УДК 004.056 **DOI: 10.18413/2518-1092-2022-7-2-0-3**

Кузьминых Е.С.
Маслова М.А.

АНАЛИЗ ОСНОВНЫХ МОБИЛЬНЫХ УГРОЗ И СПОСОБЫ ЗАЩИТЫ ОТ ВИРУСОВ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Аннотация
В век расцвета информационных технологий и развития функциональных возможностей мобильных телефонов человек начинает больше пользоваться телефоном, ведь это очень удобно, к тому же телефоны в последнее время становятся всё мощнее и мощнее. Но не стоит забывать про злоумышленников, которые начинают всё сильнее охотиться за данными пользователей на телефонах, ведь получить доступ к мобильнику гораздо легче, чем к хорошо защищённому и сложно оборудованному компьютеру, потому что мало кто пользуется специальными методами по защите своего телефона от потенциальных угроз. Если брать во внимание новые уязвимости, которые появляются после каждого обновления, что приводит к появлению угроз «нулевого дня», то бороться с такими угрозами становится невозможно для рядового пользователя. В данной статье будут рассмотрены основные мобильные угрозы, как с ними бороться, что делать, если все же угроза наступила и ваше мобильное устройство в опасности, так же произведена аналитика развития и актуальности мобильных вирусных ПО.
Ключевые слова: мобильные угрозы; вирусы; вирусное программное обеспечение (ВПО); защита от вируса; безопасность; защита мобильного телефона; антивирусы
Для цитирования: Кузьминых Е.С., Маслова М.А. Анализ основных мобильных угроз и способы защиты от вирусов // Научный результат. Информационные технологии. – Т.7, №2, 2022. – С. 28-34. DOI: 10.18413/2518-1092-2022-7-2-0-3

Kuzminykh E.S.
Maslova M.A.

ANALYSIS OF THE MAIN MOBILE THREATS AND WAYS TO PROTECT AGAINST VIRUSES

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Abstract
In the age of the heyday of information technology and the development of the functionality of mobile phones, people are starting to use the phone more, because it is very convenient, besides phones have recently become more and more powerful. But do not forget about intruders who are starting to hunt more and more for user data on phones, because it is much easier to get access to a mobile phone than to a well-protected and complexly equipped computer, because few people use special methods to protect their phone from potential threats. If we take into account the new vulnerabilities that appear after each update, which leads to the emergence of "zero-day" threats, then it becomes impossible for an ordinary user to deal with such threats. This article will discuss the main mobile threats, how to deal with them, what to do if the threat has come and your mobile device is in danger, as well as the analysis of the development and relevance of mobile virus software.
Keywords: mobile threats; viruses; virus software (VPO); virus protection; security; mobile phone protection; antiviruses
For citation: Kuzminykh E.S., Maslova M.A. Analysis of the main mobile threats and ways to protect against viruses // Research result. Information technologies. – T.7, №2, 2022. – P. 28-34. DOI: 10.18413/2518-1092-2022-7-2-0-3

ВВЕДЕНИЕ

В последние десятилетия функции мобильных телефонов значительно прогрессируют. Мобильные телефоны уже не отстают от возможностей компьютеров. Нынешнее программное обеспечение мобильных телефонов вполне способно выполнять такие же действия, как и компьютер. Если сравнивать мобильный телефон с персональным компьютером (ПК), то есть конечно минусы – это размер экрана, но на фоне плюсов он совсем не значительный, т.к. в нем можно увеличивать размер шрифта, приближать объекты и всё же мобильник не такой мощный, в отличии от компьютера. Зато плюсов очень много, а именно: автономность работы; удобность в использовании (телефон всегда находится у человека, здесь его минус в маленьком размере, становится плюсом, т.к. он занимает мало места и помещается в карман и благодаря этому им можно пользоваться где угодно от дома до работы и отдыха на природе); звонки можно осуществлять в любой момент с любой точки доступа (при наличии мобильной связи), выполнение редактирования файлов word, excel, редактирование видео и фото. Неотъемлемой частью являются развлечение и отдых - просмотр фильмов и видео, возможность играть в игры, ну а если необходимо найти необходимую информацию, воспользовавшись мобильным интернетом, голосовым помощником и найти интересующую информацию очень быстро.

Все эти модификации и улучшения мобильных телефонов породило хакеров «расшевелиться» и придумывать различные виды вирусных программ для них. Всё же с большинством компьютерных вирусов мы уже немного знакомы, а вирусы на мобильных телефонах еще остаются для многих людей чем-то новым, непонятным и незнакомым. Если на компьютере почти каждый пользователь может использовать даже самый простой антивирус для даже слабой защиты компьютера, то на телефонах очень мало кто пользуется антивирусами. Мобильные вирусы «поймать» на телефон не так уж и легко, но возможно. Проведем анализ существующих вирусов, существующие угрозы и способы их распространения, а также защита от них [1].

ОСНОВНАЯ ЧАСТЬ

История развития вирусов для мобильных телефонов началась не так давно, но набирает стремительные обороты. Первым мобильным вирусом в 2004 году был Cabir, работавший на ОС Symbain, который был на телефонах Nokia, в то время такие телефоны были редкостью, поэтому вирус не получил сильной огласки. Так как это был первый вирус в истории, он не мог многого, он только распространялся посредством передачи себя через Bluetooth на другие телефоны с нагрузкой их на центральный процессор, что быстро разряжало их. Теперь же вирусы стали более «умными» и «вредными», рассмотрим основные из них [10]:

– Adware и кликеры. Иногда для данного вида угроз используется термин «Madware» (Mobile Adware). Основная цель этого класса вредоносного программного обеспечения (ВПО) – показ пользователю нерелевантной рекламы и генерирование искусственных переходов на сайты рекламодателей. С помощью «Madware» злоумышленники зарабатывают «клики» и демонстрируют оплачивающим их компаниям иллюзию интереса пользователей.

– Spyware – ПО, осуществляющее кражу персональных данных или слежку за своим носителем. Фактически, мобильное устройство может превратиться в полноценный «жучок», передавая злоумышленникам данные о сетевой активности, геолокации, истории перемещений, а также фото и видеоинформацию, данные о покупках, кредитных картах и др.

– Дроппер – ВПО, целью которого является скачивание другого вредоносного ПО.

– Вирус – ПО, которое наносит явный вред, например, выводит из строя конкретное приложение или одну из функций устройства.

– Бот – агент бот-сетей, ВПО, которое по команде C&C-сервера осуществляет требуемую злоумышленнику сетевую активность [13].

Чтобы не стать жертвой злоумышленника, не обязательно знать каждый тип вируса, достаточно иметь поверхностные знания, что такое ВПО [4]. Самое главное, пожалуй, это знать, где вас может «подкараулить» вирус и как от него избавиться, если вы поняли, что ваш телефон даёт сбои.

Выделим основные источники угроз:

– установка приложений из неофициальных источников (кряки, взломы),

– получение SMS, или письма на почту с вредоносной ссылкой/приложением,

– социальная инженерия, а именно звонки от операторов с целью «выудить» у вас конфиденциальную информацию, или просьба подключиться к удалённому доступу, после чего злоумышленник сможет сделать всё, что угодно с компьютером и его содержимым.

Рассмотрев «предка» всех вирусов, основные виды ВПО, каналы их распространения и в кульминации необходимо понять, как же бороться с этими злосчастными вирусами.

Если вы хотите добиться максимальной защиты своего мобильного телефона, то необходимо выполнять следующие основные методы:

– одно из главных условий, необходимо установить на свое устройство антивирус. Желательно, чтоб он был не самый ресурсно-затратный, но и не самый простой (проанализировать их и выбрать удобный для вас можно в топе лучших антивирусов для мобильных телефонов);

– если у вас присутствуют важные для вас данные, тогда нужно их шифровать, даже если это обычный текст, или целые папки, ведь при взломе вашего телефона злоумышленнику будет сложно расшифровать их, или скорее всего невозможно;

– необходимо защищать сетевой трафик, пользоваться VPN, или специальными корпоративными шлюзами, фильтрующими и защищающими трафик;

– своевременно обновлять свою операционную систему, обновлять все приложения;

– запретить телефону устанавливать приложения без вашего ведома, а также запретить выполнение других важных действий;

– установить двухфакторную аутентификацию на важные для вас приложения;

– настроить очистку данных на устройстве при попытке взлома методом удалённого ввода команды, или же после нескольких неудачных попыток входа в систему [12].

Что делать если вас всё же взломали, и злоумышленник уже имеет доступ к вашему телефону? Во-первых, главное не паникуйте, скорее всего злоумышленник получил ваши данные и не имеет удалённого доступа к вашему телефону, это значит, что он просмотрит ваши данные через какое-то время и у вас есть время на смену всех паролей и очистку телефона. А если хакер всё-таки получил удалённый доступ к телефону, то вам ничто не мешает просто его выключить и повторить прошлые шаги [11].

Вирус RAT также один из применяемых вирусов заражения телефона RAT (Remote Access Trojan), через APK (Android Package), установив их в браузере, или через Google Play. [2]

Такие вирусы могут иметь возможности:

– «склеивание» вирусов и готовых приложений;

– создание зараженных приложений с невидимыми иконками;

– маскировка вируса под иконкой готового приложения;

– запуск вируса в текущей сессии или после перезагрузки устройства

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

История развития вирусного ПО в сфере мобильных телефонов довольна обширна, рассмотрим статистику, относящуюся к истории их развития, как увеличивалось количество известных семейств мобильных вирусов (рис. 1).

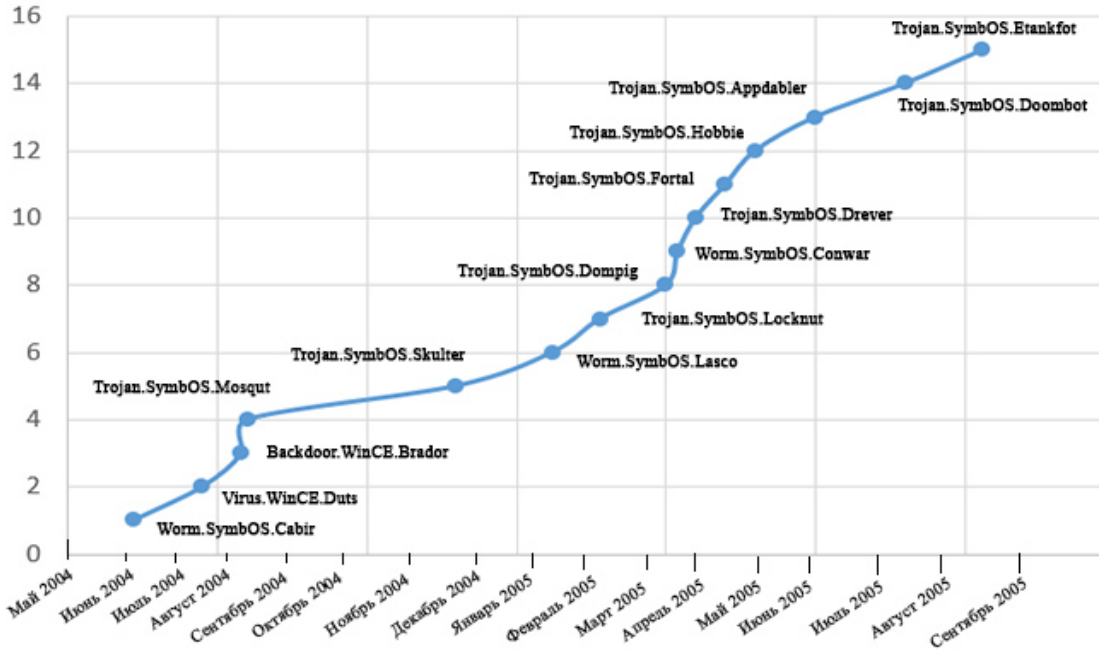

Рис. 1. Увеличение количества известных семейств мобильных вирусов [5]
Fig. 1. An increase in the number of known families of mobile viruses [5]

Вернёмся на 20 лет назад и попытаемся понять, когда же вирусное ПО получило свою огласку и стало настолько масштабно распространяться, что мировые компании обратили своё внимание на них и начали предпринимать специальные действия для борьбы с ними. К примеру «Лаборатория Касперского» является крупнейшей компанией, предоставляющей антивирусные услуги в Российской Федерации, они каждый год публикуют статистику по активности ВПО в РФ и аналитику на следующий год. Произведём сравнение опубликованных диаграмм далее.

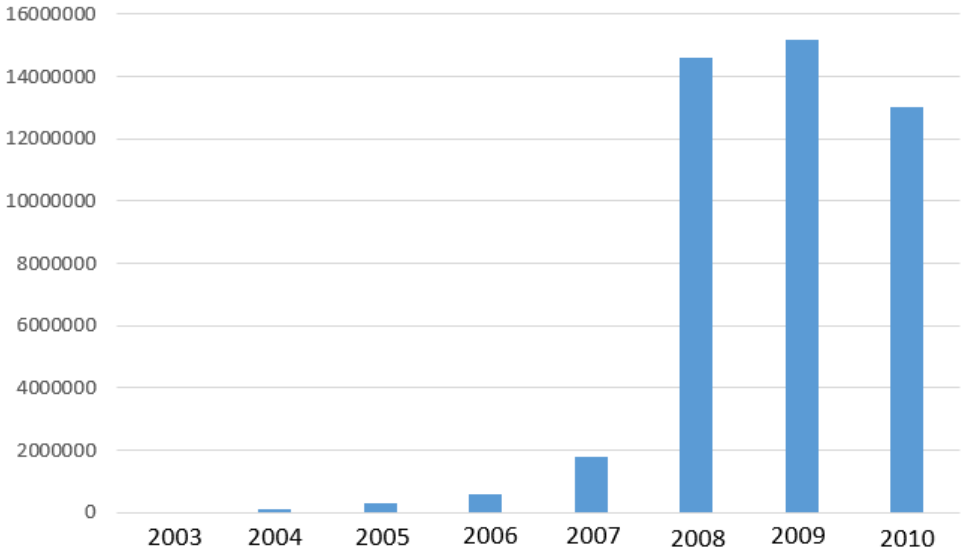

Рис. 2. Число новых вредоносных программ [8]
Fig. 2. Number of new malware [8]

Проанализировав данный график можно понять, что до 2008 года хакеры проводили так называемую «разведку», что же могут ВПО и как сложно их создать и поняв всю суть, в 2008 году появился громадный наплыв вирусов на мобильные устройства пользователей, что повергло всех в шок, ведь никто не был готов к такому развитию. Начиная с 2008 года к мобильным вирусам

перестали относиться, как к чему-то незначащему и начали серьёзно относиться к данной проблеме и постоянно искать способы уничтожения и предотвращения их появления.

После 2010 года пошёл небольшой спад, но не на долго, уже в 2011 году начали выпускать улучшения старым вирусами, что дало новый толчок в сфере мобильных ВПО и уже в 2012 году появился большой наплыв уже модифицированных вирусов. Статистика обнаружения модифицированных ВПО в 2011-2012 годах по кварталам (К) (рис. 3).

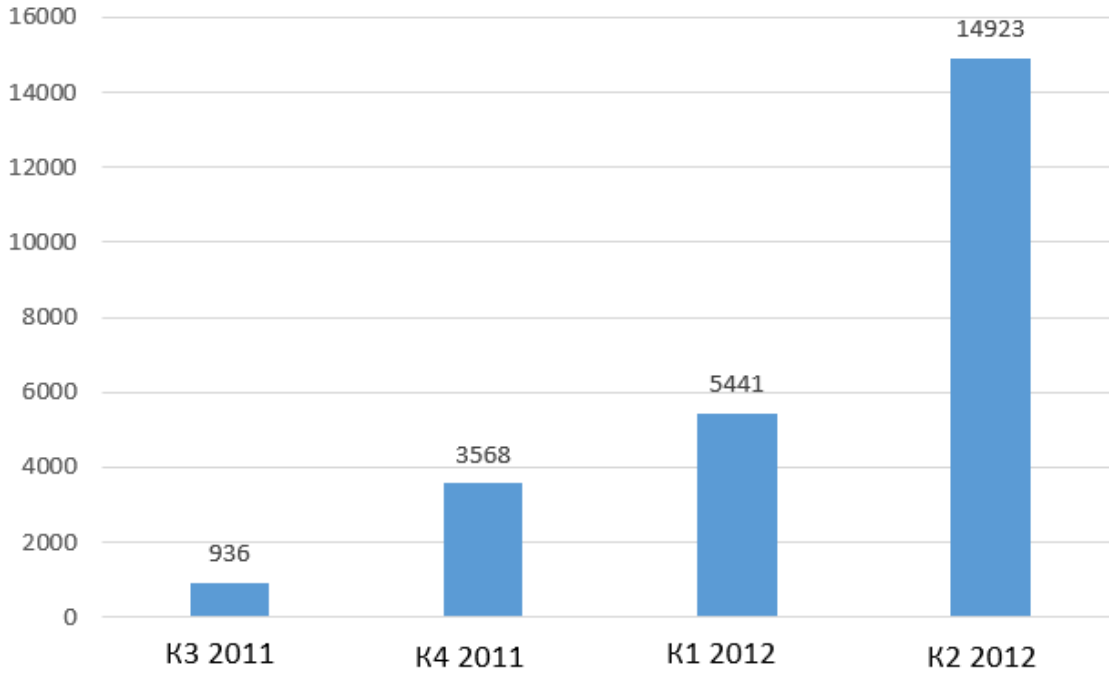

Рис. 3. Количество обнаруженных модификаций ВПО в 2011-2012 годах [7]
Fig. 3. Number of detected malware modifications in 2011-2012 [7]

В заключении далее предоставлен график, показывающий насколько спало количество появления ВПО в настоящее время. Всё довольно просто, пользователи стали информационно образованны, большинство из них теперь знает, как не попасться в «капкан», так же и антивирусы стали более умными, некоторые из них вполне способны справиться с вирусами «нулевого дня». В пример можно привести самый известный антивирус в РФ – Kaspersky, он нём, казалось бы, слышали все, в организации работают профессионалы своего дела, антивирус постоянно обновляется, качественно справляется со всеми вирусами и способен бороться с вирусами «нулевого дня». Версия Kaspersky EDR более полезна для компаний, данная версия помогает сотрудникам компании бороться с большинством угроз, влияющих на работу организации (рис 4).

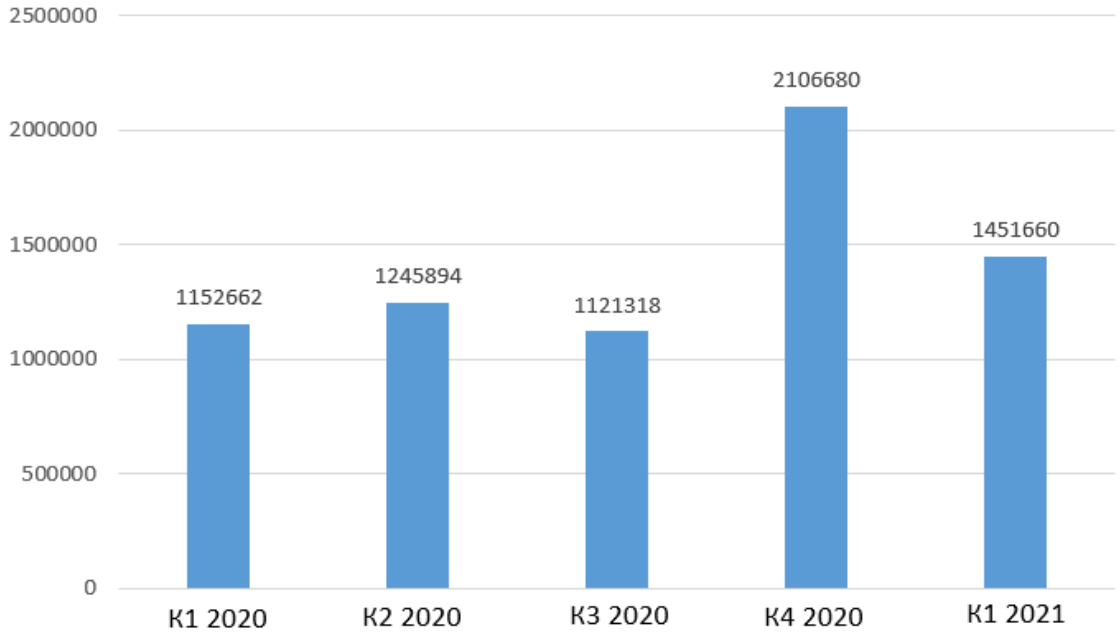

Рис. 4. Количество обнаруженных ВПО в 2020-2021 годах [6]
Fig. 4. Number of malware detected in 2020-2021 [6]

ЗАКЛЮЧЕНИЕ

Из приведённых данных становится понятно, как появились ВПО, что они могут сделать с мобильным телефоном, насколько они опасны. Были проанализированы и приведён список основных ВПО, список основных мобильных угроз и рекомендации по борьбе с ними если пользователь уже попал в «капкан». Если постоянно мониторить рынок, использовать основные способы защиты, устанавливать новые антивирусы и программы защиты, то можно защитить свой мобильный телефон на 99,9%. Полной защиты добиться практически невозможно, так как выпускаются постоянно не только новые защиты, но и новые вирусы. Если вы обычный пользователь, то навряд ли будете вызывать у хакера большой интерес, поэтому вполне достаточно будет установить обычную среднюю защиту, чтобы ваши данные были в безопасности и соблюдать основные правила пользования мобильным телефоном.

Если проанализировать все графики, приведённые в статье, и посмотреть статистику вирусов для персональных компьютеров, будет видно, что история с компьютерами повторилась, также никто не был готов к такому громадному наплыву ВПО. Оказалось всё довольно просто, хакеры нашли достаточно уязвимостей, подготовились, провели «разведку» и отправили на пользователей волну вирусов, когда к этому были плохо готовы, в последствии конечно же с ними стали усердно бороться и вирусов стало гораздо меньше.

Подводя итоги, можно выделить, чтобы оставаться в безопасности, не стоит заходить на сайты, вызывающие подозрения, не качать никакие файлы с пиратских сайтов, ну и конечно же соблюдать шаги по обеспечению безопасности своего мобильника, перечисленные в данной статье и тогда никто не украдёт пароль от вашей карточки, или социальной сети.

Список литературы

1. Исследование уязвимости мобильных устройств систем Apple и Google / Михайлов Д.М., Зуйков А.В., Жуков И.Ю., Бельтов А.Г., Стариковский А.В., Фроимсон М.И., Толстая А.М. // Спецтехника и связь. – 2011. – №. 6. – С. 38-40.

2. Какаев Д.В., Маслова М.А. Обзор вирусов удаленного доступа для мобильных устройств // Научный результат. Информационные технологии. – 2020. – Т. 5. – № 1. – С. 27-34.

3. Мобильные угрозы и методы борьбы с ними. URL: https://clck.ru/gvaQa (дата обращения: 15.04.2022).

4. Ожиганова М.И. Архитектура безопасности киберфизической системы // Защита информации. Инсайд. – 2022. – № 2(104). – С. 5-9.

5. Появление и развитие вирусов для мобильных устройств. URL: https://clck.ru/gvZCx (дата обращения: 17.04.2022).

6. Развитие информационных угроз в первом квартале 2021 г. URL: https://clck.ru/ZRvjF (дата обращения: 22.04.2022).

7. Развитие информационных угроз во втором квартале 2012 г. URL: https://clck.ru/gva7i (дата обращения: 17.04.2022).

8. Развитие угроз в 2010 году. URL: https://clck.ru/gvZyT (дата обращения: 15.04.2022).

9. Уязвимости и угрозы мобильных приложений. URL: https://clck.ru/bmpYJ (дата обращения: 15.04.2022).

10. Унучек Р. Мобильные угрозы // Системный администратор. – 2016. – №. 11. – С. 38-41.

11. Унучек Р.С., Чебышев В. В. Мобильные угрозы 2013 // Вопросы кибербезопасности. 2014. – №. 3(4). – С. 57-64.

12. Цыганенко Н. П. Статический анализ кода мобильных приложений как средство выявления его уязвимостей // Труды БГТУ. Серия 3: Физико-математические науки и информатика. – 2015. – № 6(179). – С. 200-203.

13. Cabir – первый мобильный вирус в мире. URL: https://clck.ru/gunA9 (дата обращения: 15.04.2022).

References

1. Exploring the vulnerability of Apple and Google mobile devices / D.M. Mikhailov, A.V. Zuykov, I.Yu. Zhukov, A.G. Beltov, A.V. Starikovsky, M.I. Fromoimson, A. Tolstaya. M. // Special equipment and communications. – 2011. – No. 6. – P. 38-40.

2. Kakaev D.V., Maslova M.A. Overview of remote access viruses for mobile devices // Research result. Information Technology. – 2020. – V. 5. – No. 1. – P. 27-34.

3. Mobile threats and methods of dealing with them. URL: https://clck.ru/gvaQa (date of access: 15.04.2022).

4. Ozhiganova M.I. Security Architecture of a Cyber-Physical System // Information Security. Inside. – 2022. – No. 2(104). – P. 5-9.

5. Emergence and development of viruses for mobile devices. URL: https://clck.ru/gvZCx (date of access: 17.04.2022).

6. Development of information threats in the first quarter of 2021. URL: https://clck.ru/ZRvjF (date of access: 22.04.2022).

7. Development of information threats in the second quarter of 2012. URL: https://clck.ru/gva7i (date of access: 17.04.2022).

8. Development of threats in 2010. URL: https://clck.ru/gvZyT (date of access: 15.04.2022).

9. Vulnerabilities and threats of mobile applications. URL: https://clck.ru/bmpYJ (date of access: 15.04.2022).

10. Unuchek R. Mobile threats // System administrator. – 2016. – No. 11. – P. 38-41.

11. Unuchek R.S., Chebyshev V.V. Mobile threats 2013 // Cyber security issues. – 2014. – No. 3(4). – P. 57-64.

12. Tsyganenko N. P. Static analysis of mobile application code as a means of identifying its vulnerabilities // Proceedings of BSTU. Series 3: Physical and mathematical sciences and informatics. – 2015. – No. 6(179). – P. 200-203.

13. Cabir is the first mobile virus in the world. URL: https://clck.ru/gunA9 (date of access: 15.04.2022).

Кузьминых Егор Сергеевич, студент кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Kuzminykh Yegor Sergeevich, student of the Department Information security, Institute of Radioelectronics and Information security

Maslova Maria Alexandrovna, senior lecturer of the Department Information security, Institute of Radioelectronics and Information security