

следственных связей между уязвимостями и угрозами, в которой должен быть учтен весовой коэффициент, зависящий от стажа работы сотрудника, участвующего в построении этой матрицы.

На основе результатов оценки рисков безопасности информации, циркулирующей в информационной сети предприятия отрасли связи, полученных с использованием предложенной математической модели, может разрабатываться план и очередность выполнения мероприятий, направленных на парирование угроз, а также производиться расчет экономической эффективности этих мероприятий.

Литература

1. Бойправ В.А., Утин Л.Л., Ковалёв В.В. Актуализация разработки программного средства для порведения аудита системы защиты информации организаций электросвязи // Управление информационными ресурсами: материалы XIII Международной научно-практической конференции Минск, 9 декабря 2016 г. С. 181–182.

МЕТОД ОЦЕНКИ НАДЕЖНОСТИ ПРИКЛАДНЫХ ПРОГРАММНЫХ СРЕДСТВ НА РАННИХ ЭТАПАХ ИХ РАЗРАБОТКИ

С.М. Боровиков, С.С. Дик, А.В. Будник

Надежность современных электронных систем обеспечения безопасности, в том числе информационной, зависит от надежности используемого программного обеспечения. Известные методы оценки надежности прикладных программных средств исходят из того, что устранены ошибки языка программирования, т. е. выполнена отладка кода программы и имеются определенные данные о тестировании программы. Однако в большинстве случаев проектировщиков электронных систем безопасности и разработчиков программного обеспечения для этих систем интересует ожидаемый уровень надежности прикладных программных средств еще до написания их программного кода. Возникает вопрос, как спрогнозировать ожидаемый уровень надежности программных средств на этом этапе. Наличие соответствующего метода позволит хотя бы ориентировочно оценить ожидаемый уровень надежности будущего программного средства, что даст возможность определить общую проектную надежность электронной системы безопасности (с учетом как аппаратной части, так и программного обеспечения). Для прогнозирования ожидаемой надежности разрабатываемых прикладных программных средств предлагается подход, основанный на использовании статистической модели работоспособности программных средств. Модель базируется на взятых из отечественной и зарубежной печати обобщенных статистических данных об ожидаемом числе ошибок в разрабатываемом прикладном программном средстве в зависимости от его объема, динамики уменьшения числа ошибок от времени тестирования, профессионального опыта программистов и тестировщиков. На основе указанного подхода разработан метод прогнозирования расчетным способом ожидаемой надежности прикладных программных средств на начальных этапах их разработки.

МОДЕЛИ ДЕГРАДАЦИИ ПАРАМЕТРОВ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ И ИХ ИСПОЛЬЗОВАНИЕ ДЛЯ ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ПО ПОСТЕПЕННЫМИ ОТКАЗАМ

С.М. Боровиков, Н.И. Цырельчук, Ю.Е. Велюха, В.В. Хорошко

Деградация функционального параметра полупроводникового прибора (ППП) обуславливает появление постепенного отказа ППП. По мере развития технологии изготовления ППП причины возникновения внезапных отказов могут быть в значительной мере устранены. Постепенные отказы, отражающие внутренне присущие материалам ППП свойства, в частности старение, в принципе исключить невозможно. Этим вызван повышенный интерес к постепенным (деградационным) отказам. Для прогнозирования надежности выборки ППП по постепенным отказам необходимо располагать математической моделью деградации функционального параметра. Возникает вопрос, что собою должна представлять модель, как ее получить и как применить для прогнозирования надежности?

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