

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК [004.42:373]: 004.056.5

Евдокименко
Максим Николаевич

Мобильное приложение для обеспечения информационной безопасности
служебных смартфонов

АВТОРЕФЕРАТ

на соискание степени магистра информатики и вычислительной техники

по специальности 1-40 81 02 «Технологии виртуализации и облачных
вычислений»

Научный руководитель
Сечко Георгий Владимирович
к.т.н., доцент

Минск 2019

ОГЛАВЛЕНИЕ

Общая характеристика работы	3
Введение.....	4
Краткое содержание работы	6
Заключение	7
Список публикаций соискателя.....	8

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Выдача предприятиями и учреждениями служебных гаджетов (портативных компьютеров, сотовых телефонов и гаджетов других видов) своим сотрудникам становится все более массовым явлением в мире. Видимо поэтому они наиболее подвержены атакам различных злоумышленников. В этих условиях **целью настоящей работы** является дальнейшее повышение информационной безопасности служебных смартфонов.

Для достижения поставленной цели в этой диссертации поставлены и **решены следующие задачи:**

- проведен обзор накопленного опыта в области информационной безопасности смартфонов;
- проведен анализ методов борьбы с угрозами информационной безопасности служебных смартфонов;
- разработаны собственные новые организационно-программные способы защиты информации служебных смартфонов

ВВЕДЕНИЕ

Очень многие из нас уже носят с собой устройства, которые еще несколько десятилетий назад описывали лишь в научно-фантастической литературе: телефон, компьютер, плеер с бесконечным запасом песен, видеокамера, навигатор и почти вся информация в мире. На фоне смартфонов и других мобильных аппаратов настольные компьютеры и ноутбуки выглядят такими же громоздкими и устаревшими, как сотовые телефоны 25-летней давности.

Но достаточна ли защита информации в новых мобильных устройствах – смартфонах и других гаджетах?

Компактное устройство, напичканное датчиками, – это, по сути, «кладезь» уязвимостей, которыми обязательно попытаются воспользоваться злоумышленники. Мобильные аппараты способны исполнять множество сторонних приложений, используются повсюду, постоянно на связи с сетями, часто лежат без присмотра и теряются. Им необходимы сильные меры защиты, но не в ущерб удобству.

Многие из нас считают мобильные устройства вполне безобидными, видя в них обычные телефоны, совмещенные с газетами и видеоиграми. Однако суровая реальность состоит в том, что смартфоны – это постоянная угроза пользовательским данным. Она может материализоваться через уведомление о приватности в форме длинных юридических документов; через запросы привилегий, способные запутать даже технических специалистов; через вредоносные коды, а также неверно сконфигурированные и откровенно шпионские программы.

Чтобы рядовые пользователи мобильных устройств могли рассчитывать на безопасность, прогресс и защита информации должны стать партнерами. Существует мнение (и мы его тоже придерживаемся), что информационную безопасность мобильного устройства определяют пять основных категорий лиц, причастных к мобильникам: разработчики приложений, разработчики операционных систем, поставщики оборудования, операторы мобильных услуг (лайф, Вэлком, МТС и другие) и сами пользователи.

Создатели ведущих мобильных операционных систем осознают важность приватности пользовательских данных и вложили немало усилий в то, чтобы помочь программистам ее соблюдать. Тем не менее, не все из них придерживаются необходимых правил, поэтому бдительность самих пользователей по-прежнему остается важнейшим условием надежного хранения персональных и других данных.

Ещё более важной для обеспечения информационной безопасности мобильных устройств является проблема защиты информации в

приложениях для них, решить небольшую частичку которой и сделана попытка в настоящей диссертации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, списка публикаций автора и приложений.

В первой главе представлен анализ уязвимостей и угроз мобильных приложений на Android. Приведены общие сведения об информационной безопасности мобильных устройств. Произведен анализ работ Эндрю Хуга по защите информации в смартфонах.

Во второй главе проведен анализ и сравнение методов борьбы с угрозами информационной безопасности относительно малого по меркам Беларуси предприятия (100-150 работающих), выдающего своим сотрудникам служебные гаджеты. Рассмотрены современные запатентованные зарубежные решения. Предложены рекомендации по выбору таких методов для малого белорусского предприятия. Рассмотрено специально разработанное программное средство, которое защищает мобильные устройство сотрудников от вредоносных или шпионских программ.

В третьей главе диссертации идет речь о программном обеспечении для блокировки доступа пользователям служебных ЛМУ к неразрешённым веб-ориентированным приложениям. Предложен и описан новый организационно-программный способ защиты информации в мобильных системах Android, заключающийся в выдаче руководством компании своим сотрудникам на время работы личных защищённых мобильных устройств. Рассмотрена программная реализация этого способа – приложение БП

Четвертая глава описывает предлагаемый новый вариант прошивок Android с целью повышения его информационной безопасности. Выбран вариант шифрования для защитных прошивок – вариант с использованием OpenSSL API (нативный код). Для выбранного варианта составлены вербальный алгоритм шифрования и порядок получения случайных чисел в нативном коде C и приведена их программная реализация.

Общий объем работы составляет 68 страниц, из которых основного текста – 50 страниц, 20 рисунков, 1 таблица, список использованных источников из 46 наименований, 4 приложения.

ЗАКЛЮЧЕНИЕ

Как показал обзор проанализированных литературных источников и анализ хранящихся в Национальной базе уязвимостей США уязвимостей МОС Android, основными уязвимостями Android, вызывающими угрозы его информационной безопасности, являются вредоносное ПО (ВПО) и утечка контента и хищение персональных данных. В этих условиях в диссертации проанализированы перечисленные угрозы и выбраны направления работ по парированию этих угроз.

Для этого предложен и подробно описан новый организационно-программный способ защиты информации в мобильных системах Android, заключающийся в выдаче руководством компании своим сотрудникам на время работы личных защищённых мобильных устройств. Рассмотрена программная реализация этого способа – приложение БП.

Выбран вариант шифрования для защитных прошивок – вариант с использованием OpenSSL API (нативный код). Для выбранного варианта составлены вербальный алгоритм шифрования и порядок получения случайных чисел в нативном коде С и приведена их программная реализация.

Результаты работы опубликованы в трёх статьях и обсуждены на двух научно-технических конференциях.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А Анализ методов борьбы с угрозами информационной безопасности служебных гаджетов малого белорусского предприятия / Д. К. Дедович, М. Н. Евдокименко, М. С. Журавлев, В. Л. Николаенко, Г. В. Сечко, Т. Г. Таболич // Сборник материалов XXV МНТК «Информационные системы и технологии» (ИСТ–2019), Нижний Новгород (19 апреля 2019 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2019. – 1097 с. – С. 954–561.

2-А Дедович, Д. К. Обеспечение производственной безопасности предприятия за счёт использования служебных гаджетов / Д. К. Дедович, М. Н. Евдокименко // Проблемы информатики, радиоэлектроники и защиты информации : Сборник трудов постоянно действующего семинара «Проблемы информатики, радиоэлектроники и защиты информации» / Под редакцией: Г. В. Сечко. – Минск: Общество с ограниченной ответственностью «Стрим центр», 2019. – Т. 1 (заседание 04.01.2019) – 51 с.: Библиогр.: 7 назв. Рус. – Деп. в «БелИСА» – С. 5–7.

3-А Евдокименко, М. Н. Работы Эндрю Хуга по защите информации в смартфонах / М. Н. Евдокименко, Д. К. Дедович // Проблемы информатики, радиоэлектроники и защиты информации : Сборник трудов постоянно действующего семинара «Проблемы информатики, радиоэлектроники и защиты информации» / Под редакцией: Г. В. Сечко. – Минск: Общество с ограниченной ответственностью «Стрим центр», 2019. – Т. 1 (заседание 04.01.2019) – 51 с.: Библиогр.: 7 назв. Рус. – Деп. в «БелИСА» – С. 8–15.

Труды соискателя, выходящие за рамки исследования диссертации:

4-А Гайдамака, А. В. Информационная безопасность веб-приложений / А. В. Гайдамака, М. Н. Евдокименко // 51-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 18 апреля 2015 года). – Мн.: БГУИР, 2015. – 75 с. с ил. – С. 30.