УДК 622.276.001

М.Е. Бурлаков, Ю.В. Алейнов, Д.А. Голубых

Самарский национальный исследовательский университет
им. академика С.П. Королева, Самара, Россия

ИССЛЕДОВАНИЕ ДИНАМИКИ АКТИВНОСТИ ОБНАРУЖЕНИЯ УГРОЗ В МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММАХ ОБМЕНА СООБЩЕНИЯМИ

Исследуется динамика активности обнаружения угроз в мобильных операционных системах и программах обмена сообщениями. Рассмотрена статистика использования мобильных операционных систем за последние два квартала 2015 г. и первые два квартала 2016 г. Сделан акцент на исследовании наиболее часто используемых мобильных операционных систем в настоящее время. Проанализирована динамика декларирования угроз и уязвимостей за последние 5 лет. Аналогично рассмотрена статистика использования средств оперативного обмена сообщениями (мессенджеров, *messengers*) в мире и России в частности. Выделены наиболее популярные решения. Также исследована динамика заявленных угроз и уязвимостей по мобильным программам обмена сообщениями. Анализ как для мобильных операционных систем, так и для мобильных средств передачи информации рассмотрен в рамках открытых и закрытых источников публикации данных. В качестве источников публикации данных об угрозах и уязвимостях предложено к рассмотрению 9 источников. Сделан вывод относительно качества разработки программного обеспечения с демонстрацией динамики обнаружения и устранения уязвимостей. Рассмотрена зависимость обнаружения угроз и уязвимостей между датами публикации со стороны специалистов в области информационной безопасности и злоумышленников и разработчиками соответствующего ПО. Проведено внутреннее сравнение между программным обеспечением отдельно взятого класса с подведением итогов качества разработки и реагирования официальными разработчиками на заявленные угрозы и уязвимости. Выделено наиболее безопасное программное обеспечение обмена сообщениями между пользователями мобильных сетей.

Ключевые слова: обнаружение угроз и уязвимостей, мобильная операционная система, программы обмена сообщениями, мессенджеры, критические обновления.

M.E. Burlakov, Y.V. Aleinov, D.A. Golubyh

Samara National Research University named after academician S.P. Korolev,
Samara, Russian Federation

RESEARCH THE DYNAMIC OF ACTIVITY IN MOBILE OPERATING SYSTEMS AND MESSAGING SOFTWARE THROUGH THREATS DETECTION

In article the research of activity in detection threats and vulnerabilities is made. The consideration of statistics due to using the mobile operating systems is viewed in the last two quarters of 2015 and first two quarters of 2016. The emphasis is placed on researching the most commonly used mobile

operating systems nowadays. The dynamics of declaration threats and vulnerabilities in past 5 years are analyzed. Similarly, the statistics of usage the instant messaging software (messengers) are considered in the world and in Russia. The most popular solutions are chosen. Also, the dynamics of viewed threats and vulnerabilities on mobile messaging programs are researched. Either mobile operating systems or mobile software for communicating are analyzed in public and private publication sources. For this purpose there are 9 sources are offered. The conclusion about software development is made. The dynamic of detecting vulnerabilities and threats is shown. There are dependencies between the dates of threats publications made by specialists in information security or hackers and the reaction of software developers. A comparison between the internal software in definite class is overviewed. The most secure OS and messengers are highlighted.

Keywords: threats and vulnerabilities detection, mobile operating system, messaging programs, instant messengers, critical updates, 0-day exploit.

Введение. На сегодняшний день мир мобильных платформ представляет из себя подобие олигополии с доминированием платформы Android. В табл. 1 представлена статистика распределения мобильных платформ за два последних квартала 2015 г. и два первых квартала 2016 г. [1].

Таблица 1

Распределение мобильных платформ за 2015–2016 гг.

Период	Android	iOS	Windows Phone	Другие
2015Q3	84,3 %	13,4 %	1,8 %	0,5 %
2015Q4	79,6 %	18,6 %	1,2 %	0,5 %
2016Q1	83,4 %	15,4 %	0,8 %	0,4 %
2016Q2	87,6 %	11,7 %	0,4 %	0,3 %

Как видно из таблицы, наиболее популярными платформами являются *Andoroid*, *iOS*.

Начиная с конца 2015 г., количество платформ, использующих iOS в качестве базовой операционной системы (ОС), неуклонно снижается, тогда как доля Android постоянно растет. Однако обе ОС занимают доминирующее положение на рынке, и, с точки зрения специалистов в области информационной безопасности, наиболее актуально уделять внимание именно им в области поиска уязвимостей и потенциальных угроз. С другой стороны, для любого мобильного телефона наличие защиты от угроз и уязвимостей для ОС является необходимым, но недостаточным условием при формировании надежной (обеспечивающей доступность, целостность и конфиденциальность данных) мобильной инфраструктуры. Для решения этой задачи необходимо рассмотреть программное обеспечение (ПО), работающее в рамках мобильных ОС. Зачастую наличие угроз и уязвимостей в них позволяет получать права и привилегии в рамках целой ОС [2].

Одной из наиболее востребованных категорий ПО являются средства общения (мессенджеры) [3]. Среди наиболее популярных можно выделить следующие [4] (рис. 1): WhatsApp; Facebook Messanger; QQ Mobile; WeChat; Skype; Viber; LINE; BlackBerry Messenger (BBM); Telegram; Kakaotalk.

Общее количество пользователей систем обмена сообщениями представлено на рис. 1.

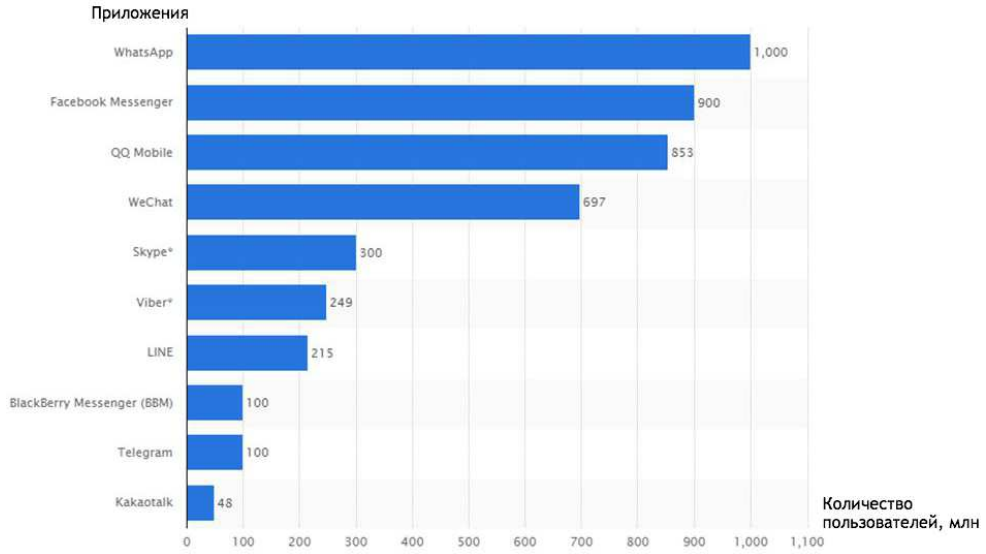

Рис. 1. Количество пользователей ПО по обмену сообщениями за 2016 г.

1. Объекты исследования. В качестве исследования угроз и уязвимостей в ОС были выбраны *Android* и *iOS*, в качестве ПО мессенджеров были выбраны наиболее популярные в России [5]: WhatsApp; Viber; Telegram; Skype.

В качестве инструмента для исследования был взят комплекс *SCAN Project v.1.9.5* (далее – *SCAN*), разработанный в рамках НИОКР «Академия Инфотекс». *SCAN* выполняет следующие функции:

1) автоматизированный сбор информации об угрозах и уязвимостях программных комплексов;

2) выделение информации о времени появления угроз и уязвимостей;

3) выделение информации об авторах, заявивших об обнаружении угроз и уязвимостей.

Для публикации знаний об угрозах и уязвимостях мобильных платформ и приложений как специалисты в области информационной безопасности (ИБ), так и злоумышленники используют источники двух типов: открытые и закрытые. Под *закрытыми источниками* понимаются источники, где доступ информации ограничен разного рода программно-аппаратными решениями. К таковым решениям можно, например, отнести:

– процесс аутентификации, который можно разделить:

- на базовую аутентификацию;
- аутентификацию с подтверждением (*email*, телефона);
- двухфакторную аутентификацию с привязкой к телефону;
- иную вариацию аутентификации;

– технологии:

- *VPN*, *Proxy*, *Socks*, *Mesh*, *TOR* (например, в рамках использовании технологии *TOR* Россия занимает второе место в мире по количество ежедневных сеансов [6], рис. 2) сети (подробнее можно узнать в [7–10]);
- доступ через канал связи с применением специальных сертификатов;
- иные технологические ограничения;

– другие решения, ограничивающие доступ к получению информации об угрозах и уязвимостях.

В случае, если доступ к информации не имеет никаких аппаратно-технических ограничений, источник называют *открытым*.

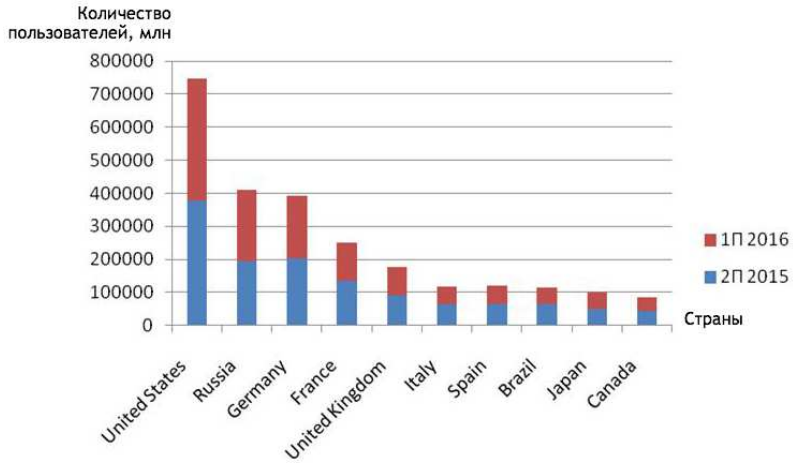

Рис. 2. Кол-во пользователей *TOR*-сети в день по странам
за 2-е полугодие 2015 и 1-е полугодие 2016 г.

На открытых и закрытых источниках как злоумышленники, так и исследователи обмениваются информацией, становясь таким образом авторами обнаруженных угроз и уязвимостей. Зачастую сигнализация о той или иной угрозе служит индикатором использования ПО для специалистов по компьютерной безопасности. В данной статье делается попытка исследовать динамику активности публикации угроз и уязвимостей для мобильных платформ и приложений.

Исследование проводилось на данных, собранных специалистами в области информационной безопасности (мобильных платформ и приложений, в частности) за последние 5 лет наблюдения. Список использованных источников указан в табл. 2.

Таблица 2

Открытые и закрытые источники данных

Наименование источника	Ссылка	Тип
Security Lab	http://www.securitylab.ru/	Открытый
Exploit-DB	https://www.exploit-db.com/	Открытый
CVE Detail	http://www.cvedetails.com/	Открытый
Malwarebytes.org	https://ru.malwarebytes.com/trial/	Закрытый
Htbridge.com	https:// htbridge.com	Закрытый
web.nvd.nist.gov	https://nvd.nist.gov/	Закрытый
0 day	Onion TOR	Закрытый
Seclists.org	http://seclists.org/	Закрытый
Stackoverflow	Stackoverflow.com	Открытый

2. Исследование динамики угроз мобильных платформ. Как было отмечено выше, в качестве исследуемых мобильных платформ были взяты *Android* и *iOS* версий, выпущенных за последний 5 лет. Общее количество заявленных уязвимостей для ОС *Android* – 2956. На рис. 3 представлено их распределение.

Можно заметить, что явно выделяются два пика обнаружения уязвимостей – сентябрь и октябрь 2014 г. В этот период на смартфонах активно работали версии Android 4.1 / 4.2 / 4.3 «Jelly Bean» [11]. Именно они обеспечивали подавляющее количество установок на мобильные телефоны, работающие под платформой *Android*. Именно в этой версии были найдены множественные уязвимости в области работы с данными и протоколами. Например, в версии 4.3.4 была обнаружена грубая ошибка по работе с протоколом *OpenSSL* [12].

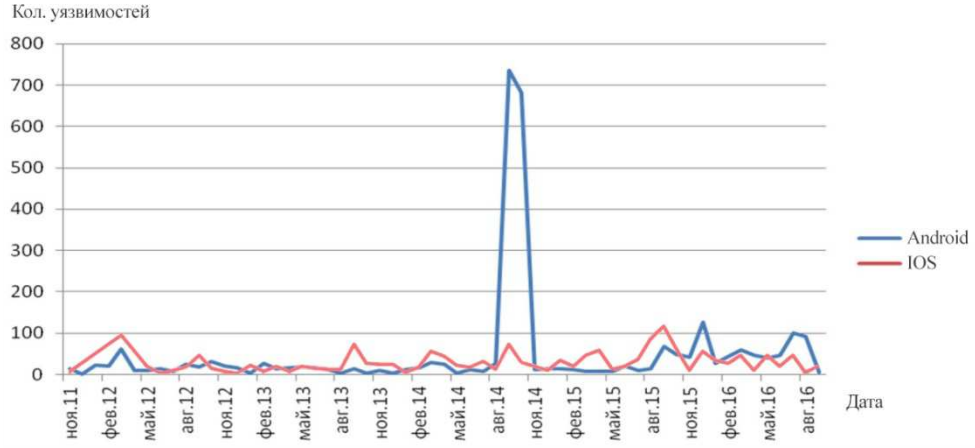

Рис. 3. Динамика распределений заявленных угроз
для ОС *Android* и *iOS* за последние 5 лет

При анализе графика можно обнаружить, что количество уязвимостей после октября 2014 г. снизилось и более не принимало столь критичных значений. До пика среднее количество угроз ровнялось 43, после – 65. Иначе обстоят дела у ОС *iOS* (см. рис. 3). Общее количество заявленных уязвимостей – 2198. Таким образом, это на 26 % меньше, нежели чем у ОС *Android*.

Среднее количество угроз за рассматриваемые периоды равно 76. Можно заключить, что если бы не пик обнаружения угроз у *Android* в среднем у ОС *iOS* среднее количество угроз и уязвимостей выше на 29 %. Исходя из этих данных, явно выделяются пять пиков обнаружения уязвимостей [13]:

- март 2012 (*iOS v 5.x*);
- сентябрь 2013 (*iOS v 5.x*);
- сентябрь 2014 (*iOS v 6.x*);
- август 2015 (*iOS v 8.x*);
- сентябрь 2015 (*iOS v 8.x*).

Стоит заметить, что в данном случае на графике просматривается периодичность, т.е. приблизительно через равные промежутки времени появляются как максимумы, так и минимумы. Это явная отличительная особенность анализа угроз и уязвимостей платформы *iOS* над платформой *Android* (см. рис. 2).

Это может быть связано с тем, что количество обновлений, выпускаемых компанией *Google* (разработчик платформы *Android*), больше,

нежели компанией *Apple* (разработчик платформы *iOS*), и скорость их применения более оперативна [14]. С другой стороны, разработчики *Android* с целью повышения качества и безопасности работы софта постоянно его улучшают, что приводит к неминуемому росту пользователей данной ОС по сравнению с другими платформами (см. табл. 1), тогда как разработчики других платформ более инертно реагируют на появившиеся угрозы, подвергая тем самым угрозе своих пользователей.

3. Исследование динамики угроз мобильных средств передачи сообщений (мессенджеров). Как было указано выше, для анализа угроз в мобильных средствах передачи сообщений (мессенджеров) были выбраны 4 наиболее популярных в России решения [15]: WhatsApp; Viber; Telegram; Skype.

Общий анализ заявленных за последние 5 лет угроз и уязвимостей позволил получить следующую картину (табл. 3).

Таблица 3

Распределение уязвимостей по средствам общения за последние 5 лет

№	Мессенджер	Количество уязвимостей	Даты публикации
1	WhatsApp	5	12.2011, 01.2012, 04.2014, 12.2014, 05.2015
2	Viber	2	08.2015, 07.2016
3	Telegram	5	06.2016
4	Skype	17	09-12.2015, 04.2016, 08.2016

Исходя из полученных статистических данных, можно заключить, что наиболее уязвимым ПО для обмена сообщений является *Skype*, тогда как самым защищенным – *Viber*. При отдельном анализе приложения *Skype* можно заявить, что уязвимости обнаруживаются в большом количестве и за сравнительно короткие промежутки времени в отличие от других заявленных средств обмена сообщениями.

Картина выглядит более странной, если заключить, что Skype начал разрабатываться задолго до появления других мессенджеров [16].

Выводы. Таким образом, исходя из полученных данных, можно сделать следующие выводы:

1. Количество обнаруженных угроз для ОС *Android* больше, чем для ОС *iOS*, однако скорость исправления выше, что подтверждается графиком распространения ОС *Android* среди пользователей мобильных платформ.

2. Пики обнаружения угроз приходятся либо сразу после обнародования новой версии ОС *Android* и *iOS* (ошибки «свежей» системы), либо на момент перед обновлением – критические уязвимости, исправление которых приурочено к выходу новой версии.

3. Наиболее защищенным ПО для оперативного обмена сообщениями на данный момент является *Viber*, тогда как *Skype* – наименее защищенная платформа. Если у *Viber*, *WhatsApp* и *Telegram* уязвимости обнаруживаются небольшим объемом и периодически, то у *Skype* имеет место множественное обнаружение проблем за короткий промежуток времени (не более 1 месяца).

Библиографический список

1. Smartphone OS Market Share, 2016 Q2 [Электронный ресурс]. – URL: http://www.idc.com/prodserv/smartphone-os-market-share.jsp (дата обращения: 01.11.2016).

2. Donenfeld A. QuadRooter: New Android Vulnerabilities in Over 900 Million Devices [Электронный ресурс]. – URL: http://blog.checkpoint.com/2016/08/07/quadrooter/ (дата обращения: 30.10.2016).

3. Печеровий А. Мобильные приложения: Тренды и итоги 2015 года [Электронный ресурс]. – URL: https://thatsmart.ru/2016/01/mob-apps-trends/ (дата обращения: 01.11.2016).

4. Most popular mobile messaging apps worldwide as of April 2016, based on number of monthly active users (in millions) [Электронный ресурс]. – URL: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (дата обращения: 30.10.2016).

5. ТОП мессенджеров – обзор и рейтинг мессендежров [Электронный ресурс]. – URL: http://xn--d1ababe6aj1ada0j.xn--p1ai/top-messendzherov-obzor-i-rejting-messendezhrov.html (дата обращения: 29.10.2016).

6. Top-10 countries by directly connecting users [Электронный ресурс]. – URL: https://metrics.torproject.org/userstats-relay-table.html (дата обращения: 01.11.2016).

7. Julian Applebaum. A Model of Outbound Client Traffic on the Tor Anonymity Network // Wesleyan University. – 2013. – С. 54–58.

8. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – С. 368–376.

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. – СПб.: Питер, 2001. – С. 670–672.

10. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. – М.: Вильямс, 2002. – С. 429–440.

11. Android: A visual history [Электронный ресурс]. – URL: http://www.webcitation.org/6DpDvrrwH (дата обращения: 28.10.2016).

12. Whitwam R. Google Rolling Out Android 4.4.4 Update (KTU84P) With A Security Fix, Factory Images/Binaries Up For Nexus Devices [Электронный ресурс]. – URL: http://www.androidpolice.com/2014/06/19/google-rolling-out-android-4-4-4-update-ktu84p-with-a-security-fix-factory-images-binaries-up-for-nexus-devices/ (дата обращения: 28.10.2016).

13. Обновления системы безопасности Apple [Электронный ресурс]. – URL: https://support.apple.com/ru-ru/HT201222 (дата обращения: 28.10.2016).

14. When Malware Goes Mobile [Электронный ресурс]. – URL: https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx (дата обращения: 28.10.2016).

15. Исследование App Annie: самые-самые мессенджеры [Электронный ресурс]. – URL: http://gdetraffic.com/Analitika/Issledovanie_App_Annie_samye (дата обращения: 29.10.2016).

16. Краткая история Skype: к десятилетию революционного сервиса [Электронный ресурс]. – URL: http://www.computerra.ru/81802/kratkaya-istoriya-skype-k-desyatiletiyu-revolyutsionnogo-servisa/ (дата обращения: 28.10.2016).

References

1. Smartphone OS Market Share, 2016 Q2, available at: http://www.idc.com/prodserv/smartphone-os-market-share.jsp (accessed 01 November 2016).

2. Donenfeld A. QuadRooter: New Android Vulnerabilities in Over 900 Million Devices, available at: http://blog.checkpoint.com/2016/08/07/quadrooter/ (accessed 30 October 2016).

3. Pecherovii A. Mobil'nye prilozheniia: Trendy i itogi 2015 goda [About mobile software, it’s trends and results in 2015 year], available at: https://thatsmart.ru/2016/01/mob-apps-trends/ (accessed 01 November 2016).

4. Most popular mobile messaging apps worldwide as of April 2016, based on number of monthly active users (in millions), available at: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (accessed 30 October 2016).

5. TOP messendzherov – obzor i reiting messendezhrov [About top messengers, it's overviewed and raitings], available at: http://xn--d1ababe6aj1ada0j.xn--p1ai/top-messendzherov-obzor-i-rejting-messendezhrov.html (accessed 29 October 2016).

6. Top-10 countries by directly connecting users, available at: https://metrics.torproject.org/userstats-relay-table.html (accessed 01 November 2016).

7. Julian Applebaum. A Model of Outbound Client Traffic on the Tor Anonymity Network. Wesleyan University, 2013, pp. 54-58.

8. Ivanov M.A. Kriptograficheskie metody zashchity informatsii v komp'iuternykh sistemakh i setiakh [The cryptographic methods of information security in computer systems and networks]. Moscow: KUDITs-OBRAZ, 2001, pp. 368-376.

9. Olifer V.G., Olifer N.A. Komp'iuternye seti. Printsipy, tekhnologii, protokoly [Computer networks. Principles, technologies, protocols: Textbook for high schools]. Saint Petersburg: Piter, 2001, pp. 670-672.

10. Stollings V. Osnovy zashchity setei. Prilozheniia i standarty [Fundamentals of network security. Applications and Standards = Network Security Essentials]. Moscow: Vil'iams, 2002, pp. 429-440.

11. Android: A visual history, available at: http://www.webcitation.org/6DpDvrrwH (accessed 28 October 2016).

12. Whitwam R. Google Rolling Out Android 4.4.4 Update (KTU84P) With A Security Fix, Factory Images/Binaries Up For Nexus Devices, available at: http://www.androidpolice.com/2014/06/19/google-rolling-out-android-4-4-4-update-ktu84p-with-a-security-fix-factory-imagesbinaries-up-for-nexus-devices/ (accessed 28 October 2016).

13. Obnovleniia sistemy bezopasnosti Apple [About security system updates on Apple devices], available at: https://support.apple.com/ru-ru/HT201222 (accessed 28 October 2016).

14. When Malware Goes Mobile, available at: https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx (accessed 28 October 2016).

15. Issledovanie App Annie: samye-samye messendzhery [Research App Annie: the most-most messengers], available at: http://gdetraffic.com/Analitika/Issledovanie_App _Annie_samye (accessed 29 October 2016).

16. Kratkaia istoriia Skype: k desiatiletiiu revoliutsionnogo servisa [About the anniversary of Skype due to ten years of developing], available at: http://www.computerra.ru/81802/kratkaya-istoriya-skype-k-desyatiletiyu-revolyutsionnogo-servisa/ (accessed 28 October 2016).

Сведения об авторах

Бурлаков Михаил Евгеньевич (Самара, Россия) – лаборант кафедры безопасности информационных систем Самарского национального исследовательского университета им. академика С.П. Королева (443086, г. Самара, ул. Московское шоссе, 34, e-mail: knownwhat@gmail.com).

Алейнов Юрий Викторович (Самара, Россия) – старший преподаватель кафедры безопасности информационных систем Самарского национального исследовательского университета им. академика С.П. Королева (443086, г. Самара, ул. Московское шоссе, 34, e-mail: aleinov@gmail.com).

Голубых Денис Алексеевич (Самара, Россия) – студент Самарского национального исследовательского университета им. академика С.П. Королева (443086, г. Самара, ул. Московское шоссе, 34, e-mail: den1008@bk.ru).

About the authors

Burlakov Mikhail Evgenyevich (Samara, Russian Federation) is a Laboratory Assistant in Department of information security systems Samara National Research University named after academician S.P. Korolev (443086, Samara, 34, Moskovskoye Shosse, e-mail: knownwhat@gmail.com).

Aleinov Yury Viktorovich (Samara, Russian Federation) is a Senior Lecturer in Department of information security systems Samara National Research University named after academician S.P. Korolev (443086, Samara, 34, Moskovskoye Shosse, e-mail: aleinov@gmail.com).

Golubyh Denis Alekseevich (Samara, Russian Federation) is a Student Samara National Research University named after academician S.P. Korolev (443086, Samara, 34, Moskovskoye Shosse, e-mail: den1008@bk.ru).

Получено 16.02.2017