здесь $\Delta_{доп}$ – множество допустимых альтернатив реализации средств защиты.

Из введенного показателя качества выбора средств защиты, который должен стремиться к максимуму и с учётом множества допустимых альтернатив реализации средств защиты, решением математической постановки задачи будет являться нахождение всех неизвестных компонент вектора $\boldsymbol{X}$ и выбор тех средств защиты b_j, для которых компонента вектора x_j равна 1.

В соответствии с разработанной математической моделью, необходимо разработать алгоритм, направленный на решение задачи обеспечения целостности информации в облачных структурах коммерческого применения.

Для того чтобы определить, какие средства защиты необходимы для максимальной степени защиты системы, необходимо рассмотреть классы атак.

В контексте облачных хранилищ можно разделить класс атаки на целостность на две:

– атака на облачное хранилище с целью нарушение целостности в облаке вне синхронизации, например, подмена файла;

– атака на облачное хранилище при синхронизации файлов, используя уязвимости мобильного устройства, канал связи или облачного хранилища.

Таким образом, разрабатываемое решение будет состоять из модуля проверки целостности файла, взаимодействующего с основным модулем облачного сервиса, обеспечивающего версионность файлов, авторизацию пользователей и так далее. Проверка целостности от динамических атак актуальна при записи файла из источника, при чтении файла актуальна проверка целостности от статических атак. Результаты проверки целостности файлов будут выводиться на консоль либо в графический интерфейс.

Согласно модели обеспечения целостности информации, источник с высоким уровнем целостности может писать в файлы как с высоким уровнем целостности, так и с низким. Если пришёл запрос от источника с низким уровнем целостности, программа должна ограничить источник, чтобы он имел возможность записывать в файлы с низким уровнем целостности. После записи в файл производится проверка целостности информации.

Литература

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: Логос, 2001. – 256 с.

2. Клементьев И.П., Устинов В.А. Введение в облачные вычисления // Интернет университет информационных технологий. – Режим доступа: http://www.intuit.ru/department/se/incloudc/. – Дата доступа 22.10.2016.

3. Li J., Wang Q., Wang C., Cao N., Ren K., Lou W. Fuzzy keyword search over encrypted data in cloud computing. Mini-Conf. IEEE INFOCOM, 2010, Digital Object Identifier 10.1109/INFOCOM.2010.5462196

4. Android vulnerabilities. – Режим доступа: https://www.androidvulnerabilities.com/. – Дата доступа: 15.09.2020.

УДК 681.326

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ В ОПЕРАЦИОННОЙ СИСТЕМЕ ANDROID

Карташова Ж.К.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

ОС Android за небольшой промежуток времени стала одной из самых популярных систем для всевозможных мобильных устройств. Ее используют как крупные производители с мировым именем, так и небольшие компании. Данная публикация посвящена анализу существующих решений в области защиты мобильных устройств, анализу алгоритмов управления доступом. Описаны программные и аппаратные требования для функционирования мобильной программы в операционной системе Android

На современном этапе развития все более активно в повседневную деятельность внедряются различные мобильные устройства. Уже несколько лет рынок мобильных устройств занимает лидирующие позиции по количеству пользователей, превосходя рынок персональных компьютеров. Учитывая возможности современных мобильных устройств перед разработчиками встают новые вопросы и проблемы в области обеспечения информационной безопасности. Для достижения этих целей мобильные устройства необходимо защищать от самых разных угроз.

Популярность использования мобильных устройств требует больших ресурсов для управления настройками и обеспечения информационной безопасности.

Разработанные для управления инфраструктурой мобильных устройств Mobile Device Management системы задают настройки соответствия политикам безопасности и настройки доступа в корпоративную сеть для всех одобренных мобильных устройств. При этом с их помощью осуществляется регистрация и мониторинг

устройств, а в случае потери или кражи смартфона или планшета с помощью MDM с него можно удалить конфиденциальные либо все данные.

Основные угрозы и уязвимости информационной безопасности мобильных устройств под управлением ОС Android. *Использование недоверенных мобильных устройств.* Сегодня в мобильных устройствах не реализованы технологии «корня доверия» (root of trust), например, модули Trusted Platform Module, (TPM), которые все чаще встраиваются в ноутбуках и рабочих станциях. К тому же нередко встречаются такие действия, как «rooting» мобильных устройств, свидетельствующие о том, что встроенные ограничения по безопасности, используемые операционной системой можно обойти.

Использование недоверенных сетей. Поскольку мобильные устройства используют для доступа в интернет внешние каналы связи, пользователь обычно не может контролировать безопасность используемых устройством сетей. В их число могут входить широкополосные сети, в том числе кабельные и беспроводные, например, Wi-Fi или сотовые сети. Эти системы связи не защищены от перехвата данных, что создает риск кражи конфиденциальной информации с целью перехвата и модифицирования сообщений.

Риски, возникающие при использовании недоверенных сетей, можно уменьшить, применяя технологии шифрования (например, виртуальные частные сети, VPN) для защиты конфиденциальности и целостности сообщений, а также с помощью механизмов взаимной аутентификации для проверки подлинности обеих сторон, участвующих в передаче данных.

Использование недоверенных приложений. Мобильные устройства позволяют легко находить, приобретать, устанавливать и использовать приложения сторонних разработчиков из магазинов мобильных приложений. Это создает очевидные риски, особенно для платформ и магазинов приложений, не накладывающих на приложения ограничений, обусловленных требованиями безопасности, или иных условий.

Риск, связанный с этими приложениями, можно уменьшить несколькими способами. Можно запретить установку посторонних приложений, создать «белый список» для допуска к установке только доверенных приложений, проверять, что приложение имеет только необходимый доступ к ресурсам мобильного устройства, или реализовать безопасную программную среду, которая изолирует конфиденциальные данные от прочих данных и приложений на мобильном устройстве.

Взаимодействие с другими системами. Мобильные устройства могут взаимодействовать с другими системами в рамках обмена данными и хранения данных. Взаимодействие с локальной системой чаще всего подразумевает соединение мобильного устройства со стационарным компьютером или ноутбуком по беспроводному каналу или через кабель для зарядки и/или синхронизации. В момент синхронизации устройств злоумышленник может перехватить конфиденциальную информацию.

Троянские программы. В зависимости от семейства, эти вредоносные программы обладают таким функционалом, как, сбор конфиденциальной информации пользователя, добавление закладок в браузер, выполнение команд, поступающих от злоумышленников, отправка СМС-сообщений, установка других приложений и многое другое. Чтобы реализовать возможность установки приложений, не вызывая подозрений со стороны пользователя, троянцам необходимы права root, которые в ОС Android можно получить, установив стороннюю прошивку на мобильное устройство.

Программные и аппаратные требования при разработке мобильной программы в ОС Android. Основную информацию о программе в системе предоставляет файл манифеста *AndroidManifest.xml.* Каждое приложение должно иметь свой файл *AndroidManifest.xml.*

Назначение файла:

– объявляет имя Java-пакета приложения, который служит уникальным идентификатором;

– описывает компоненты приложения – деятельности, службы, приемники широковещательных намерений и контент-провайдеры, что позволяет вызывать классы, которые реализуют каждый из компонентов, и объявляет их намерения;

– содержит список необходимых разрешений для обращения к защищенным частям API и взаимодействия с другими приложениями;

– объявляет разрешения, которые сторонние приложения обязаны иметь для взаимодействия с компонентами данного приложения;

– объявляет минимальный уровень API Android, необходимый для работы приложения;

– перечисляет связанные библиотеки.

Версия операционной системы. Устройства могут поддерживать разные версии ОС Android, такие как Android 4.0 или Android 5.0. Каждая последующая версия системы часто дополняется новыми функциями API, которые недоступны в предыдущих версиях системы. Для определения набора доступных функций API каждой версии ОС соответствует уровень API. Например, Android 1.0 – это 1-й уровень API, а Android 5.0 – этой 20-й уровень.

Каждая последующая версия ОС Android обеспечивает совместимость для приложений, которые были составлены с помощью функций API предыдущих версий, то есть мобильное приложение всегда будет совместимо с будущими версиями ОС Android.

Выводы. В результате были проанализированы существующие угрозы и уязвимости в ОС Android, проведен обзор версий операционной системы и рассмотрены аппаратные и программные требования для функционирования мобильной программы в ОС Android.

На основании анализа выявлено, что основными угрозами противодействия несанкционированного доступа являются использование недоверенных приложений, что может привести к несанкционированному доступу в устройство, троянские программы, эта угроза является следствием недоверенных программ.

Литература

1. Михайлов С.Ф., Петров В.А Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие М.: МИФИ, 2015. 192 с..

2. Мельникова О.В. Смартфоны на Android Москва, 2013. – 304 с.

3. Список уязвимостей ОС Android. Система известных уязвимостей: MITRE corp.

4. Android vulnerabilities. – Режим доступа: https://www.androidvulnerabilities.com/. – Дата доступа: 27.09.2020.

УДК 376.356: 004.9

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПОДГОТОВКЕ ИНЖЕНЕРНЫХ КАДРОВ

Боженков В.В.[1], Шахлевич Г.М.[2]

[1]Белорусская государственная академия связи
Минск, Республика Беларусь
[2]Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

В условиях лавинообразного роста объема и обновления информации все актуальней становится необходимость повышения качества, эффективности и доступности знаний. Проблема соответствия системы образования вызовам современности решается только за счет коренной модернизации основных звеньев образовательного процесса: преподаватель – учебно-методическое, техническое и организационное обеспечение – учреждение образования. Носителем самого ценного в образовательном процессе (живая беседа, дискуссия, совместный анализ и исследовательская деятельность) является преподаватель. Общение с аудиторией в рамках традиционного занятия сегодня непозволительная роскошь. Условием эффективного использования уникальных возможностей преподавателя и инструментом интенсификации образовательной деятельности являются интерактивные электронные образовательные ресурсы (ЭОР) [1]. Однако их неквалифицированные применение в подготовке инженерных кадров сопряжено с определенными опасностями: меньше времени уделяется изучению применяемых техническом творчестве математических методов, физическому смыслу моделируемых явлений и другим теоретическим аспектам специальных дисциплин [2]. Как следствие, отсутствие хорошей теоретической подготовки вызывает непонимание студентами результатов моделирования технических устройств и физических явлений на компьютерах с использованием программ стимуляторов.

Например, широкое использование презентаций для предоставления теоретического материала имеет ряд недостатков. Как отмечается в работе [3] это прежде всего информационная перегрузка студентов. Каждый преподаватель имеет естественное желание предоставить максимальный объём знаний по читаемой дисциплине. Обладая значительными возможностями в текстовом и графическом предоставлении материала он часто готовит сложные информационно-перегруженные слайды. Следствием этого является высокая скорость изложения материала и невозможность его записи и усвоения студентами. Теряется эмоциональная привлекательность занятий. Как при перегрузке, так и в случае простоты материала и малозагруженности презентации студенты демонстрируют отказ от записи и осмысления учебного материала. Нередко это приводит к нарушению дисциплины и пропускам лекционных и других видов занятий. Возможность рассылки или копирования презентаций успокаивает студентов в благом намерении посмотреть учебный материал в «домашнй обстановке». Методисты рекомендуют подавать «дозируемые порции информации». Но как определить размер этой дозы в условиях разной подготовки и способностей студентов?

Следующий недостаток использования презентаций информационно-ограничительный. Задача высшей школы научить студента ориентироваться в пространстве знаний самостоятельно остается невыполненной. Студенты даже на младших курсах уже достаточно загружены, поэтому не могут или не хотят читать учебники, монографии и другие материалы, ограничивая себя объёмом презентаций представленных в их распоряжение.

Конечно, эти недостатки не мешают грамотно применять презентации на лекциях и семинарах