УДК 004.23 **DOI: 10.18413/2518-1092-2020-5-1-0-4**

Какаев Д.В.
Маслова М.А.

ОБЗОР ВИРУСОВ УДАЛЕННОГО ДОСТУПА ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

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

e-mail: 619deniss61999@gmail.com, mashechka-81@mail.ru

Аннотация
Современный уровень распространенности мобильных устройств делает их доступными каждому. На смартфонах хранятся многие важные файлы и с помощью смартфонов осуществляют финансовые операции и операции авторизации. В связи с этим возросло количество мошенников, желающих получить, хранящиеся на телефоне данные. Но защиты мобильных устройств не позволяет быть спокойным за безопасность информации. Создание вредоносного программного обеспечения не составляет труда и по силам любому энтузиасту. Для этого не нужно обладать навыками программирования, разбираться в уязвимостях операционных систем или обладать каким-то труднодоступным софтом. Достаточно воспользоваться одной из многих программ, находящихся в открытом доступе и доступным всем желающим. В статье рассмотрены варианты распространения вирусов удаленного доступа на примере операционной системы Android, как самой популярной, алгоритм создания простейшего вируса, с помощью программы AhMyth, и некоторые рекомендации по защите своего устройства.
Ключевые слова: Вирус удаленного доступа; RAT; Remote Access Trojan; Android; AhMyth; безопасность; уязвимость.

UDC 004.23

Kakaev D.V.
Maslova M.A.

OVERVIEW OF REMOTE ACCESS VIRUSES FOR MOBILE DEVICES

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

e-mail: 619deniss61999@gmail.com, mashechka-81@mail.ru

Abstract
The current level of prevalence of mobile devices makes them available to everyone. Many important files are stored on smartphones and financial transactions and authorization operations are performed using smartphones. In this regard, the number of scammers who want to get the data stored on the phone has increased. But the protection of mobile devices does not allow you to be calm about the security of information. Creating malicious software is not difficult and can be done by any enthusiast. To do this, you do not need to have programming skills, understand operating system vulnerabilities, or have some hard-to-access software. It is enough to use one of the many programs that are in the public domain and available to everyone. The article discusses options for the distribution of remote access viruses on the example of the Android operating system, as the most popular, the algorithm for creating a simple virus using the program AhMyth, and some recommendations for protecting your device.
Keywords: remote access Virus; RAT; Remote Access Trojan; Android; AhMyth; security; vulnerability.

ВВЕДЕНИЕ

Смартфон является одним из самых популярных гаджетов в современном мире. Практически у каждого человека имеется хотя бы один смартфон или планшет. По данным NICE LAB на 2019 год в мире используется 5.6млрд. смартфонов, а на 100 человек населения приходится примерно 74 смартфона. [1] В России этот показатель на 10 сентября 2019 года по

данным Inventive Retail Group составляет 88.1млн. смартфонов, что составляет 60 смартфонов на сто человек населения. [2] Но помимо колоссального удобства и постоянной мобильности, смартфоны несут и угрозы. Одними из самых распространенных пользователей, подвергающихся угрозам, являются дети и пожилые люди, которые могут плохо разбираться в работе гаджетов и не знать основных действий, предотвращающих угрозам, что может повлечь за собой определенные проблемы. Ведь правилам безопасного использования «гаджетами», к сожалению, не обучают ни при покупке их, ни в школах или где-то еще. Следовательно, неумелые пользователи – это большая угроза безопасности, чем какие-либо ошибки в программном обеспечении устройства.

ОСНОВНАЯ ЧАСТЬ

Сейчас на смартфонах хранится большое количество личной информации: фотографии в памяти телефона и облачных хранилищах, аккаунты в социальных сетях и иных ресурсах, телефонные номера и другие файлы. Социальные сети, интернет-банкинг и интернет ресурсы обеспечивают защиту данных с помощью криптографии и защищенных протоколов от попыток взлома алгоритма защиты или перехвата данных. Но вся эта защита бессмысленна, если злоумышленник имеет удаленный доступ к смартфону «жертвы».

По данным Statcounter Global на июнь 2019 года доля смартфонов под управлением операционной системы Android на мировом рынке составляет 76.03%, под управлением iOS – 22.04%, на другие операционные системы приходится 1.93%. (рис. 1) [3].

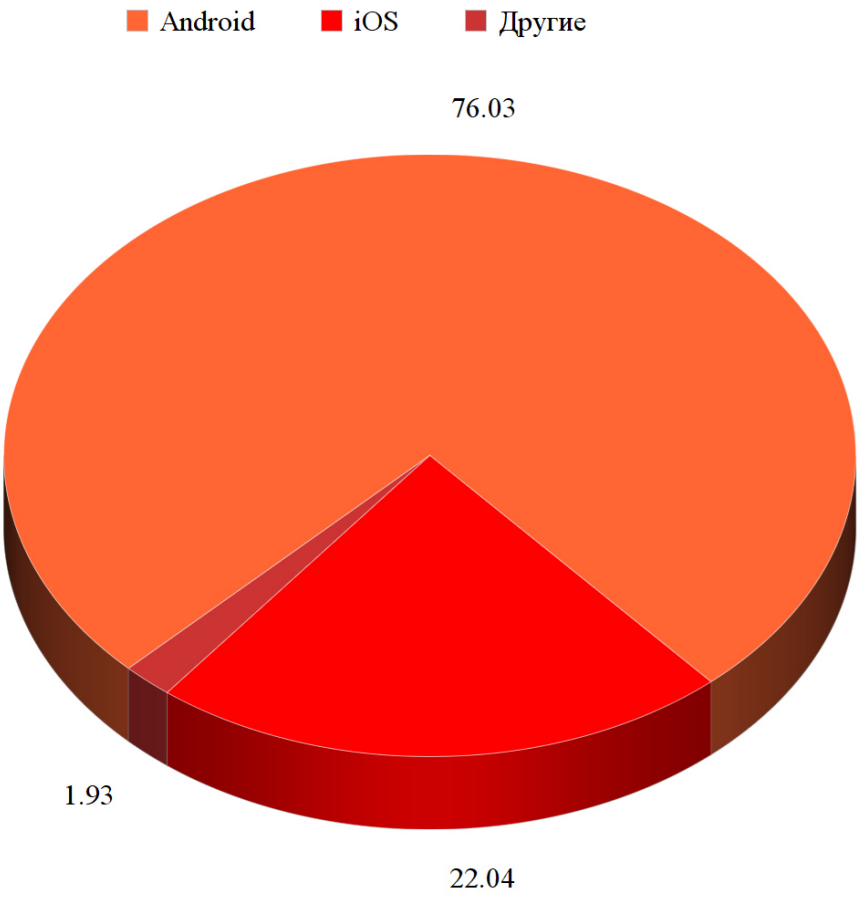

Рис. 1. Доля смартфонов на мировом рынке
Fig. 1. Share of smartphones in the global market

При этом Android смартфоны являются более уязвимыми из-за своей популярности, а также открытости исходного кода системы. У злоумышленников имеется больше возможностей для создания вирусов из-за доступности системы для подробного исследования и выявления

уязвимостей. Так же возможностей распространения «зараженных» приложений больше, чем в iOS смартфонах.

Помимо официального магазина приложений Play Маркет, приложения могут распространяться на сторонних интернет ресурсах в виде APK-файлов. APK (англ. Android Package) – формат архивных исполняемых файлов-приложений для Android. Стоит уточнить, что скачивания приложений из Play Маркета тоже происходит с помощью APK-файлов, только после установки файл автоматически удаляется. Аналогично с компьютерными вирусами, зловредный код вшивается в APK-файл и начинает работу после установки. Существует множество способов создания приложений с замаскированным вирусом удаленного доступа (RAT) и возможности этих приложений так же разнятся. RAT – аббревиатура англ. Remote Access Trojan, в переводе – «Троян удаленного доступа» или «средство удалённого управления». Популярными программы для создания RAT из общедоступных являются: SpyNote, SpyMax, DroidJack, AhMyth, AndroRat [4]. Эти программы уже появились в открытом доступе и каждый желающий может ими воспользоваться. Размещение программ в открытом доступе обусловлено тем, что они уже были замечены крупными компаниями, занимающимися безопасностью, и были созданы какие-либо решения по выявлению этих RAT на устройствах. Соответственно злоумышленник потерял возможность продавать данный софт, но тем не менее множество устройств подвержены воздействию данных вирусов из-за старых версий операционной системы или ошибок пользователя. У программ по созданию RAT могут быть такие 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 [5].

Эти возможности предназначены для лучшей маскировки вирусов. К примеру, вирусы «вшитые» в уже известные приложения подавляют бдительность неопытного пользователя, и он подсознательно уверен, что с хорошо ему известным приложением все в порядке. Вирусы с невидимыми иконками предназначены для скрытия самого факта установки вируса.

Зараженные таким образом приложения могут иметь такие возможности:

- полная информация о телефоне (модель, версия ОС, IMEI, MAC-адрес);
- читать и писать смс сообщения;
- доступ к памяти телефона (просмотр, удаление, модификация, отправление на сервер злоумышленнику);
- доступ к контактам, возможность совершать и прослушивать звонки;
- запись звука с микрофона;
- кейлогер (считывание нажатых клавиш, предназначенный для кражи паролей);
- устанавливать новые приложения на смартфон;
- скрытый доступ к камерам смартфона;
- отправление скриншотов с экрана злоумышленнику;
- получить местонахождение через GPS;
- другие возможности, по желанию злоумышленника [6].

Имея такой функционал, злоумышленник может нанести большой ущерб «жертве». При этом создать такой вирус может любой пользователь, ведь для этого не требуются навыки написания вирусов.

Разберем алгоритм создания RAT с помощью AhMyth. После запуска программы открывается вкладка APK Bilder (рис. 2), где и будет происходить создание APK-файла.

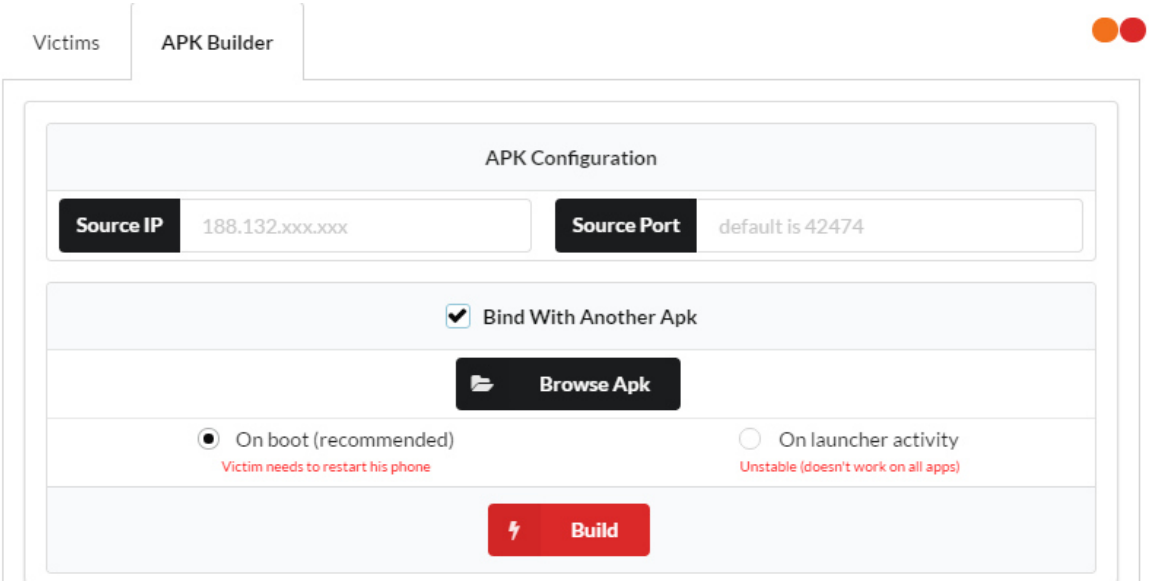

Рис. 2. Вкладка APK Bilder
Fig. 2. APK Builder Tab

В поле Source IP указывается IP адрес, с которого будет происходить управление устройством. В поле Source Port указывается номер свободного порта на устройстве злоумышленника. Перед этим действием может понадобиться предварительное открытие портов. В меню Bind With Another Apk имеется возможность выбрать вшить вирус в другое приложение или создать собственное приложение. Собственное приложение, созданное программой, будет иметь стандартную иконку приложения андроид и после установки не появится на рабочих столах устройства. Далее необходимо выбрать момент активации вируса: после перезагрузки устройства или сразу же после установки. Рекомендуется выбирать активацию после перезагрузки, в ином случае могут быть проблемы с получением отклика от приложения. После выполнения всех вышеперечисленных пунктов запускаем Build для создания APK. При успешном создании APK размещается в корневой папке AhMyth и злоумышленнику остается только каким-либо образом вынудить «жертву» установить его.

После того как приложение каким-либо образом было установлено на телефон «жертвы» и телефон был перезагружен (если на момент создания была выбрана активация после перезагрузки) злоумышленник переходит во вкладку Victims (рис. 3).

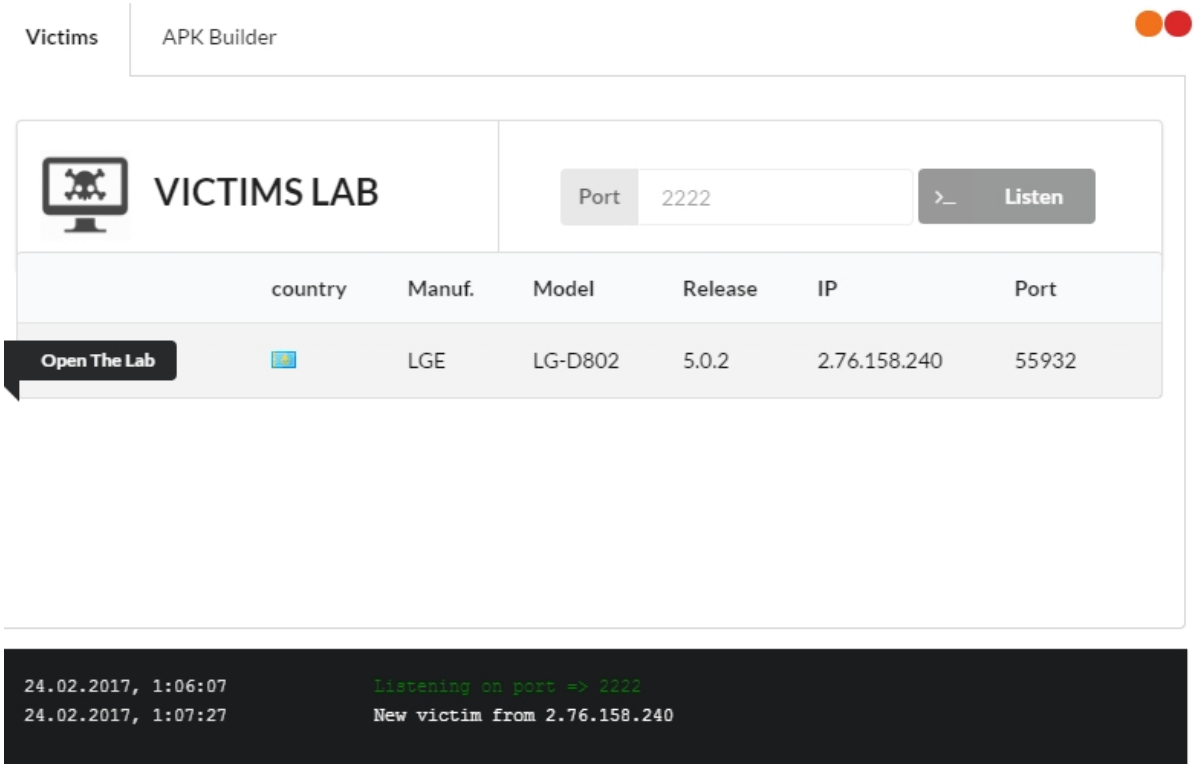

Рис. 3. Вкладка
Fig. 3. Victims

В этой вкладке указывается порт, который был выбран при создании APK, и нажимается Listen. Через какое-то время появляется «жертва», при условии, что телефон подключен к интернету. После установления соединения с «жертвой» появляется меню (рис. 4) для дальнейших манипуляций.

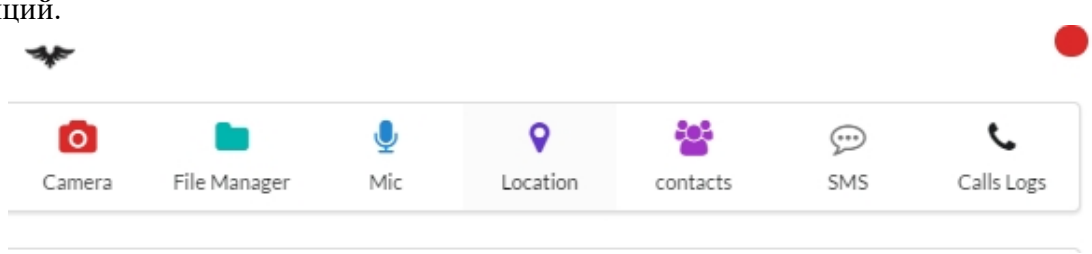

Рис. 4. Функционал программы
Fig. 4. The functionality of the program

«Жертва» скачивает зараженный файл и начинает установку. Перед началом установки всплывает обычное окно (рис. 5), где указаны необходимые приложению разрешения.

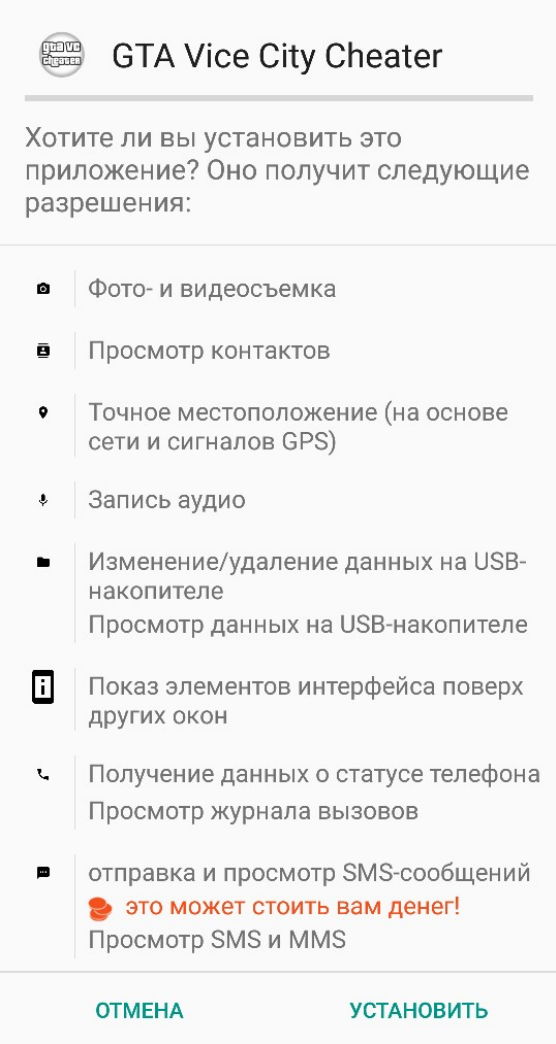

Рис. 5. Окно установки программы
Fig. 5. Program installation window

Список разрешений – один из вариантов определения вшитого в приложение вируса. Но об этом речь пойдет в способах защиты от таких вирусов. Другие программы по созданию RAT работают почти так же, с небольшими индивидуальными отличиями. [6]

ЗАКЛЮЧЕНИЕ

Таким образом видно, что создание подобных вирусов не требует каких-то профессиональных знаний и умений. Любой желающий сможет с легкостью создать и распространить зараженное приложение. Самый популярный способы распространения таких вирусов – это сайты с пиратскими приложениями. Под видом какого-нибудь платного приложения, которое предлагают скачать бесплатно, или приложения, у которого еще не было релиза, злоумышленник выставляет вирус. Реже зараженные приложения могут распространяться с помощью Play Маркета, т.к. приложения перед выпуском в продажу на площадке, проходят обязательную проверку Google Play App Security Improvement [7]. Эта проверка способна выявить RAT, описанные выше и подобные им, поскольку они уже известны. Но более продвинутые вирусы могут пройти проверку и быть допущены для размещения на площадке Play Маркета. Такие вирусы более опасные, поскольку их создают профессионалы и сами вирусы могут оставаться на устройстве после удаления зараженного приложения. А для пользователя такие приложения автоматически кажутся безопасными, ведь они скачаны из официального магазина. Но в данной статье рассматриваются более слабые вирусы. Как уже говорилось раннее андроид является слабо защищенной системой, до пятой версии системы разработчики уделяли этому мало

внимания. И тем не менее приложения, созданные с помощью AhMyth, не были помечены опасными всеми версиями ОС до седьмого. По данным на 2018 год пользователей андроид младше 7-ой версии – 70.4%, а старше всего 29.6%. 2/3 всех пользователей андроид не защищены от установки зараженных приложений [8].

Отсюда можно сделать вывод и выделить некоторые рекомендации для повышения защищенности своих данных:

1. Оперативно обновлять версию операционной системы или прошивки телефона до последней. Почти во всех, даже мелких, обновлениях проводится работа над повышением безопасности.

2. Избегать скачивания из неизвестных источников, а тем более из СМС рассылок. При необходимости скачать приложения из неизвестных источников стоит проявлять особую бдительность. Перед установкой приложения необходимо проанализировать запрашиваемые разрешения. Например, необходимо скачать ридер для книг, а в разрешениях требуется доступ к файлам, телефонной книге и камере. Доступ к файлам необходим для получения доступа к сохраненным на устройстве книгам. Но доступ к телефонной книге и камере ридеру совсем ни к чему. Ненужные для функционала приложения разрешения сразу должны насторожить и стоит отказаться от их установки [9].

3. Установка антивируса. Многие пользователи полагают, что не существует вирусов на андроид, поэтому пренебрегают антивирусом. Но это далеко не так, каждый год обнаруживается десятки тысяч новых мобильных вирусов. И абсолютное большинство из них на андроид. Для обнаружения таких слабых вирусов, как созданный с помощью AhMyth, достаточного самого простого бесплатного антивируса.

4. Регулярное обновление антивируса. По мере выявления в антивирусную базу добавляются новые зловредные программы. Если была скачана программа с еще не известным вирусом, которая смогла пройти проверку Play Маркета, то антивирус сразу проинформирует пользователя, как только будет создан алгоритм определения и удаления вируса. Таким образом, пользователь быстрее сможет избавиться от зараженной программы и избежать лишнего ущерба [10].

Список литературы

1. Development of power converter system for mobile systems, URL: http://nice.kaist.ac.kr/index.php?mid=Research03_2 (дата обращения 05.08.2019)

2. Tadviser. Смартфоны (рынок России), URL: http://www.tadviser.ru/index.php/Статья:Смартфоны_(рынок_России)#.2A_Inventive_Retail_Group (дата обращения 05.08.2019)

3. Statcounter Global. Mobile Operating System Market Share Worldwide, URL: https://gs.statcounter.com/os-market-share/mobile/worldwide (дата обращения 05.08.2019)

4. Codeby. Android RAT. URL: https://codeby.net/threads/android-rat.60456/ (дата обращения 05.08.2019)

5. Spy-soft. Что такое RAT? Всё про шпионские RAT-трояны, URL: http://www.spy-soft.net/chto-takoe-rat/ (дата обращения 05.08.2019)

6. Dedicatet RAT вирус, URL: https://yandex.ru/turbo?text=https%3A%2F%2Fdedicatet.com%2Fthreads%2Frat-virus.918%2F (дата обращения 05.08.2019)

7. Github. AhMyth-Android-RAT, URL: https://github.com/AhMyth/AhMyth-Android-RAT (дата обращения 05.08.2019)

8. Xda-developers. Google’s App Security Improvement Program has helped catch vulnerabilities in over 1,000,000 apps https://www.xda-developers.com/google-application-security-improvement-program-recap/ (дата обращения 05.08.2019)

9. Itsecforu. Трояны удаленного доступа (RAT) – что это такое и как защитить от них, URL: https://itsecforu.ru (дата обращения 05.08.2019)

10. Kumaser. Защита от скрытого удалённого доступа, URL: https://www.kumaser.com/ns25.html (дата обращения 05.08.2019)

References

1. Development of power converter system for mobile systems, URL: http://nice.kaist.ac.kr/index.php?mid=Research03_2 (accessed 05.08.2019)
2. Tadviser. Smartphones (Russian market), URL: http://www.tadviser.ru/index.php/Статья:Смартфоны_(market_russia)#. 2A_Inventive_Retail_Group (accessed 05.08.2019)
3. Statcounter Global. Mobile Operating System Market Share Worldwide, URL: https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed 05.08.2019)
4. Codeby. Android RAT. URL: https://codeby.net/threads/android-rat.60456/ (accessed 05.08.2019)
5. Spy-soft. What is a RAT? All about spyware RAT Trojans, URL: http://www.spy-soft.net/chto-takoe-rat/ (accessed 05.08.2019)
6. Dedicatet RAT virus, URL: https://yandex.ru/turbo?text=https%3A%2F%2Fdedicatet.com%2Fthreads%2Frat-virus.918%2F (accessed 05.08.2019)
7. Github. AhMyth-Android-RAT, URL: https://github.com/AhMyth/AhMyth-Android-RAT (accessed 05.08.2019)
8. Xda-developers. Google's App Security Improvement Program has helped catch vulnerabilities in over 1,000,000 apps https://www.xda-developers.com/google-application-security-improvement-program-recap/ (accessed 05.08.2019)
9. Itsecforu. Remote access Trojans (RAT) – what they are and how to protect them, URL: https://itsecforu.ru (accessed 05.08.2019)
10. Kumaser. Protection from hidden remote access, URL: https://www.kumaser.com/ns25.html (accessed 05.08.2019)

Какаев Денис Валерьевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Kakaev Denis Valerievich, 4th year student of the Department Information security, Institute of Radioelectronics and information security
Maslova Maria Aleksandrovna, postgraduate student, senior lecturer of the Department Information security, Institute of Radioelectronics and information security