Для цитирования: Баркалов Ю.М., Нестеров А.Д. Особенности обеспечения информационной безопасности в мобильных устройствах под управлением операционной системы Android. Вестник Дагестанского государственного технического университета. Технические науки. 2019; 46 (2): 71-80. DOI:10.21822/2073-6185-2019-46-2-71-80.

For citation: Barkalov Yu.M., Nesterov A.D. Peculiarities of information security in mobile devices running the Android operating system. Herald of Daghestan State Technical University. Technical Sciences. 2019; 46 (2): 71-80. (In Russ.) DOI:10.21822/2073-6185-2019-46-2-71-80

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 621.3

DOI:10.21822/2073-6185-2019-46-2-71-80

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ УСТРОЙСТВАХ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

Баркалов Ю.М.², Нестеров А.Д.¹

¹⁻²Воронежский институт Министерства внутренних дел Российской Федерации,
¹⁻²394065, г. Воронеж, пр. Патриотов, 53, Россия,

¹e-mail: nevvostok@gmail.com, ²email: ekcvor@mail.ru

Резюме. Цель. В статье приведена формальная модель обеспечения информационной безопасности в мобильных устройствах под управлением операционной системы Android, а также рассмотрен статический и динамический анализ вредоносного программного обеспечения. **Метод.** Для обеспечения защиты конфиденциальной информации в мобильных устройствах можно одновременно использовать программные обеспечения, а также организационные мероприятия. **Результат.** Предложенная формальная модель обеспечения информационной безопасности и анализ предположительно вредоносного программного обеспечения позволят обеспечить безопасность информации в мобильных устройствах, а также снизить риск реализации угроз до приемлемого уровня при минимальной стоимости системы защиты. Представленный алгоритм работы приложения, предназначенного для незаконного перевода денежных средств, а также пример анализа данного приложения позволят специалисту повысить качество выполнения своих профессиональных задач при разборе инцидентов в сфере информационной безопасности. **Вывод.** В связи с тем, что на сегодняшний день отсутствует научно-обоснованная методика выявления и анализа вредоносного программного обеспечения в памяти мобильных устройств, сведения, приведенные в данной статье, будут способствовать повышению эффективности защиты информации в мобильных устройствах под управлением операционной системы Android.

Ключевые слова: информационная безопасность, мобильные устройства, Android

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

PECULIARITIES OF INFORMATION SECURITY IN MOBILE DEVICES RUNNING THE ANDROID OPERATING SYSTEM

Yuri M. Barkalov², **Anton D. Nesterov**¹

¹⁻²Voronezh Institute of the Ministry of the Interior of the Russian Federation,

¹⁻²53 Patriotov Str., Voronezh 394065, Russia,

¹e-mail: nevvostok@gmail.com, ²email: ekevov@mail.ru

Abstract. Objectives The article presents a formal model of information security in mobile devices running the Android operating system, an example of detection and investigation of malicious software, as well as static and dynamic analysis of malicious software. **Method** To protect sensitive information on mobile devices, you can use software and organizational measures at the same time. **Result** The proposed formal model of information security and analysis of suspected malicious software will ensure the security of information in mobile devices, as well as reduce the risk of threats to an acceptable level at a minimum cost of the protection system. The presented algorithm of the application designed for illegal transfer of funds, as well as an example of the analysis of this application will allow the specialist to improve the quality of their professional tasks in the analysis of incidents in the field of information security. **Conclusion** Due to the fact that today there is no scientifically based method of detection and analysis of malicious software in the memory of mobile devices, the information provided in this article will help to improve the efficiency of information protection in mobile devices running the Android operating system.

Keywords: information security, mobile devices, Android

Введение. На сегодняшний день для получения конфиденциальной информации, хранящейся в памяти мобильных устройств, а также с целью денежного обогащения, злоумышленники стали разрабатывать вредоносные программные обеспечения для мобильных устройств под управлением операционной системы Android, которые позволяют осуществить несанкционированный доступ к информации, хранящейся в памяти мобильного устройства [1,2].

Актуальной задачей является обеспечение информационной безопасности в мобильных устройствах под управлением операционной системы Android. Одним из основных требований к обеспечению безопасности является использование современных методов защиты информации с возможностью адаптации к возникающим вызовам и угрозам информационной безопасности [3,15], а также своевременное выявление угроз «нулевого дня».

В то же время, для снижения стоимости системы защиты и ее влияния на производительность системы, необходимо искать незадействованные ресурсы информационной системы и направлять их на решение задач обеспечения безопасности [4,5].

Постановка задачи. Предлагаемая формальная модель обеспечения безопасности, а также проведение анализа предположительно вредоносного программного обеспечения, позволят обеспечить безопасность информации в мобильных устройствах, а также позволят добиться снижения риска реализации угроз до приемлемого уровня при минимальной стоимости системы защиты.

Методы исследования. Для обеспечения защиты конфиденциальной информации в мобильных устройствах возможно использовать программные и одновременно организационные мероприятия [6]. Ниже приведена формальная модель обеспечения безопасности информации в мобильных устройствах.

Для решения поставленной задачи введем следующие обозначения:

$A = \{a_1, \dots, a_m\}$ – множество всех возможных программных средств, обеспечивающих защиту информации;

$B = \{b_1, \dots, b_n\}$ – множество всех возможных организационных мероприятий по защите информации;

$x_i = \begin{cases} 1, & \text{если используется } i - e \text{ программное обеспечение;} \\ 0, & \text{иначе.} \end{cases}$

$y_i = \begin{cases} 1, & \text{если применяется } i - e \text{ организационное мероприятие;} \\ 0, & \text{иначе.} \end{cases}$

W – возможное количество одновременно используемых программных средств;

Q – возможное количество одновременно применяемых организационных мероприятий;

c_{ij} – стоимость применяемых программных средств i -го типа и j -го организационного мероприятия;

C – максимально возможные затраты;

p_{ij} – коэффициент надежности при использовании программного обеспечения i -го типа и j -го организационного мероприятия.

Количество всех возможных действий по защите информации с использованием мобильных устройств представляет декартово произведение $N \subset A \times B$.

Следовательно, задача оптимизации обеспечения защиты информации решается в условиях следующих ограничений:

– на количество программных средств i -го типа

$$\sum_{i=1}^k x_i \leq W, k \in Z^+;$$

– на количество организационных мероприятий i -го типа

$$\sum_{i=1}^k y_i \leq Q, k \in Z^+;$$

– на затраты по защите информации

$$\sum_{i=1}^s \sum_{j=1}^d c_{ij} \cdot (x(a_i) + y(b_j)) \leq C;$$

– на значение переменных

$x_i \in \{0, 1\}, y_i \in \{0, 1\}, i, j = 1, 2, \dots$

Задача нахождения оптимального набора действий по защите информации принимает следующий вид:

найти

$$C^* = Arg \max_{i,j} P_{ij}, \text{ где } P_{ij} = p_{ij}(\{A\}, \{B\}).$$

Для обеспечения информационной безопасности следует также проводить анализ приложений в памяти мобильного устройства [7,9]. Существует два типа анализа предположительно вредоносных программ: динамический и статический.

В рамках динамического анализа предположительно вредоносной программы анализируются особенности ее поведения, в частности её взаимодействие с операционной системой.

Для проведения динамического анализа используются программные продукты, позволяющие собрать информацию о программе и ее деятельности в системе:

- хеш-сумма APK-файла (алгоритмы MD5, SHA-1 и SHA-256);
- сведения о полученных и отправленных по сети данных;
- сведения об операциях чтения и записи файлов;

- сведения о запущенных службах и загруженных классах;
- сведения о сборе и отправке пользовательских данных;
- сведения о разрешениях, которые получило приложение;
- сведения об отправляемых SMS-сообщениях и осуществляемых вызовах.

В рамках статического анализа предположительно вредоносной программы производится анализ ее кода. Главной задачей рассматриваемого типа анализа является выделение части кода, ответственной за предположительно вредоносные действия исследуемой программы.

Существует два наиболее распространенных способа проведения статического анализа, а именно с использованием программного обеспечения ArkTool, которое позволяет произвести дизассемблирование предположительно вредоносной программы, а также с помощью программного продукта JD-GUI, для анализа исходного кода. По результатам проведения динамического и статического анализа специалист может сделать вывод, является ли исследуемая программа вредоносной [10,11].

В качестве примера рассмотрим вредоносное программное обеспечение, предназначенное для несанкционированной отправки СМС - сообщений на короткие номера.

Использование вредоносных приложений, способных незаметно для владельцев мобильных устройств на платформе Android отправлять СМС - сообщения на короткие номера, уже длительное время является одним из главных способов обогащения для злоумышленников [12,13]. С ростом популярности дистанционного банковского обслуживания злоумышленники стали применять более продвинутые вирусы.

Алгоритм работы приложения, предназначенного для незаконного перевода денежных средств представлен на рис.1.

Умение правильно получить информацию из памяти мобильного устройства требует от специалиста глубоких знаний и компетентности, а также основательной подготовки. Для получения и исследования приложения, расположенного в памяти мобильного устройства, необходимо снять дампы памяти и выполнить декомпиляцию интересующего приложения [8,14].

Для исследования вредоносного кода в APK приложениях необходимо выполнить декомпиляцию приложения, то есть извлечь все данные, которые находятся в APK.

Приложение работает в изолированной среде и имеет в своей структуре собственные разрешения и область рабочей памяти. Различные приложения могут взаимодействовать между собой, а также запрашивать систему для выделения ресурсов через предписания.

Все приложения для Android компилируются в файл AndroidPackage и устанавливаются на мобильное устройство.

Файл APK является вариантом формата JAR и в основном содержит две папки META-INF и RES со следующими файлами: AndroidManifest.xml, classes.dex и resources.arsc. AndroidManifest.xml содержит основную информацию о приложении и включает в себя список библиотек, необходимых для работы программы, указывает необходимые разрешения, а также выполняет следующие задачи:

- задает имя пакета Java для приложения. Данное имя пакета служит уникальным идентификатором приложения;
- описывает компоненты приложения — операции, службы, приемники широковестьных сообщений и поставщиков контента, из которых состоит приложение. AndroidManifest.xml содержит имена классов, которые реализуют каждый компонент, и публикует их возможности.

Рис. 1. Алгоритм приложения для незаконного перевода денежных средств

Fig. 1. The algorithm of the application for illegal money transfers

На основании этих деклараций операционная система определяет, из каких компонентов состоит приложение и при каких условиях их можно запускать;

– определяет, в каких процессах будут размещаться компоненты приложения;

- объявляет, какие разрешения должны быть выданы приложению, для получения доступа к защищенным частям API-интерфейса, а также для взаимодействия с другими приложениями;
- объявляет минимальный уровень API-интерфейса Android, который требуется приложению.
- содержит список библиотек, с которыми должно быть связано приложение.

Classes.dex содержит код всего приложения для Dalvik. Dalvik это регистровая виртуальная машина для выполнения программ, написанных на языке программирования Java, которая входит в операционную систему Android.

Обсуждение результатов. В качестве разбора вредоносного кода в приложении рассмотрим приложение, которое осуществляло несанкционированную отправку СМС - сообщений. По результатам анализа приложений, имеющихся на мобильном устройстве, выявлено приложение «SMSSender».

Первым шагом стала декомпиляция приложения, которая позволила получить необходимый для исследования код.

Дальнейшее исследование файла, а именно определение содержащихся в нем данных или команд, осуществлялось при помощи «AndroidStudio» - интегрированной средой разработки для работы с платформой Android.

Проанализировав файл «AndroidManifest.xml», который содержит запросы для получения различных функций и прав на мобильном устройстве, обнаружена функция «SMS_SEND», которая позволяет приложению осуществлять отправку SMS-сообщений.

Далее исследовался метод «onCreate», который содержится в классе приложения «Activation». Данный метод содержит следующий код:

```
new-instance v0, Lcl/catsboat/c;  
invoke-direct {v0, p0}, Lcl/catsboat/c;-><init>(Lcl/catsboat/Main;)V  
invoke-virtual {v0}, Lcl/catsboat/c;->
```

Анализ кода показывает, что после запуска приложения дополнительно открывается еще одно активное окно, которое не отображается на экране мобильного устройства.

Стоит обратить внимание на класс «cl/catsboat/c», который содержит следующий код:

```
invoke-direct {v1, v2, v3}, Lcl/catsboat/a;-  
><init>(Landroid/content/Context;Landroid/os/Handler;)V
```

Данная строка кода содержит обращение к классу «a.smali». Конструкция данного класса содержит следующий код:

```
const-string v1, "image.png"  
invoke-virtual {v0, v1}, Landroid/content/res/AssetManager;-  
>open(Ljava/lang/String;)Ljava/io/InputStream;  
move-result-object v0  
const-wide/16 v2, 0x3486  
invoke-virtual {v0, v2, v3}, Ljava/io/InputStream;->skip(J)J  
new-instance v1, Ljava/io/DataInputStream;
```

```
invoke-direct {v1, v0}, Ljava/io/DataInputStream;-><init>(Ljava/io/InputStream;)V
```

Данный блок кода создает объект, представляющий собой поток байтов для чтения из файла «image.png», находящегося в каталоге «Assets» приложения «SMSSender». Далее блок пропускает первые 13446 байт и создает на основе него поток для чтения Java данных. Логично предположить, что в файле «image.png» имеется зашифрованный код, к которому обращается приложение после запуска.

Для получения зашифрованного кода в файле «image.png» необходимо воспользоваться шестнадцатеричным редактором «WinHex» и выполнить следующие действия:

В редакторе «WinHex» выбрать изображение «image.png», которое находится в каталоге «\SMSSender\assets». Так как графическое изображение «image.png» имеет формат png, то его байт-код всегда заканчивается как 44 4E 44 AE 42 60 82 (END@B',).

Переход к байт - коду (END@B',) показывает окончание файла. Однако в исследуемом графическом изображении image после него имеется дополнительный код, представленный на рис. 2.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000033F0	20	2C	17	A3	AF	CF	C4	B6	BC	0F	F9	10	72	26	06	CC	, 4-TAT4 u r4 i
00003400	59	F4	FF	58	5A	C7	FF	90	1A	24	80	48	41	D7	C7	80	Y0yXZCqY S*HA>CE
00003410	A5	65	8D	3E	21	40	53	00	10	40	03	1D	81	0C	58	72	We >!8S 8 Xr
00003420	22	F2	6A	67	E4	D9	6E	E4	40	43	0F	6C	64	8C	6D	65	"0jq8Un8@C l0dme
00003430	D8	7F	B4	00	C5	35	89	8C	EF	82	0E	46	34	9A	01	4B	0 - A5u8i, F48 K
00003440	F7	E0	3F	11	E6	50	15	00	04	D0	60	88	40	74	CF	FF	+a? eP B`@tiy
00003450	45	CA	5D	8C	0C	B8	97	29	A0	E7	1A	62	02	8C	92	80	E8]E .-) q b G'e
00003460	1D	94	3B	90	01	02	88	11	72	5B	E8	28	18	AA	00	20	"; - rfe(a
00003470	C0	00	E6	A5	34	7D	A3	3A	16	51	00	00	00	00	49	45	A eY4): Q IE
00003480	4E	44	AE	42	60	82	63	6F	74	6A	74	73	28	3D	43	7C	ND8B',cotjts(=C
00003490	4A	21	63	66	2A	66	69	69	7C	39	43	6C	16	0D	65	6C	U!cf*fi1 9Cl el
000034A0	70	60	7E	73	33	56	44	75	48	21	78	76	24	64	68	63	p'~s3VDuH!xv\$dhc
000034B0	7A	33	44	7C	16	3A	6F	6E	61	75	6E	68	66	25	03	4B	z3D :onaunhf% K
000034C0	55	3D	47	63	6A	64	61	62	7A	67	27	71	55	3E	65	70	U=Gcjdabzq'qU>ep
000034D0	70	25	67	69	6C	2E	42	71	5C	60	7D	6B	60	62	63	73	p%q11.Bq\`)'k'bc8
000034E0	26	08	42	79	4B	3A	31	08	57	68	75	4A	69	32	4C	7F	& ByK:l WhuJ12L
000034F0	5D	3C	2A	6F	24	38	26	54	65	2F	60	79	56	2F	6D	67	l<*oS84Te`y'v/mg
00003500	76	2B	61	62	7C	18	48	7E	59	3B	66	76	2C	2C	3D	0D	v+abl H-Y'fv,=
00003510	65	72	5E	7D	56	2A	5E	67	7C	71	4B	62	7B	2F	4C	7F	er^V*^g qKb{/L
00003520	5D	66	28	33	35	34	37	31	3D	6F	19	3A	14	6E	28	33	lf(35471=0 : n(3
00003530	35	34	24	2B	28	7E	EF	B9	70	21	66	63	25	27	2A	27	54S+(-1'p:fc%'*
00003540	66	29	41	74	14	6E	64	77	68	69	2F	3C	02	2E	0D	25	f)At ndwhi/< . %
00003550	18	20	6F	75	24	57	73	69	66	3D	4F	74	5D	66	23	22	ou\$Welf=Ot]f#"
00003560	7F	0F	26	75	7D	32	05	31	18	35	00	22	24	25	26	53	6u)2 1 S "S%6S
00003570	67	3D	5E	6C	16	23	6B	69	61	51	63	7F	7C	74	4E	6C	g=^l #kiaQc ltnl
00003580	40	62	2A	20	C6	A4	4E	66	7B	28	4C	38	54	2F	2A	74	@b* E8Pfl(L8T/*t
00003590	6D	76	72	66	29	7E	01	4C	57	2F	79	76	2A	49	43	49	mvrfl~ LW/yv*ICI
000035A0	4F	08	65	47	74	01	44	45	2D	2B	75	6F	67	2B	05	31	O eGt DE~+uog+ 1
000035B0	03	44	2A	7F	0E	78	3D	0D	02	34	03	68	57	3D	7E	2A	D* x= 4 hW=~*
000035C0	76	2C	3D														v, 4

Рис. 2. Дополнительный код

Fig. 2. Additional code

Скопировав данный блок кода в отдельный файл, и присвоив ему имя «malware», переходим к его расшифровке. Для расшифровки байт-кода используется нижеприведенный код, который читает первые 317 байтов, по одному байту из файла «malware». Каждый из байтов выполняет сложение по модулю 2 (XOR) поочередно с байтом из буфера «key» и сохраняет их в буфер «buf».

```
import java.io.*;

public class test
{
    public static void main(String[] args)
    {
        byte [] key = {10,2,4,5,6,7,8,92,45,24,56,78};
        int kPos = 0;
        char[] buf = new char[317];
        try
        {
            InputStream is = new FileInputStream(new File("c:\night"));
            for(int i = 0;i<buf.length;i++) {
                if(is.available() == 0) break;
                buf[i] = (char)(is.read() ^ key[kPos]);
                kPos = (kPos == key.length - 1) ? 0 : (kPos + 1);
            }
            System.out.println(buf);
        }
        catch(Exception ex){}
    }
}
```

Создав файл «test», с приведенным выше кодом в каталоге «*\Java\jdk1.7.0_79\bin» с расширением java, необходимо в командной строке выполнить следующую команду: «cd *\Java\jdk1.7.0_79\bin». Далее выполняем следующую команду: «javac test.java». После этого в каталоге «bin» создается файл «test.class». Для расшифровки байт-кода, находящегося в файле «malware», воспользуемся командой: «java -classpath .test».

Далее в консоли отобразится расшифрованный код:

```
import android.content.Context;
import android.telephony.SmsManager
import android.widget.Toast
SmsManager m = SmsManager.getDefault();
m.sendMessage("900", "null", "Перевод 89001230000", null, null);
r = new Runnable() {
    run() {
        Toast.makeText(ctx, "??Hasta la vista!", Toast.LENGTH_LONG).show();
    }
}
h.post(r);
```

По результатам анализа кода было установлено, что приложение отправляет SMS-сообщения на абонентский номер «900» с текстом «89001230000».

Данное приложение может быть использовано злоумышленниками для хищения денежных средств с мобильных устройств и банковских карт. В связи с этим, стоит отметить, что необходимо исследовать все вложения, являющиеся продолжением головного кода приложения.

Вывод. Предложено использовать формальную модель, позволяющую находить оптимальный набор действий по защите информации с целью обеспечения информационной безопасности в мобильных устройствах под управлением операционной системы Android, а также проводить анализ приложений для выявления вредоносного программного обеспечения.

Исследование вредоносного программного обеспечения, предназначенного для незаконного перевода денежных средств, является актуальной задачей современной криминалистики. При этом следует учитывать отсутствие научно обоснованных методик решения данных криминалистических задач.

На сегодняшний день существуют несколько проблем в защите ОС Android. Отсутствует самозащита операционной системы Android, система должна защищаться от воздействий ещё неизвестных вредоносных приложений. Кроме перехвата вредоносного приложения необходимо распознать вирус в упакованном, зашифрованном или обфусцированном виде. Необходимо противодействовать неизвестным вредоносным приложениям, которые созданы злоумышленниками, с учетом знаний об антивирусных программах, а также получать обновление баз данных антивирусных программ для активного противодействия вредоносным приложениям.

Современные методы выявления вредоносного программного обеспечения не гарантируют надежной защиты. Сведения, приведенные в данной работе, позволят повысить качество выполнения специалистами своих профессиональных задач при разборе инцидентов в сфере информационной безопасности, связанных с незаконным переводом денежных средств, с использованием устройств под управлением операционной системы Android.

Библиографический список:

1. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. – взамен ГОСТ Р 50922-96; введ. 01.02.2008 // СПС «Консультант-Плюс». – Режим доступа: <http://www.consultant.ru>.
2. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Введ. 2009-10-01.
3. Доктрина информационной безопасности Российской Федерации : утв. Президентом Российской Федерации №646 от 06.12.2016 // СПС «Консультант Плюс». Режим доступа: <http://www.consultant.ru>.
4. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. Москва : Издательство Юрайт, 2017. 321 с. (Университеты России). ISBN 978-5-534-00258-4. Текст : электронный // ЭБС Юрайт [сайт]. URL: <https://www.biblio-online.ru/bcode/398687> (дата обращения: 15.06.2019).
5. Бирюков А.А. Информационная безопасность. Защита и нападение. 2-е издание. М.: ДМК-Пресс, 2017.
6. Нестеров А.Д., Баркалов Ю.М. Выявление угроз информационной безопасности в мобильных операционных системах // Всероссийская научно-практическая конференция. Актуальные вопросы эксплуатации

систем охраны и защищенных телекоммуникационных систем. - Воронеж: Воронежский институт МВД России, 2016. С. 17-19.

7. Кичук Д.Я., Бурдинский И.А. Особенности исследования информации в мобильных устройствах под управлением ОС Android по преступлениям в сфере дистанционного банковского обслуживания // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. Воронеж: Воронежский институт МВД, 2018. С. 123-124.

8. Нестеров А.Д., Баркалов Ю.М. Организационно-правовое обеспечение получения информации из мобильных устройств и облачных хранилищ при расследовании инцидентов в сфере информационной безопасности // Международная научно-практическая конференция. Преступность в СНГ: Проблемы предупреждения и раскрытия преступлений. - Воронеж: Воронежский институт МВД России, 2015. - С. 34-36.

9. Анализ угроз информационной безопасности современных мобильных систем / Жернаков С. В., Гаврилов Г. Н. // Интеграционные процессы науки XXI века: сборник статей Международной научно-практической конференции. Стерлитамак: РИЦ АМИ, 2015. С. 54 - 60.

10. Детектирование вредоносного программного обеспечения в мобильной операционной системе на базе Android на основе разрешений с применением метода опорных векторов / Жернаков С. В., Гаврилов Г. Н. // Научно периодическое издание Ceteris Paribus: Европейский фонд инновационного развития. Ежемес. науч. журнал «Ceteris Paribus», 2015.С. 10 -14.

11. Мастхэв для мобильной аналитики. Что нужно, чтобы вскрывать приложения для Android на Android // Хакер URL: <https://xakep.ru/2019/03/12/mobile-analytics-must-have/> (дата обращения: 15.06.2019).

12. Уязвимость в Android позволяет перехватывать конфиденциальные данные // Хакер URL: <https://xakep.ru/2018/09/03/wifi-broadcasts-leak/> (дата обращения: 15.06.2019).

13. Баркалов Ю.М. Методика расследования преступлений в сфере дистанционного банковского обслуживания // Общественная безопасность, законность и правопорядок в III тысячелетии. Воронеж: Воронежский институт МВД России, 2015. С. 172-176.

14. Баркалов Ю.М. Проведение экспертизы программного обеспечения мобильных устройств под управлением ОС "Андроид" // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронеж: Воронежский институт МВД России, 2016. С. 137-142.

15. Баркалов Ю.М., Перминов Г.В. Выявление НСД к мобильным устройствам, используемым в ИСОД МВД России // Охрана, безопасность, связь. Воронеж: Воронежский институт МВД России, 2017. С. 32-36.

References:

1. Zashchita informatsii. Osnovnyye terminy i opredeleniya: GOST R 50922-2006. – vzamen GOST R 50922-96; vved. 01.02.2008 // SPS «Konsul'tant-Plyus». – Rezhim dostupa: <http://www.consultant.ru>. [Information protection. Basic terms and definitions: GOST R 50922-2006. – instead of GOST R 50922-96; enter. 01.02.2008 // ATP "Consultant-Plus". – Access mode: <http://www.consultant.ru>. (In Russ.)]

2. GOST R ISO/MEK 15408-1-2008. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast' 1. Vvedeniye i obshchaya model'. – Vved. 2009-10-01. [GOST R ISO/IEC 15408-1-2008. Information technology. Methods and means of security. Criteria for assessing the security of information technology. Part 1. Introduction and General model. – Enter. 2009-10-01. (In Russ.)]

3. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii : utv. Prezidentom Rossiyskoy Federatsii №646 ot 06.12.2016 // SPS «Konsul'tant Plyus». – Rezhim dostupa: <http://www.consultant.ru> [The doctrine of information security of the Russian Federation : app. President of the Russian Federation №646 from 06.12.2016 // ATP "Consultant Plus". – Access mode: <http://www.consultant.ru>. (In Russ.)]

4. Nesterov S. A. Informatsionnaya bezopasnost' : uchebnik i praktikum dlya akademicheskogo bakalavriata / S. A. Nesterov. Moskva : Izdatel'stvo Yurayt, 2017. 321 s. (Universitety Rossii). ISBN 978-5-534-00258-4. Tekst : elektronnyy // EBS Yurayt [sayt]. URL: <https://www.biblio-online.ru/bcode/398687> (data obrashcheniya: 15.06.2019). [Nesterov S. A. Information security : textbook and workshop for academic undergraduate / S. A. Nesterov. Moscow : Yurayt Publishing House, 2017. 321 p. (Russian Universities). ISBN 978-5-534-00258-4. Text : electronic // EBS yurayt [website]. URL: <https://www.biblio-online.ru/bcode/398687> (date accessed: 15.06.2019). (In Russ.)]

5. Biryukov A.A. Informatsionnaya bezopasnost'. Zashchita i napadeniye. 2-ye izdaniye. M.: DMK-Press, 2017. [Biryukov A. A. Information security. Defense and offense. 2nd edition. M.: DMK-Press, 2017. (In Russ.)]

6. Nesterov A.D., Barkalov YU.M. Vyavleniye ugroz informatsionnoy bezopasnosti v mobil'nykh operatsionnykh sistemakh // Vserossiyskaya nauchno-prakticheskaya konferentsiya. Aktual'nyye voprosy ekspluatatsii sistem okhrany i zashchishchennykh telekommunikatsionnykh sistem. - Voronezh: Voronezhskiy institut MVD Rossii, 2016. - S. 17-19. [Nesterov A.D., Barkalov Yu. M. Identification of information security threats in mobile operating systems // all-Russian scientific and practical conference. Topical issues of operation of security systems and secure telecommunications systems. - Voronezh: Voronezh Institute of the Russian interior Ministry, 2016. pp. 17-19. (In Russ.)]

7. Kichuk D.YA., Burdinskiy I.A. Osobennosti issledovaniya informatsii v mobil'nykh ustroystvakh pod upravleniyem OS Android po prestupleniyam v sfere distantsionnogo bankovskogo obsluzhivaniya // Aktual'nyye voprosy ekspluatatsii sistem okhrany i zashchishchennykh telekommunikatsionnykh sistem. Voro-nezh: Voronezhskiy institut MVD, 2018. S. 123-124. [Kichuk D. Ya., Burdinsky I. A. Features of information research in mobile devices running Android OS on crimes in the field of remote banking // Actual issues of operation of security systems and secure telecommunications systems. Voronezh: Voronezh Institute of the interior Ministry, 2018. pp. 123-124. (In Russ.)]

8. Nesterov A.D., Barkalov YU.M. Organizatsionno-pravovoye obespecheniye polucheniya informatsii iz mobil'nykh ustroystv i oblachnykh khranilishch pri rassledovanii intsidentov v sfere informatsionnoy bezopasnosti // Mezhdunarodnaya nauchno-prakticheskaya konferentsiya. Prestupnost' v SNG: Problemy preduprezhdeniya i raskrytiya prestupleniy. - Voronezh: Voronezhskiy institut MVD Rossii, 2015. - S. 34-36. [Nesterov A.D., Barkalov Yu. M. Organizational and legal support for obtaining information from mobile devices and cloud storage in the investigation of incidents in the field of information security // international scientific and practical conference. Crime in the CIS: Problems of crime prevention and detection. - Voronezh: Voronezh Institute of the Russian interior Ministry, 2015. pp. 34-36. (In Russ.)]
9. Analiz ugroz informatsionnoy bezopasnosti sovremennykh mobil'nykh sistem / Zhernakov S. V., Gavrilov G. N. // Integratsionnyye protsessy nauki XXI veka: sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Sterlitamak: RITS AMI, 2015. С. 54 - 60. [Analysis of threats to information security of modern mobile systems / Zhernakov S. V., G Gavrilov. N. // Integration processes of science of the XXI century: collection of articles of scientific and practical International conference. Sterlitamak: the RITZ, 2015. pp. 54 - 60. (In Russ.)]
10. Detektirovaniye vredonosnogo programmnoy obespecheniya v mobil'noy operatsionnoy sisteme na baze Android na osnove razresheniya s primeneniye metoda opornykh vektorov / Zhernakov S. V., Gavrilov G. N. // Nauchno periodicheskoye izdaniye Ceteris Paribus: Yevropeyskiy fond innovatsionnogo razvitiya. Yezhemes. nauch. zhurnal «Ceteris Paribus», 2015.S. 10 -14. [Detection of malicious software in Android-based mobile operating system based on resolutions using the support vector machine / Zhernakov S. V., Gavrilov G. N. // Scientific periodical Ceteris Paribus: European Foundation for innovative development. Every minute. science. journal "Ceteris Paribus", 2015.pp. 10 -14. (In Russ.)]
11. Mastkhev dlya mobil'noy analitiki. Chto nuzhno, chtoby vskryvat' prilozheniya dlya Android na Android // Khaker URL: <https://xakep.ru/2019/03/12/mobile-analytics-must-have/> (data obrashcheniya: 15.06.2019). [A must have for mobile Analytics. You need to open Android apps on the Android // Hacker URL: <https://xakep.ru/2019/03/12/mobile-analytics-must-have/> (accessed: 15.06.2019). (In Russ.)]
12. Uyazvimost' v Android pozvolyayet perekhvatyvat' konfidentsial'nyye dannyye // Khaker URL: <https://xakep.ru/2018/09/03/wifi-broadcasts-leak/> (data obrashcheniya: 15.06.2019). [Vulnerability in Android allows you to intercept sensitive data // Hacker URL: <https://xakep.ru/2018/09/03/wifi-broadcasts-leak/> (date of application: 15.06.2009). (In Russ.)]
13. Barkalov YU.M. Metodika rassledovaniya prestupleniy v sfere distantsionnogo bankovskogo obsluzhivaniya // Obshchestvennaya bezopasnost', zakonnost' i pravoporyadok v III tysyacheletii. Voronezh: Voronezhskiy institut MVD Rossii, 2015. S. 172-176. [Barkalov Yu. M. Methods of investigation of crimes in the field of remote banking // Public security, law and order in the III Millennium. Voronezh: Voronezh Institute of the Russian interior Ministry, 2015. pp. 172-176. (In Russ.)]
14. Barkalov YU.M. Provedeniye ekspertizy programmnoy obespecheniya mobil'nykh ustroystv pod upravleniyem OS "Android" // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. Voronezh: Voronezhskiy institut MVD Rossii, 2016. S. 137-142. [Barkalov Yu. M. Examination of software for mobile devices running OS "Android" // Crime in the field of information and telecommunication technologies: problems of prevention, detection and investigation of crimes. Voronezh: Voronezh Institute of the Russian interior Ministry, 2016. pp. 137-142 (In Russ.)]
15. Barkalov YU.M., Perminov G.V. Vyyavleniye NSD k mobil'nykh ustroystvam, ispol'zuyemykh v ISOD MVD Rossii // Okhrana, bezopasnost', svyaz'. Voronezh: Voronezhskiy institut MVD Rossii, 2017. S. 32-36. [Barkalov S. M., Perminov, G. V., Detection of unauthorized access to mobile devices used in ISOD of the MIA of Russia // Security, safety, connectivity. Voronezh: Voronezh Institute of the Russian interior Ministry, 2017. pp. 32-36. (In Russ.)]

Сведения об авторах:

Баркалов Юрий Михайлович – заместитель начальника кафедры информационной безопасности.

Нестеров Антон Дмитриевич – адъюнкт.

Information about the authors:

Yuri M. Barkalov – Deputy head of information security Department.

Anton D. Nesterov–Adjunct.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию 19.04.2019.

Принята в печать 01.06.2019.

Conflict of interest.

The authors declare no conflict of interest.

Received 19.04.2019.

Accepted for publication 01.06.2019.