Для имитации деградации функционального параметра выборки однотипных ППП использована модель в виде условного (для заданной наработки) закона его распределения. Коэффициенты модели для конкретной (прогнозируемой) выборки ППП находят по уравнениям в зависимости от заданной наработки и статистических особенностей функционального параметра этой выборки. Уравнения для интересующего типа ППП получают один раз с помощью предварительных исследований выборки данного типа ППП объемом примерно 60…100 экземпляров. О надежности прогнозируемой выборки по постепенным отказам для заданной наработки судят по вероятности нахождения функционального параметра в пределах указанных норм. Прогнозное значение вероятности находят по общепринятым правилам теории вероятности, используя построенный закон распределения функционального параметра для заданной наработки.

ПРОБЛЕМА ДЕЛЕГИРОВАНИЯ ОТВЕТСТВЕННОСТИ НА ПОЛЬЗОВАТЕЛЯ ПРИ ИСПОЛЬЗОВАНИИ ПЛАТЕЖНЫХ ПРИЛОЖЕНИЙ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

О.В. Бородюк

В настоящее время постоянно растет число пользователей, совершающих финансовые операции посредством мобильных приложений. Согласно результатам исследования, проведенного компанией «Яндекс» осенью 2016 года, 58 % пользователей смартфонов регулярно заходят на сайты и в приложения интернет-магазинов, а также из тех пользователей, которые используют смартфон для выбора товаров, большинство (72 %) имеют опыт и в оформлении заказа с телефона [1]. В связи с тем, что телефоны используются для большего количества задач, то необходимо принимать разумные меры защиты информации от вредоносных атак. Одним из важных аспектов безопасности современных мобильных устройств является наличие прав доступа уровня root. Автором было проведено исследование мобильных платежных приложений, в ходе которого проверялось запускаются ли такие приложения на устройствах с правами root и в случае, если запускаются, оповещается ли пользователь о возможных угрозах. Исследование проводилось на устройствах с операционной системой Android. В ходе исследования были протестированы популярные во всем мире приложения для совершения покупок, а также решения белорусских банков в сфере мобильного-банкинга. Всего было протестировано 17 приложений, среди которых «PayPal», «Amazon shopping», «М-банкинг» (приложение от «Беларусбанка»), «V-banking» от компании «Velcom». Все 17 приложений запустились на устройстве с правами root, 11,76 % – сократили функциональные возможности приложения, 29,41 % – оповестили пользователя о возможных рисках, 35,29 % – никак не прореагировали на наличие прав суперпользователя и 70,59 % – делегировали ответственность на пользователя добавлением новых пунктов в пользовательское соглашение. Результаты исследования показывают, что проблема делегирования ответственности на пользователя становится все более актуальной. Многие компании снимают с себя ответственность посредством добавления дополнительных пунктов в пользовательское соглашение.

Литература

1. Развитие онлайн-торговли в России: покупки со смартфонов // yandex.ru [Электронный ресурс]. – URL: https://yandex.ru/company/researches/2017/mobile_retail (дата обращения: 02.04.2018).

АРХИТЕКТУРА СИСТЕМЫ АНАЛИЗА МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ КЛАССА IaaS

А.И. Бражук

Технологическую основу уровня «Инфраструктура как услуга» (Infrastructure as a Service – IaaS) облачных компьютерных систем составляют системы виртуализации, программно-определяемые сети и хранилища, а также современные методы использования ресурсов. Системообразующий характер обуславливает актуальность проблемы моделирования

информационной безопасности данного уровня [1, 2]. Системы анализа (поддержки принятия решений), построенные на основе предметно-ориентированных моделей информационной безопасности, могут использоваться при проектировании систем защиты и анализе защищенности (детализация существующих риск-ориентированных моделей).

Архитектура системы анализа моделей информационной безопасности включает три подсистемы: база знаний (высокоуровневые и детальные модели), обеспечивающая представление и обработку знаний предметной области; подсистема анализа и защищенности (прикладные и синтезируемые модели), позволяющая потребителям создавать высокоуровневые формальные описания конкретных систем и получать рекомендации по улучшению безопасности или настройке средств защиты; подсистема интеграции с внешними источниками знаний, обеспечивающая актуальность базы знаний.

Предложенная архитектура является ориентированной на модели; также, предполагает функции автоматизированной и автоматической обработки знаний в области информационной безопасности. При этом, используемые модели являются архитектурными моделями в терминах архитектурного описания (ISO/IEC 42010); совместимы с терминологией, используемой в стандартах, литературе и реализациях средств информационной безопасности (ISO/IEC 15408-1).

Основными проблемами реализации представленной архитектуры являются построение иерархий моделей архитектур (типовые компоненты – элементы типовых компонентов) и моделей угроз (типовые угрозы – атаки, уязвимости, злоумышленники, контрмеры, метки безопасности).

Литература

1. Листопад Н.И., Олизарович Е.В., Бражук А.И. Практические аспекты внедрения облачных технологий в учреждении образования // Информатизация образования. 2014. № 2 (74). С. 55–65.

2. Управление программным обеспечением и архитектура отказоустойчивого IaaS-облака на основе универсальных узлов. / Ю.И. Воротницкий [и др.] // Электроника ИНФО. 2013. № 9. С. 21–24.

КОЛИЧЕСТВЕННЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.В. Валаханович, Л.В. Михайловская

Для лиц, принимающих решение в любой сфере деятельности, критично обеспечение оптимального соотношения доступности информации и ее надежной защиты от угроз. Первоочередной задачей управления рисками информационной безопасности становится определение наиболее значимых активов. В ходе анализа ценности активов применяются следующие методы оценки риска: в денежном выражении, вероятностный и балльный, позволяющие определить уровень уязвимости для каждой комбинации информационного актива, а также степень потенциальной опасности угроз.

Для оценки стоимости потерь используется «аддитивная модель» [1], когда информация представляется в виде конечного множества элементов и осуществляется экспертная оценка компонент исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

При использовании вероятностного метода оценивается риск вероятности обхода системы защиты, с целью чего задается формальное описание ее структуры и связности для множества элементов системы защиты и для множества элементов информационных угроз. Математическое описание связности построено на использовании теории графов и алгебраической топологии.

При оценке риска по балльному методу [2] определенным категориям угроз присваиваются значения баллов в зависимости от уровня их воздействия. Также присваивается соответствующий балл уровням уязвимости системы при действии на нее определенной