В результате проделанной работы была спроектирована информационная система, которая обеспечит ускорение принятия решения по выдаче займа за счет агрегирования полной информации о клиенте в единой системе и утверждения четко определяемых критериев оценки надежности заемщика. Кроме этого, уменьшится время на оформление документов, что приведет к увеличению производительности труда сотрудников и повышению удовлетворенности клиентов.

Литература.

1. Линькова В. П., Линькова А. В.,Кликунова И. В. – Описание процесса оценки кредитоспособности юридических лиц коммерческим банком с использованием CASE технологий // Известия Пензенского государственного педагогического университета им. В. Г. Белинского №24, 2011г. [Электронный ресурс]. URL: http://cyberleninka.ru/article/n/opisanie-protsessa-otsenki-kreditosposobnosti-yuridicheskih-lits-kommercheskim-bankom-s-ispolzovaniem-case-tehnologii (Дата обращения: 03.12.2015)
2. Программное обеспечение для микрофинансовых организаций и кредитных кооперативов. Российский микрофинансовый центр [Электронный ресурс]. URL: http://www.rmcenter.ru/isupport/soft/ (Дата обращения: 03.12.2015)

НЕЗАЩИЩЕННОСТЬ МОБИЛЬНЫХ ПЛАТФОРМ ANROID, IOS

Б.С. Мухамадиев, студент группы 17В41,
научный руководитель: Маслов А.В.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: john.love96@mail.ru

Каждый человек при выборе оптимального телефона руководствуется несколькими критериями, к которым относится также безопасность самой операционной системы. Пользователей настолько волнует сохранность своих персональных данных, что при покупке того же пк они сразу приобретают антивирусное программное обеспечение, потому как число вредоносных программ для смартфонов и планшетов возрастает с каждым годом.

Большинство вирусов выпускается для операционной системы android, но эксперты в последнее время замечают попытки создания вредоносного программного обеспечения и для гаджетов apple.

Основной причиной хакерских атак на ос android является открытость исходного кода операционной системы и ее распространенность на многочисленных устройствах. По данным фбр, 79% всех вирусов, обнаруженных в ходе исследования, приходилась именно на android. Для сравнения, вирусов, написанных под ios, всего 0,7% от общего числа. [1]

В основном мошеннические или вредоносные приложения осуществляют отправку платных сообщений, копируют базы контактов или сообщения для авторизации в интернет – банкинге.

троян trojan-sms.androidos.fakeplayer.a проникает на носители, замаскировавшись под установочную программу видеоплеера. Вирус рассылает сообщения на платные номера. Существует также аналогичный вирус trojan-sms.androidos.fakeplayer.b, который распространяется через платное видео.

Наиболее опасными вирусами на ос android являются [2]:

1. Golddream и noname. Эти вирусы крадут персональные данные владельца смартфона: телефонные номера контактов, даты, информацию из сообщений, а также осуществляют платную sms-рассылку.

2. Droiddream и droiddreamlight. Эти вирусы распространяются через официальный каталог приложений android market. Согласно неофициальной статистике, примерно 30% вирусов попадают в смартфоны из этого каталога. Их можно скачать в таких популярных поддельных играх, как angry birds, cut the rope, assassin's creed. После скачивания одной из игр осуществляется отправка платных сообщений, после чего у пользователя снимаются деньги со счета и крадутся все персональные данные.

3. Ggtracker. Этот вирус вместе с двумя приложениями был распространен на фишинговых сайтах. Одно из приложений увеличивало продолжительность жизни заряда батареи. Пользователи теряют не только персональные данные, но и остаются без денег на счету, поскольку вирус осуществляет платную sms-рассылку.

Можно сказать, что пользователи операционной системы android подвержены большей опасности получения на свои устройства вредоносного программного обеспечения, способного переда-

вать злоумышленникам персональные данные и деньги пользователей, чем владельцы гаджетов apple. Однако пользователи ос ios также подвержены угрозам.

В основном, пользователи apple сами являются виновниками заражения своих гаджетов, потому как хотят получить полный доступ к файловой системе ios через программы jailbreak и unlock. Вирусы для ios в большинстве случаев как раз и написаны так, что на немодифицированной операционной системе просто не запустятся, она им не даст сделать этого.

Наибольшее число пострадавших, как было замечено исследователями вопроса, получили ущерб, скачивая программы из app store. Вирусы создаются под видом приложений для ios с полезной функциональностью, которая действительно присутствует. Так как программы работают и соответствуют заявленному назначению, модераторы их пропускают. [3]

Владельцы своих гаджетов готовы скачивать и устанавливать все подряд, хотя в комментариях к такому по можно увидеть и предупреждения от других пострадавших. По мере выявления все это убирается из свободного доступа, но не всегда быстро и своевременно.

Пророссийская группа хакеров под названием “operation pawn storm” разработала новый вирус-шпион, заражающий ios устройства apple, который не может быть установлен без согласия пользователя.[4]

Вирус получает доступ к списку контактов, сообщениям, гео-локационным данным, используемым wi-fi сетям, внутренним процессам и используемым приложениям. Полученные данные пересылаются на сервера хакеров для дальнейшей обработки. Хакеры, имеющие доступ к управляющей программе могут, незаметно для пользователя, активировать микрофон и прослушать не только телефонные разговоры, но и все происходящее вокруг.

Американская компания palo alto networks, занимающаяся безопасностью в сети интернет, выявила новое семейство вредоносных программ, которые атакуют устройства корпорации apple. [5]

Целый ряд вирусов, получившее название wirelurker, были созданы в китае. Вирус атакует операционные системы компьютеров mac и iphone. Он попадает на компьютеры mac через сторонний магазин приложений для устройств apple — китайский maiyadi app store. Этот вирус автоматически устанавливается на iphone или ipad через usb-кабель, подключенный к компьютеру или ноутбуку mac. Причем вирус может проникнуть, даже если iphone или ipad не проходили процедуру jailbreak. После попадания на устройство вирус получает доступ к адресной книге и сообщениям, но конечная цель вредоносной программы пока не выявлена.

Кроме того, плохо защищены и от вредоносных вторжений ранние версий ios, особенно те, что ниже ios 6. Они лучше изучены киберпреступниками и в них больше известных уязвимостей, через которые вирусы и проникают.

Также одним из опасных вирусов является masque attack, так как он может подвергнуть заражению мобильные устройства на любой версии системы ios, не исключая самую последнюю ios 8.1.1 beta 1.[6]

Пользователю предлагается пройти по ссылке и скачать приложение. Скачивание происходит не из app store. Обычно речь идет о популярных приложениях, их новых версиях и так далее. В процессе работы оно подменяет все программы, в которых используются персонаальные данные пользователя, например, его пароли или адрес почты.[7]

Нельзя считать ос ios полностью защищенной от вирусного программного обеспечения. Устройства, функционирующие на этой платформе, с каждым днем набирают все большую популярность, поэтому хакерам становится все интереснее пытаться взломать ос ios.[8]

Пользователи могут сами обезопасить себя от вирусов, соблюдая такие меры защиты такие, как:

- не устанавливать приложения со сторонних сайтов;
- читать отзывы и описания приложений, которые хотите загрузить на смартфон;
- следить за обновлениями на свой телефон и источниками их загрузки;
- устанавливать официальные версии прошивок, ведь новая версия системы - это не только обновленный функционал, но и перекрытые лазейки для вирусов;
- не пользоваться модифицированными версиями, ведь доступ к файловой системе устройства получите не только вы, но и непрошенные гости;
- следить за работой своего антивируса.

Подводя итог, можно сказать, что ни одна из мобильных платформ не защищена от вирусных атак, поэтому владельцы должны сами следить за безопасностью своих гаджетов, работающих и на платформе android, и на ios, ведь с каждым днем выпускается все большее количество вредоносных программ.

Литература.
1. Aggle.ru [электронный ресурс] url: http://aggle.ru/ios/virusy.html (дата обращения: 16.05.2015)
2. Appleface [электронный ресурс] url: http://appleface.ru/iphone-news/virus-atakoval-ustrojstva-apple/ (дата обращения: 16.05.2015)
3. Антамошкин, о.а. модели и методы формирования надежных структур информационных систем бработки информации [текст] / антамошкин о.а., кукарцев в.в. // информационные технологии и математическое моделирование в экономике, технике, экологии, образовании, педагогике и торговле.— 2014.— № 7.— с. 51-94.
4. Железный сайт. Новости и обзоры железа [электронный ресурс] url: http://www.gelezki.info/mobile-news/2090-samyje-rasprostranjennyje-android-virusy-i-sposoby-borby-s-nimi.html (дата обращения: 16.05.2015)
5. Новости apple [электронный ресурс] url: http://apple-dev.ru/3154-novyj-virus-pod-ios-ne-trebuyushhij-jailbreak/ (дата обращения: 16.05.2015)

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОДДЕРЖКИ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ СЛОЖНЫХ ИНЖЕНЕРНЫХ ОБЪЕКТОВ

М.Е. Некрасова, студентка гр. 17ВМ51, М.А. Морозов, студент гр. 10700,
научный руководитель: Захарова А.А., к.т.н
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail:malyitka-nekrasova@mail.ru

За последнее время сформировались пути повышение эффективности научно-производственных, проектно- конструкторских и других организаций, участвующих в создании сложных технических систем. Главными являются эффективность процессов за счет внедрения амортизации проектирования и использование методов системной инженерии (управление жизненным циклом сложных объектов). Управление жизненным циклом представляет собой термин, который обозначает практику обеспечения связности всех этих состояний системы, в двух направлениях (в прямом и обратном) [1].

Управление жизненным циклом достаточно успешно зарекомендовало себя во многих государственных и частных корпорациях западных странах (NASA, DoD, Lockheed Martin, Siemens и др.). Но в России фактического внедрения подхода управлением жизненными циклами в деятельности крупных компаний не наблюдается, но ведь многие понимают, что такой подход более перспективен, чем закупка «тяжелых» систем автоматизированного проектирования (САПР) и автоматизация на их основе рабочих мест [2].

Из опроса компаний России был подведен итог, что инструменты управления жизненным циклом в своей деятельности применяет лишь небольшая часть компаний. Эта часть компаний разделилась на 5 групп, которые используют различные виды программного обеспечения для управления жизненными циклами. Более популярным программным обеспечением оказались PLM-системы (около 40%). Далее по популярности были ERP-системы (около 21%). Третье место разделили программы собственной разработки и Системы CAD/CAD/CAE (по 17%). Но и на последнем месте оказались «Управление производством»1С (около 12%) [2].

К PLM-системы относятся программы такие, как «Enovia», «Windchill», Teamcenter.

«Enovia» является продуктом французской компании Dassault Systems. Данное PLM-решение обеспечивает сервисно-ориентированную архитектуру, которая помогает дальнейшему развитию сотрудничества и инноваций. ENOVIA имеет три линии продуктов такие, как

1. ENOVIA VPLM для коллективного виртуального управления жизненным циклом сложных изделий.

2. ENOVIA MatrixOne – эта система управления бизнес-процессами совместной разработки изделий для предприятий различных отраслей промышленности.

3.ENOVIA SmarTeam - систему совместного управления данными о продукции для небольших и средних компаний, конструкторских отделов крупных предприятий [3].

«Windchill» является продуктом американской компании PTC. Windchill – это программа по управлению жизненным циклом изделия, которая разработана для работы через Интернет в распре-