

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Локтионова Оксана Геннадьевна  
Должность: проректор по учебной работе  
Дата подписания: 09.09.2021 14:08:03  
Уникальный программный ключ:  
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждение высшего образования

«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ  
Проректор по учебной работе  
О.Г. Локтионова  
«15» 12 2017 г.



### Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android

Методические указания по выполнению лабораторной работы  
по дисциплине «Защита информации в системах беспроводной  
связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22(076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент

Кандидат технических наук, доцент кафедры  
информационной безопасности *А.Г. Сневаков*

**Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android:** методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 9 с.: Библиогр.: с. 9.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. 15.12.17      Формат 60x84 1/16.  
Усл. печ. л. 10. Уч. – изд. л. 10. Тираж 30 экз. Заказ 2979. Бесплатно.  
Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

## Содержание

1 Цель лабораторной работы.....	4
2 Задание.....	4
3 Порядок выполнения работы .....	4
4 Содержание отчета .....	4
5 Теоретическая часть .....	5
6 Контрольные вопросы.....	9
Библиографический список.....	9

## **1 Цель лабораторной работы**

Ознакомление с методами защиты абонентского терминала сотовой связи GSM в системе Android.

Перед выполнением лабораторного задания студенты должны ориентироваться в основных аспектах информатики и иметь основные понятия о функционировании системы сотовой связи GSM и используемых методах защиты информации.

В результате выполнения лабораторного задания студенты должны получить навыки защиты абонентского терминала сотовой связи GSM в системе Android.

## **2 Задание**

При подготовке к лабораторному занятию следует предварительно изучить: методы защиты мобильного терминала (т.е. сотового телефона и смартфона) от несанкционированного доступа в сеть.

1. Ознакомиться со всеми опциями системы безопасности смартфона, приведенными в теоретической части.
2. Установить блокировку экрана.
3. Установить режим видимости вводимых паролей.
4. Исследовать порядок шифрования данных (но не шифровать!)
5. Ознакомиться с порядком работы с сертификатами безопасности.

## **3 Порядок выполнения работы**

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить задание на основе методических указаний;
4. Составить отчет.

## **4 Содержание отчета**

1. Краткие теоретические сведения по методам кодовой защиты мобильного терминала.

2. Выполненное задание.

## 5 Теоретическая часть

Одним из наиболее важных аспектов защиты информации в системах сотовой связи GSM является защита личной информации, хранящейся в абонентском терминале пользователя.

С этой целью используются разнообразные программные средства ограничения доступа к мобильному терминалу со стороны посторонних лиц.

Конкретные средства обеспечения безопасности терминала зависят от конкретного терминала, наличия или отсутствия в нем предустановленной операционной системы и типа операционной системы, используемой в терминале.

В данной работе рассматриваются средства безопасности, используемые в операционной системе Android 4.X.

### Установка блокировки экрана

В зависимости от того, как используется устройство, можно установить автоматическую блокировку экрана, чтобы предотвратить несанкционированный доступ. Когда дисплей устройства переходит в спящий режим, включается автоматическая блокировка экрана.

Для настройки параметров блокировки:

- 1 Нажмите иконку «Настройки» на «Домашнем экране» или в меню приложений.
- 2 Выберите **Личные > Безопасность (Защита) > Блокировка экрана**
- 3 Выберите тип блокировки, который хотели бы использовать.

Можно выбрать один из вариантов блокировки, перечисленных в приблизительном порядке защиты:

- «Провести пальцем»: не обеспечивает защиту, но позволяет быстро получить доступ к «Домашнему экрану» или открыть камеру и начать съемку немедленно.

- «**Графический ключ**» позволяет рисовать простые модели пальцем, чтобы разблокировать телефон.

- «**Пароль**» состоит из четырех или более символов. Это самый безопасный вариант при условии создания надежного пароля. Для лучшей безопасности укажите пароль, состоящий не менее, чем из 8 символов. Пароль может содержать в себе сочетание цифр, букв и специальных символов.

## **Дополнительные параметры**

Настройки > Устройство > Экран > Спящий режим  
Настройки > Личные > Безопасность > Блокировка экрана

## **Настройки безопасности**

Настройки безопасности размещены в специальном разделе меню смартфона и содержат следующие опции:

### **1. Настройки блокировки экрана.**

Нажмите, чтобы настроить блокировку экрана с запросом графического ключа, PIN-кода или пароля для разблокировки экрана или чтобы никогда не блокировать экран.

### **2. Зашифровать устройство.**

Нажмите, чтобы зашифровать содержимое устройства и запрашивать цифровой PIN-код или пароль для расшифровки устройства при каждом включении.

### **3. Настроить блокировку SIM-карты.**

(Только для устройств, использующих SIM-карты). Открывает экран, на котором можно настроить обязательный ввод PIN-кода SIM-карты для использования устройства, а также поменять PIN-код SIM-карты.

#### **4. Видимые пароли.**

Установите этот флажок для краткого отображения каждого символа по мере ввода пароля, чтобы видеть, что именно вы набираете.

#### **5. Администраторы устройства.**

Открывает экран со списком приложений, которые Вы авторизовали для выполнения действий администратора в операционной системе устройства. Как правило, это электронная почта, календарь и другие корпоративные приложения, которым подобное право предоставляется при добавлении учетной записи корпоративной службы, требующей, чтобы на подключенных устройствах применялись корпоративные политики. Нажмите приложение в этом списке, чтобы отключить его право на выполнение функций администратора устройства. В этом случае добавленная учетная запись потеряет ряд функциональных возможностей, например, не сможет загружать электронную почту или события календаря до тех пор, пока приложение вновь не получит права администратора устройства. Приложение, у которого были подобным образом отключены права администратора устройства, но использующее аккаунты с возможностью администрирования устройства, начнет, как правило, уведомлять Вас о необходимости восстановления прав, если только Вы не удалите соответствующие учетные записи.

#### **6. Использовать безопасные учетные данные.**

Установите этот флажок, чтобы приложения могли получать доступ к зашифрованному хранилищу сертификатов безопасности, соответствующих паролей и других учетных данных на устройстве. Используйте хранилище учетных данных для установки подключения к VPN и Wi-Fi, как описано в разделе Подключение к сетям и устройствам. Если пароль для хранилища учетных данных не установлен, этот параметр будет недоступен для выбора.

## **7. Устанавливать с карты памяти.**

Нажмите, чтобы установить сертификат безопасности из памяти устройства, как описано в разделе Работа с сертификатами безопасности.

## **8. Установить пароль.**

Открывает диалоговое окно, в котором можно задать или изменить пароль для безопасного хранилища учетных данных. В пароле должно быть не менее 8 символов (см. раздел «Работа с сертификатами безопасности»).

## **9. Очистить хранилище.**

Удаляет все сертификаты безопасности и связанные учетные данные, а также, получив подтверждения пользователя, стирает собственный пароль хранилища.

## **Работа с сертификатами безопасности**

Если в организации используются VPN или сети Wi-Fi, основанные на сертификатах безопасности, то пользователю мобильного терминала нужно получить такие сертификаты и сохранить их на устройстве в безопасном хранилище учетных данных. После этого можно настроить доступ к VPN и сетям Wi-Fi с данного терминала.

Если администратор сети попросил загрузить сертификаты с веб-сайта, при загрузке сертификатов Вам будет предложено установить пароль для хранилища учетных данных.

Android поддерживает зашифрованные сертификаты X.509 в формате DER, сохраненные в файлах с расширением .crt (если файл сертификата имеет расширение .cer, .der или другое, его нужно изменить на расширение .crt).

Android поддерживает также сертификаты X.509, сохраненные в файлах хранения ключей PKCS#12 с расширением



.p12 (если хранилище ключей имеет расширение .pfx или другое, его необходимо заменить на .p12). При установке сертификата из хранилища ключа PKCS#12 Android также устанавливает сопутствующие закрытые ключи или сертификаты-разрешения, содержащиеся в хранилище ключей.

## **6 Контрольные вопросы**

1. Для чего нужны меры по обеспечению безопасности мобильного терминала от НСД?
2. Какая информация должна быть защищена от НСД?
3. Как производится настройка параметров блокировки экрана?
4. Как ввести пароль и обеспечить его видимость при вводе ?
5. Как зашифровать устройство?
6. Для чего нужны сертификаты безопасности?

## **Библиографический список**

- 1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.
- 2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.