная модель*

Введение

Для анализа поведения пользователя необходимо осуществлять анализ ряда его поступков и принимать решение о его аномальности. Нельзя считать неправомерным увеличение сетевого трафика пользователя – для принятия решения о