УДК 519.8

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В.Ю. Анисимов, А.В. Пинчук
(***ОАО «Корпорация «ВНИИЭМ»***)

Рассматривается методический подход к оценке уровня угрозы возникновения функционального несоответствия при использовании информационной системы по совокупности отношений целевого назначения и отношений реализуемости.
Ключевые слова: *информационная система, безопасность информационной системы, объекты информационной системы.*

Одной из важнейших качественных характеристик информационной системы является её информационная безопасность, под которой будем понимать способность системы обеспечивать выполнение информационных функций с заданными требованиями в определённых условиях своего функционирования. Чаще всего в качестве информационных функций для информационных систем рассматриваются функции доступа к информационным ресурсам, а требованиями к выполнению этих функций являются требования обеспечения конфиденциальности, целостности и доступности.

Все источники несоответствия выполнения информационных функций системы предъявляемым требованиям можно условно разделить на две группы: внутренние и внешние.

К внутренним источникам несоответствия выполняемых системой функций заданным требованиям можно отнести те, которые обусловлены, в частности, ошибками в программном обеспечении (ПО) реализации информационной системы.

Понятие ошибки в ПО для информационной системы в этих случаях аналогично понятию ошибки в конструкции физического устройства (конструктивный или производственный брак).

Способность выполнять заданные функции при наличии внутренних источников несоответствия характеризует надёжность информационной системы и её ПО.

Устранение несоответствий выполняемых операций заданным требованиям, вызванных внутренними источниками, и повышение надёжности ПО обеспечиваются его тестированием с максимально реализуемым перебором всех предусмотренных спецификацией входных данных и контролем значений всех выходных данных. Естественно, что даже для информационных систем средней сложности это может привести к необходимости использования безграничного по объёму и стоимости ресурса, поскольку необходимо протестировать все допустимые функции обработки информации для различных состояний информационного ресурса. Учитывая, что информационные системы, как правило, разрабатываются фирмами с ограниченными финансовыми ресурсами, то выявление всех возможных отказов при использовании ПО информационной системы на этапе его разработки и тестировании часто является нереализуемой задачей.

Основным средством защиты ПО от внутренних источников отказов является использование квалифицированных программистов и эффективное тестирование ПО при его разработке и использовании, что образует элементы системы защиты ПО информационной системы.

К внешним источникам функционального несоответствия информационной системы, обусловленных не состоянием её программного обеспечения (оно не подвержено старению, как, например, элементы технической системы), можно отнести те источники, которые обусловлены особенностями системного окружения (аппаратные средства и операционные системы, на которых установлена информационная система), ошибками или безответственностью пользователей, искажениями данных в каналах передачи, несанкционированным проникновением непредусмотренных данных (например, вирусов) и т. п.

Способность выполнять заданные пользователем функции при наличии внешних источников функционального несоответствия характеризует защищённость информационной системы.

Для защиты от влияния этих источников функционального несоответствия используются специальные средства защиты, например, антивирусные программы, которые образуют соответствующие элементы системы защиты ПО.

При выборе показателей и критериев для оценки безопасности информационных систем безот-

казности, важно учитывать не только источники функционального несоответствия и возможность (вероятность) их проявления, но и размер ущерба, наносимого проявлением тех или иных видов функционального несоответствия. Например, грамматическая ошибка в написании предъявляемой пользователю словесной информации без изменения её смысла наносит пользователю относительно малый ущерб, и возникновение подобного типа функционального несоответствия зачастую является приемлемым с точки зрения пользователя информационной системы. Но предоставление доступа к конфиденциальной информации пользователю без соответствующих прав доступа может привести к существенному ущербу.

Если в условиях существования внутренних и внешних источников при использовании информационной системы функциональных несоответствий не возникает, например из-за эффективной работы системы защиты, то такая ситуация характеризуется наличием лишь потенциальной опасности. К подобной ситуации можно отнести и ситуацию, когда возникающие типы функционального несоответствия не наносят существенного ущерба пользователю информационной системы или другим субъектам.

Если использование информационной системы происходит в условиях возможного внезапного или реального появления таких функциональных несоответствий, которые могут привести к существенному ущербу и для которых система обеспечения безопасности не может выработать соответствующих мер противодействия, то такая ситуация характеризуется наличием трансграничной или реальной опасности.

Угроза безопасности использования информационной системы – это ситуация использования системы в условиях реальной или трансграничной опасности возникновения таких типов функционального несоответствия, которые могут нанести или наносят пользователю неприемлемый ущерб.

Для формализации приведённых понятий и разработки методического аппарата для оценки уровня угроз безопасности информационных систем предлагается применить объектно-ориентированный подход.

Согласно такому подходу, предметная область исследований представляется множеством объектов, под которыми понимается некоторая сущность, обладающая определёнными свойствами и вступающая в отношения с другими объектами.

Всю совокупность объектов предметной области можно разделить на три класса:

– объекты информационной системы (само ПО);

– объекты системного окружения (аппаратура или операционные системы, с которыми взаимодействует информационная система, безответственные или ошибочно действующие пользователи, каналы передачи данных с соответствующими искажениями, объекты несанкционированного проникновения данных, например, вирусов и т. п.);

– объекты ресурсов, потребление которых обеспечивает условия соблюдения качественной определённости объектов исследуемой информационной системы (средства защиты от отказов, вызванных внутренними и внешними источниками).

В процессе своего функционирования объекты системы вступают в различного рода отношения с объектами внешней среды и объектами ресурсов. При этом для успешного использования информационной системы совокупность этих отношений должна быть стабильной и обеспечивать требуемый уровень надёжности и защищённости.

Как правило, отношения объектов информационной системы с объектами внешней среды определяют целевое назначение системы, а отношения с объектами ресурсов определяют условия обеспечения того или иного состояния системы, например отсутствие угроз возникновения функционального несоответствия при использовании ПО информационной системы.

В связи с этим первую группу отношений будем определять как отношения целевого назначения, а вторую группу как отношения реализуемости.

Угроза возникновения функционального несоответствия при использовании информационной системы в этом случае будет определяться как совокупность условий, приводящих к недопустимому уровню нарушений системы отношений.

В формализованном виде система отношений может быть представлена системой неравенств (уравнений):

– для отношений целевого назначения

$$\varphi_{\mu}(\{s_j^G\},\{s_l^V\}) \le 0,\ \mu = \overline{1,M};$$

– для отношений реализуемости

$$\varphi_{\eta}(\{s_j^G\},\{s_l^R\}) \le C_{\eta},\ \eta = \overline{1,N},$$

где $\{s_j^G\},\{s_l^V\},\{s_l^R\}$ – свойства объектов системы, системного окружения и ресурсов соответственно; $\varphi_{\mu}(\{s_j^G\},\{s_l^V\})$ – функциональные соотношения, определяющие условия соблюдения соответствующего отношения целевого назначения (в качестве таких условий могут выступать различ-

ного рода требования по выполнению целевых задач, условия обеспечения информационной безопасности функционирования при различного рода внешних воздействиях и т. д.); $\varphi_\eta(\{s_j^G\},\{s_l^R\})$ – функциональные соотношения, определяющие потребность в обеспечении соответствующего типа отношения ресурсов для достижения заданных значений свойств объектов системы (в качестве таких функциональных зависимостей выступают, как правило, либо функции достижимости, характеризующие уровень достижимости свойств системы при выделенных ресурсах, либо функции, определяющие потребности в тех или иных типах отношений ресурсов для достижения соответствующих значений свойств объектов системы); C_η – объёмы выделенных ресурсов для объектов системы; N – количество типов отношений ресурсов; M – число отношений целевого назначения.

Уровень нарушения отношений целевого назначения и отношения ресурсов (уровень ущерба) предлагается оценивать взвешенной суммой нарушений каждого из условий, входящих в систему отношений:

– для отношений целевого назначения

$$\sum_\mu \alpha_\mu \max[0,\varphi_\mu(\{s_j^G\},\{s_l^V\})];$$

– для отношений ресурсов

$$\sum_\eta \beta_\eta \max[0,[\varphi_\eta(\{s_j^G\},\{s_l^R\})-C_\eta]],$$

где α_μ, β_η – весовые коэффициенты, характеризующие ущерб, вызванный нарушением того или иного целевого условия или недостаточности того или иного типа ресурсов.

Обобщённый показатель уровня угроз предлагается определять как линейную комбинацию уровней нарушения отношений целевого назначения и отношений ресурсов:

$$U(\{s_j^G\},\{s_l^V\},\{s_l^R\}) = k_1\sum_\mu \alpha_\mu \max[0,\varphi_\mu(\{s_j^G\},\{s_l^V\})]+$$
$$+k_2\sum_\eta \beta_\eta \max[0,[\varphi_\eta(\{s_j^G\},\{s_l^R\})-C_\eta]],$$

где k_1, k_2 – коэффициенты, определяющие значимость нарушений целевых условий или нехватки ресурсов соответственно.

Значение $U(\{s_j^G\},\{s_l^V\},\{s_l^R\})$ определяет уровень нарушения отношений системы при фиксированном состоянии объектов системы, объектов внешней среды и объектов ресурсов.

Оценку степени угрозы возникновения отказов при использовании информационной системы для фиксированного состояния объектов системы, объектов внешней среды и объектов ресурсов предлагается проводить на основе применения показателя потенциала угрозы:

$$W(\{s_j^G\}) = \int\limits_{\substack{\{s_l^V\}\in\{S_j^V\}\\ \{s_l^R\}\in\{S_j^R\}}} U(\{s_j^G\},\{s_l^V\},\{s_l^R\})\omega_V(\{s_l^V\})\omega_R(\{s_l^R\})d(\{s_l^V\})d(\{s_l^R\}),$$

где $\omega_v(\{s_l^V\}),\omega_R(\{s_l^R\})$ – характеристики возможности действий со стороны объектов внешней среды и объектов ресурсов, характеризующихся свойствами объектов $\{s_l^V\},\{s_l^R\}$ при состоянии системы, определяющемся свойствами $\{s_j^G\}$.

В случае, если в качестве характеристик возможностей действий со стороны объектов внешней среды и объектов ресурсов используется вероятностная мера, то показатель потенциала угрозы определяется как математическое ожидание показателя уровня опасности.

Для вычисления показателя потенциала угрозы предлагается применять стандартные процедуры определения математического ожидания функции случайных величин.

В качестве функции случайных величин в данном случае выступает показатель уровня опасности, а случайными величинами – значения свойств объектов внешней среды и объектов ресурсов. В зависимости от числа случайных (псевдослучайных) параметров может быть использована процедура либо полного перебора, либо статистического моделирования.

Предложенный методический подход позволяет оценить уровень угрозы возникновения функционального несоответствия при использовании информационной системы по совокупности отношений целевого назначения и отношений реализуемости. Специфика применения такого подхода будет определяться в первую очередь спецификой формирования отношений целевого назначения и отношений реализуемости, а также спецификой предметной области использования информационной системы.

Литература

1. Майерс Г. Надёжность программного обеспечения / Г. Майерс. – М. : Мир, 1980. – 360 с.

2. Методы и средства обеспечения надёжности автоматизированных информационных систем [Электронный ресурс] / К. Мышенков, А. Васильев, А. Трофимов // Автоматизированная информационная система комбината хлебопродуктов. – АО «ИНФО», 1996. – http://www.aiskhp.ru/articles/15.htm.
3. Сизак А. С., Тарасов В. Н. Оценка защищённости и надёжности программного обеспечения персонального компьютера / А. С. Сизак, В.Н. Тарасов // Вестник ОГУ. – Технические науки, 2011. – № 1. – С. 128 – 132.

Поступила в редакцию 06.12.2013

***Владимир Юрьевич Анисимов**, д-р техн. наук, профессор, т. 8 (910) 405-54-44,*
e-mail: anisimov-vl-ur@yandex.ru
***Александр Васильевич Пинчук**, канд. воен. наук, доцент, т. 8 (903) 707-92-27,*
e-mail: Pinchuk_aleks@inbox.ru.