УДК 378.1

РЕАЛИЗАЦИЯ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ ТЕХНОЛОГИЙ

Хвостов В.А., Денисенко В.В., Скрыпников А.В., Высоцкая И.А., Савченко И.И., Сапелкин Р.С.

ФГБОУ ВО «Воронежский государственный университет инженерных технологий», Воронеж, e-mail: hvahva1@mail.ru, v.denisenko1@yandex.ru, skrypnikovvsafe@mail.ru, i.a.trishina@gmail.com, ilona.savchenko.2016@mail.ru, SapRS@mail.ru

На основе проведенного анализа предоставления дистанционных образовательных услуг с использованием мобильных технологий сделан вывод о обработке персональных данных при их реализации. Мобильные технологии в связи с рядом особенностей реализации дистанционного образования характеризуется рядом критических уязвимостей, вызванных особенностями архитектуры мобильных устройств (смартфонов, планшетов, смарт устройств, и т.п.), применяемой технологией доступа к интернет мобильными системами (как сети сотовой связи, так и сети беспроводного доступа) и серверной части информационных систем образовательных учреждений. В связи с обработкой персональных данныхпри дистанционном образовании с использованием мобильных систем, защита от угроз безопасности информации требует реализации технических и организационных мероприятий, заданных на законодательном уровне. В руководящих документах регуляторов обработки персональных данных России вопросы защиты информации при использовании мобильных технологий не рассматриваются в связи с новизной проблемы. Поэтому проблема обеспечения безопасности персональных данных при реализации дистанционных образовательных услуг с применением мобильных технологий является актуальной. В статье, на основе анализа актуальной угроз мобильных технологий и средств защиты информации, применяемых при использовании мобильных систем, предлагается система защиты для дистанционных образовательных технологий, использующих мобильный доступ.

Ключевые слова: дистанционная образовательная услуга, мобильная станция, шлюз безопасности, менеджер мобильных устройств

REALIZATION AND REMOTE EDUCATIONAL SERVICES USING MOBILE TECHNOLOGIES

Khvostov V.A., Denisenko V.V., Skrypnikov A.V., Vysotskaya I.A., Savchenko I.I., Sapelkin R.S.

Voronezh State University of Engineering Technologies, Voronezh, e-mail: hvahva1@mail.ru, v.denisenko1@yandex.ru, skrypnikovvsafe@mail.ru, i.a.trishina@gmail.com, ilona.savchenko.2016@mail.ru

Based on the analysis of the provision of distance educational services using mobile technologies, a conclusion was made about the processing of personal data during their implementation. A number of critical vulnerabilities caused by the peculiarities of the architecture of mobile devices (smartphones, tablets, smart devices, etc.), the technology used to access the Internet by mobile systems (both cellular networks and wireless access networks) and the server side of information systems of educational institutions characterize mobile technologies. In connection with the processing of personal data in distance education using mobile systems, protection against information security threats requires the implementation of technical and organizational measures specified at the legislative level. In the guidance documents of the regulators of personal data processing in Russia, the issues of information protection when using mobile technologies are not considered due to the novelty of the problem. Therefore, the problem of ensuring the security of personal data in the implementation of distance educational services using mobile technologies is urgent. In the article, based on the analysis of the current threats of mobile technologies and information security tools used when using mobile systems, a protection system for distance educational technologies using mobile access is proposed.

Keywords: distance education service, mobile station, security gateway, mobile device manager

Индивидуальный подход к обучению, свободный доступ к электронной образовательной среде, требования индивидуального слежения и контроль процессов самостоятельного освоения учебного материала учащимися обусловили широкое применение мобильных технологий в средней и высшей школе.

Целью работы является обнаружение возможных угроз и уязвимостей, обусловленных использованием мобильных технологий при реализации образовательного процесса, и формулирование рекомендаций по обеспечению безопасности персональных данных в мобильных образовательных информационных системах.

В современных электронных образовательных системах (ЭОС) мобильные станции выполняют следующие функции:

1) реализуют управление учебно-методическими комплексами, размещенными в ЭОС, координацию педагогических процессов в образовательном учреждении;

2) обеспечивают дистанционное взаимодействие внутри педагогического сообщества и связи с обучающимися;

3) мобильные устройства контроля и непосредственного воспитательного воздействия на обучающихся, используются для накопления, обработки и передачи необходимой информации;

4) обеспечивают непосредственный доступ к ЭОС, включая возможности непосредственного тестирования и контроля знаний;

Как показывает анализ современных мобильных приложений, большинство их имеют клиент-серверную архитектуру [1]. При этом клиентская часть работает на мобильной операционной системе (Android или iOS). Установка клиентской части обеспечивается магазином приложений – специализированной площадки, где разработчики размещают свои программы.

Пользователь устанавливает на мобильную станцию программу и взаимодействует напрямую с ЭОС: изучает теоретический материал лекций, получает консультации педагогов, проходит промежуточное и результирующее тестирование. При этом в качестве основного компонента ЭОС выступает сервер образовательного учреждения.

Сервер является платформой, размещаемой в образовательной организации, содержащей в большинстве случаев вебприложение. Установленное на сервере программное обеспечение взаимодействует с мобильными клиентами учащихся через INTERNET посредством интерфейса (API). Сервер образовательной организации является основой ЭОС. Здесь обрабатывается и хранится информация, осуществляется управление мобильными станциями и происходит синхронизация пользовательских данных.

Функционирование ЭОС с применением мобильных технологий связано с обработкой в технических средствах идентификационной информации учащихся, персональных данные педагогов и конфиденциальной информации образовательных учреждений [2].

Следовательно, применение мобильных технологий доступа в ЭОС имеет непосредственную связь с обработкой конфиденциальной информации различного уровня и, соответственно [3, 4], требует реализации организационных и технических мер по защите [5].

Проведенный в [6] анализ стандартов и руководящих документов в области защиты персональных данных выявил, что в России в настоящее время вопросы защиты информации в информационных системах, использующих мобильные технологии, не регламентируются. Требования к защите персональных данных, технические и организационные мероприятия по защите, содержащиеся в [3, 4], ориентированы на традиционные ЭВМ. Аналогичным образом, методический подход к разработке актуальной модели угроз информационных систем персональных данных не рассматривает мобильные системы.

Таким образом, применяемые в мобильных информационных системах средства обеспечения безопасности персональных данных не регулируются нормами законодательства и в связи с этим используются без правового и методического обоснования.

Как объект защиты от несанкционированного доступа, ЭОС с мобильным доступом обладают рядом отличий от традиционных информационных систем. В частности, применение в технологическом цикле обработки конфиденциальной информации приводит к существенному увеличению возможных уязвимостей ЭОС и большого количества новых по сравнению с традиционно рассматриваемыми угрозами [6].

По отношению к мобильным технологиям можно выделить следующих пользователей.

Сотрудники учреждения – имеют доступ к данным и услугам организации. Уровень доступа основывается на требованиях, прописанных в должностных обязанностях, а также уровне конфиденциальности информации, к которой сотрудник должен получить доступ.

Партнеры – персонал сторонних компаний, который сотрудничают с образовательной организацией для реализации определенных задач. Данной категории может потребоваться доступ к системе и инфраструктуре для проведения регламентных работ, однако отметим, что они не имеют такие доступ и права, как сотрудники образовательной организации.

Внешние пользователи – это лица, которые осуществляют доступ к общедоступным данным организации через предоставляемые и поддерживаемые организацией интерфейсы. Данная категория обычно не имеет учетных данных в ЭОС для идентификации.

Поставщики компонентов мобильных устройств – имеют возможность физически вмешиваться в работу мобильного устройства перед его поставкой. С точки зрения источника угрозы данная категория имеет возможность устанавливать вредоносное программное обеспечение.

Поставщики услуг сервисов беспроводных технологий – имеют полный доступ к сети сотовой связи, имеют возможность перенастройки мобильного устройства, имеют доступ к информационному ресурсу мобильной станции, что может привести к кэшированю данных пользователя.

Использование в технологическом цикле мобильных станций, провайдера беспровод-

ного доступа в Интернет, сотрудничество с организациями, предоставляющими высокоскоростные каналы передачи цифрового потока, приводят к тому, что уязвимости всех технических и программных средств, формирующих каналы удаленного доступа в ЭОС, должны быть учтены в актуальной модели угроз и парироваться с применением соответствующих организационных и технических мероприятий.

Как было показано ранее, нормативное и методическое регулирование применения средств защиты информации от несанкционированного доступа для ЭОС с мобильным доступом в России на сегодняшний день отсутствует. В связи с этим необходимо провести анализ международного опыта обеспечения ЗИ при организации мобильного доступа при реализации дистанционных образовательных услуг.

Угрозы, обусловленные применением мобильных станций. Уязвимости мобильных систем включают уязвимости аппаратной составляющей мобильной станции, мобильной операционной системы и мобильного приложения.

Анализ уязвимостей аппаратной составляющей мобильной станции, проведенный в [6], показал, что они по большей части обусловлены ошибками или с преднамеренно установленными в мобильные станции аппаратными люками. Локализация уязвимостей в основном ограничивается прошивкой мобильной станции. Также мобильные станции для обнаружения уязвимостей дополняют техническими средствами с функциями слежения и перехвата информации [1].

Уязвимости операционной системы и уязвимые приложения представляют большую опасность, поскольку для них открыт доступ с высоким уровнем привилегий. Мобильные приложения, как и программы для ЭВМ, могут иметь уязвимости и подвергаться атакам при эксплуатации. Как правило, приложения могут иметь уязвимости из-за низкого уровня программирования, проектирования или выбора конфигурации в вопросах обеспечения информационной безопасности.

Также для мобильных станций актуальной угрозой является отключение пользователем встроенных функций безопасности операционной системы [6]. Перечисленные уязвимости приводят к реализации совокупности угроз, направленных на мобильные системы.

Методы обеспечения безопасности персональных данных в мобильных образовательных информационных системах. При защите от угроз информационной безопасности можно применить менеджер мобильных устройств (MDM). Он реализует основы политики безопасности персональных данных при настройке параметров и режимов работы мобильных устройств пользователей. Можно выделить следующие параметры:

– параметры оборудования (например, разрешение на использование Bluetooth, NFC и т.д.);

– параметры пароля (включая длину и качество пароля);

– параметры шифрования;

– настройки браузера (например, запрет на сохранение cookie, блокировка jscript);

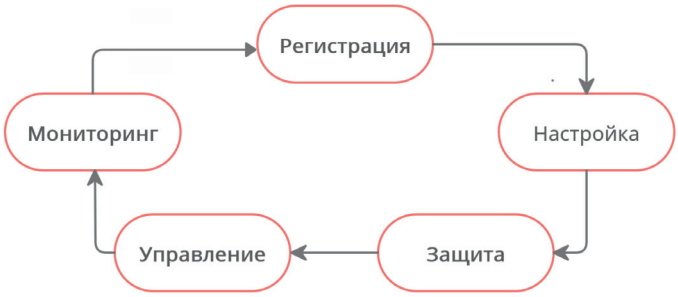
– разрешенные и запрещенные приложения;

– политики соответствия требованиям (например версия ОС).

При реализации угрозы нарушения физической целостности мобильной станции пользователя программа производит удаление конфиденциальной информации с мобильного устройства. Также может быть реализована очистка секретных кодов, удаленная блокировка или антивирусная поддержка.

Наиболее эффективными MDM являются MicrosoftIntune, AirWatchbyVMWare, CitrixXenMobile.

Процесс управления мобильными устройствами представим в виде последовательности, представленной на рисунке.



Процесс управления мобильными устройствами с использованием типовых решений MDM

Также для защиты от угроз информационной безопасности можно использовать менеджер мобильных приложений (MAM). Данный класс СЗИ предоставляет подмножество функций управления мобильными устройствами. Программа реализует функции распределения и управления данными, а также регулирует жизненный цикл некоторых мобильных приложений.

MAM поддерживает безопасность средств, предназначенных для аутентификации устройства. Также может включать диагностические функции, такие как удаленный вход в систему, создание отчетов и устранение неполадок. Специализированные реализации MAM являются отдельным компонентом мобильного приложения, так как не подлежат интеграции с реализациями MDM. Примером наиболее эффективных MAM являются Kaspersky Security for Mobile, SOTI Mobicontrol.

При организации защиты информационных ресурсов образовательной организации от угроз, направленных на уязвимости сервисов мобильного доступа образовательных информационных систем, рекомендуется применение средств идентификации и управление доступом (IAM). Этот класс СЗИ используют для внедрения аутентификации и авторизации, формирования единого профиля безопасности для всех пользователей в мобильном решении. Система IAM помогает гарантировать единый подход к обеспечению безопасности для всех мобильных сервисов и позволяет внедрять в мобильные решения корпоративные системы аутентификации пользователей.

Применение IAM в сочетании с MDM обеспечивает возможность пользователю иметь несколько мобильных устройств, настроенных с одним и тем же уровнем доступа. Синхронизацию данных между несколькими устройствами и пользователями так же обеспечивает система IAM.

Мобильные устройства используют беспроводную сетевую связь Wi-Fi, основанную на семействе стандартов IEEE 802.11a/b/g/n, и могут подключаться к персональным или корпоративным точкам доступа или аналогичным устройствам. Устройства, использующие беспроводную сетевую связь, уязвимы для перехвата информации анализаторами сигналов. Непроверенные точки доступа также представляют потенциальную угрозу «человек посередине» [6]. При организации защиты требуется применение шлюза и стека безопасности (GSS).

Через мобильные устройства могут реализовываться атаки на иные используемые сетевые устройства. Одновременное наличие сотовой и беспроводной сети в мобильных устройствах делает их идеальными платформами для обхода традиционной защиты информации. Чтобы минимизировать ущербы в ЭОС от скомпрометированного мобильного устройства, доступ к информационным ресурсам организации должен быть ограничен через один или несколько сетевых маршрутов и проверен стандартными сетевыми средствами защиты: проверка пакетов с отслеживанием состояния, обнаружение вторжений, а также фильтрация цифрового потока.

Кроме того, при трансляции цифрового потока мобильной станцией по высокоскоростным магистральным каналам, обеспечить защиту данных возможно только с использованием методов криптографической защиты информации. При этом применяются средства защиты, реализующие виртуальную частную сеть (VPN). Данный класс средств защиты обеспечивают надежный метод создания безопасных соединений между мобильными устройствами и информационными ресурсами образовательной организации при использовании публичных неуправляемых сетей. Технологии VPN, как правило, используются только авторизованными и партнерскими пользователями, но существуют технологии, которые позволяют устанавливать VPN-подключения для внешних пользователей [1].

Заключение

При организации образовательного процесса с помощью мобильных технологий используется конфиденциальная информация различного уровня, технологическая информация и ключевая информация криптографических протоколов различного вида. Таким образом, при использовании мобильных технологий необходимо обеспечить правильную организацию обработки конфиденциальной информации различного уровня [2–4].

Новые угрозы, обусловленные использованием современных технологий и новые векторы реализации образовательного процесса с использованием мобильных технологий, рассмотренные в статье, позволили выявить возможные уязвимости при использовании конфиденциальной информации и рекомендации по ее защите.

Список литературы

1. Ретабоуил С. Android NDK. Разработка приложений под Android на C/C++. М.: ДМК пресс. Электронные книги, 2014. 496 с.

2. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. № 165. 29 июля 2006 г.

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Российская газета. № 256. 07 ноября 2012 г.

4. Лузгина В.Б., Стаховская Ж.А. Опыт использования мобильных технологий в образовательной среде вуза // Образовательные технологии и общество. 2016. № 3. С. 463–472.

5. Арапов Д.В., Скрыпников А.В., Денисенко В.В., Высоцкая И.А. Разработка и защита баз данных. Учебное пособие по дисциплине «СУБД Oracle». Воронеж: ВГУИТ, 2020. 100 с.

6. Гулов В.П., Хвостов В.А., Скрыпников А.В., Косолапов В.П., Сыч Г.В. Анализ угроз безопасности информации при обработке персональных данных в мобильной медицине. Системный анализ и управление в биомедицинских системах. 2020. Т. 19. № 2. С. 129–138.