4. USAARL Report No. 88-13 [Электронный ресурс]. – Режим доступа: http://www.usaarl.army.mil/TechReports/88-13.PDF. – Дата доступа:18.03.2018

5. Авиашлемы. Виртуальная реальность в настоящем бою [Электронный ресурс]. – Режим доступа: https://naked-science.ru/article/tech/aviashlemy-virtualnaya-realnost-v/. – Дата доступа: 18.03.2018.

6. Joint Helmet Mounted Cueing System [Электронный ресурс]. – Режим доступа: https://www.rockwellcollins.com/Products and Services/Defense/Avionics/Displays and Controls/Helmet Mounted Displays/ Joint Helme Mounted Cueing System.aspx. – Дата доступа: 18.03.2018

7. F-35 Gen III Helmet Mounted Display System [Электронный ресурс]. – Режим доступа: https://www.rockwellcollins.com/Products and Services/ Defense/Avionics/Displays and Controls/Helmet Mounted Displays/F-35 Gen III Helmet Mounted Display System.aspx. –Дата доступа: 18.03.2018

8. Rash C.E. Helmet Mounted Displays: Design Issues for Rotary-wing Aircraft / C. E. Rash. – SPIE, 2001. – 258 p.

9. Newman D.G. Flying Fast Jets: Human Factors and Performance Limitations/D.G. Newman.– CRC Press, 2014.– 184 p.

10. Pentagon: Here are all the problems with the F-35 [Электронный ресурс]. – Режим доступа: http://www.businessinsider.com/here-are-all-the-problems-with-the-f-35-that-the-pentagon-found-in-a-2014-report-2015-3. – Дата доступа: 18.03.2018.

УГРОЗЫ ДЛЯ УСТРОЙСТВ, РАБОТАЮЩИХ ПОД УПРАВЛЕНИЕМ ОС ANDROID

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Бакунович Д.В.

Пачинин В.И., зав. кафедрой ИСиТ, к.т.н.,доцент

В докладе проведен анализ угроз для устройств, работающих под управлением ОС Android. На основе проведенного анализа рассмотрен ряд примеров устранения возникающих угроз и расширения возможностей программных продуктов.

В настоящее время мобильные устройства активно внедряются во все сферы жизни современного человека. Смартфоны, планшеты, электронные книги – все эти устройства уже стали неотъемлемой частью жизни. Большинство мобильных устройств работают на ОС Android. Однако эта ОС используется практически везде: начиная от домашних бытовых приборов (холодильники, телевизоры и т.д) и заканчивая различными помощниками управляемых голосом, жестами и т.д. Существуют системы “Умный дом” которые управляются при помощи голоса, жестов и приложений.

Такое широкое распространение ОС Android повлияло на очень быстрый рост различных вредоносных программ. Сначала они были весьма безобидными: показывали рекламу, воровали деньги путем рассылок платных смс, блокировали работу устройства (баннеры-вымогатели), но из-за стремительного роста Android, вредоносные программы становились все более изощренными и опасными. К примеру, развитие интеллектуальных помощников, которые могут совершать покупки в интернет магазинах, при помощи вредоносной программы можно похитить денежные средства, делать фото, включать микрофон, а также повлиять на работу всех функций, которые может использовать система. Например, была ситуация, когда система “умный дом” была заряжена трояном-вымогателем. Уязвимость в приложении “умного” термостата позволяла дистанционно поднимать или опускать температуру, а после этого требовала выкуп за возвращение контроля. Данная уязвимость, в случае отсутствия хозяев либо их сна, может привести к таким негативным последствиям, как различные болезни от переохлаждения или даже смерти домашних животных.

Для удаленного управления различными устройствами используются приложения на смартфоне. Чаще всего в таких приложениях отношение к безопасности посредственное и наиболее распространенными уязвимостями являются:

— Нет проверки целостности кода. Данная уязвимость позволяет добавлять свой вредоносный код или целиком менять различные функции в приложении.

— Нет обфускации. Это значит, что при декомпиляции приложения код никак не защищен и злоумышленник может просмотреть как реализовываются те или иные функции, что позволит потенциально добраться до дыр в системе.

— Нет технологии обнаружения root. Права суперпользователя позволят вредоносным программам полностью взять контроль над устройством.

— Нет зашифрованные логин и пароль. Доступ к внутренним файлам приложения позволит получить персональные данные пользователей.

— Нет защиты от троянов, которые помещают свое окно поверх окна приложения. Распространенная уязвимость, которая позволяет обманом вынудить ввести логин и пароль через фишинговое окно.

Например, автомобиль Tesla уже неоднократно дистанционно взламывался с практически полным контролем над мультимедийной системой автомобиля. Но такие взломы обычно строятся на основе компрометации бортового ПО самого автомобиля. Но специалисты решили атаковать официальное Android-приложение Tesla. Пользователь, после установки приложения, должен ввести имя пользователя и пароль, после которого формируется токен OAuth. Исследователи выявили, что токен хранится в незашифрованном виде в директории sandbox. Получив токен уже доступен ряд некоторых действий над автомобилем, однако одного токена недостаточно для запуска двигателя. Для того, чтобы получить полный доступ к автомобилю можно установить вирус с root доступом, который скопирует данные на необходимый адрес. Специалисты пошли

другим путем: изменили код приложения и предложили его скачать за бесплатный ужин в ресторане. Приложение сразу имело root доступ и сразу же отправляло учетные данные владельца авто на свой сервер. После этого, имея доступ к приложению, можно совершать ряд действий: заводить двигатель без ключа, открывать двери, отслеживать местоположение автомобиля и так далее. Для того, чтобы защитить свой автомобиль от взлома необходимо пользоваться официальным приложением производителя, регулярно обновлять ПО и систему, не подключаться к незнакомым wifi сетям и быть предельно осторожными при вводе учетных данных.

Таким образом, безопасность Android-приложений должна обеспечиваться в полном объеме, так как от этого можно потерять не только личные данные, но и получить различные травмы, поскольку приложения применяются уже практически во всех сферах жизни современного человека.

Список использованных источников:

1. Kaspersky.ru [Электронный ресурс] — Режим доступа: https://www.kaspersky.ru/resource-center/threats/android-mobile-threats. Дата доступа: 02.03.2018.
2. Першин Александр. Безопасность мобильных технологий в корпоративном секторе /Александр Першин — М: 2015.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ОБРАЗОВАНИИ

Институт информационных технологий БГУИР
г. Минск, Республика Беларусь

Беликов А.С. Агапкин Л.М, Чучвал А.Ю, Мирончик А.Н.

Бакунова О.М. – ст. преподаватель каф. ИСиТ, м.т.н.

Современное образование уже как множество лет остается неизменным на фоне стремительных изменений в различных сферах деятельности современного общества. Справедливо сказать, что темпы эволюции образования отстают от скорости развития общества. Получения актуального и качественного образования будущими специалистами является одной из главных проблем в обществе. Однако вопросы оценки качества образования остаются почти не исследованными, при этом большинство вузов понимает, что без создания внутренней информационно-аналитической системы проблему качества образования не решить. Эти вопросы рассматриваются в настоящей работе.

Как правило, рост контингента студентов и сотрудников, быстрое развитие вуза, непрерывно увеличивающийся объем информации в различных подразделениях – все эти факторы становятся предпосылками для создания собственной информационной системы в вузе. Также немаловажным условием является наличие общеуниверситетской компьютерной сети и программных систем по сбору информации о преподавателях, студентах, научной деятельности вуза, материально-технической базе, востребованности выпускников на рынке труда.

Однако в наше время уже недостаточно просто создание информационных подсистем по сбору информации, связанной с деятельностью вуза. Появляется необходимость в создании эффективных и производительных средств анализа полученной информации для оценки качества образования. Только так возможно преобразовать информационную систему вуза в информационно-аналитическую систему. При построении таких систем, вуз, с точки зрения проблемы качества образования, получает возможность оценивать:

качество преподавательского состава;

качество полученных студентами знаний;

состояние материально-технической базы вуза;

уровень конкурентоспособности специалистов на рынке труда.

Одним из способов решения данной проблемы, является внедрение в образовательный процесс всевозможных технических средств, обучающих систем, использование Internet-обучения.

Разработка обучающих систем в настоящее время очень популярный и интенсивно развивающийся вид научной деятельности, из-за возобновившегося интереса использованию на практике технологий искусственного интеллекта, а также интенсивного развитие Internet-технологий, которые дают возможность инженерам использовать новые производительные средства разработки, которых не было ранее. Популярность в этой области научных исследований привела к тому, что в настоящее время существует большое количество научных исследований по данной теме, разработаны сотни обучающих систем, реализованы уникальные подходы и методологии.

В настоящее время функционируют множество систем для создания обучающих структур, среди которых лидирующие места занимают искусственные нейронные сети.

Нейронные сети - вычислительные структуры, которые моделируют простые биологические процессы, обычно ассоциируемые с процессами человеческого мозга.

Основные свойства нейронных сетей:

– обучение сети, обобщение;
– параллелизм;
– представление информации в распределенном виде и дальнейшие вычисления;
– адаптивность;
– умеренное энергопотребление;
– контекстуальная обработка информации;
– обработка ошибочных ситуаций.