УДК 004.056.53

Д. Н. Генералов, О. А. Шлегель,
Н. Н. Пыркин

МОДЕЛИ ЖИЗНЕННОГО ЦИКЛА ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ БОРТОВОГО УСТРОЙСТВА С ПРОТИВОДЕЙСТВИЕМ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Предложен алгоритм разработки и выбора оптимального варианта защиты от атак инсайдера при моделировании жизненного цикла информационной системы бортовых встраиваемых устройств. Приведены результаты теоретического исследования и анализа модели с промежуточным контролем, каскадной и спиральной моделей жизненного цикла информационной системы с противодействием атакам инсайдера. Показана эффективность алгоритма выполнения этапа разработки выбора оптимального варианта защиты и противодействия угрозам инсайдера.

E-mail: kaf_pmii@tolgas.ru

Ключевые слова: *информационная система, жизненный цикл, алгоритм, несанкционированный доступ, защита информации.*

Определить требования к безопасности информационных систем для бортовых встраиваемых устройств (БВУ) можно на стадии их разработки. Под информационной системой (ИС) в настоящей работе понимаются специализированные прикладные программные реализующие процессы организации, хранения, передачи, преобразования и обработки информации; под БВУ — устройства управления, сбора и преобразования информационных сигналов для хранения, передачи, преобразования, обработки, контроля целостности и защиты информации. Для обеспечения эффективности функционирования ИС БВУ необходима защита информации от несанкционированного доступа (НСД) инсайдера.

В качестве инсайдера может выступать сторонний пользователь с авторизированным (санкционированным) или неавторизированным (несанкционированным) доступом к конфиденциальной ИС. Нарушение целостности данных, поступающих от первичных и вторичных преобразователей в устройство обработки, хранения и управления при НСД к ИС и злоумышленных действиях инсайдера, может повлечь за собой нестабильную работу, ошибочные действия и отказы БВУ.

Для предотвращения НСД и атак инсайдера необходимо разработать и выбрать оптимальный вариант защиты ИС БВУ. Для решения задачи противодействия НСД целесообразно определить соответствующую модель жизненного цикла ИС БВУ.

Существуют международные стандарты, регламентирующие способ организации процесса жизненного цикла программных средств. Стандарт ISO/IEC 12207:2008 определяет процесс организации жизненного цикла и направлен на соответствующие области применения ИС. Данный стандарт не содержит конкретных методов выполнения и решения задач, входящих в процессы жизненного цикла ИС. Это связано с тем, что регламенты стандарта ISO/IEC 12207:2008 являются общими для любых моделей жизненного цикла, методологии и технологии разработки [1]. Содержание модели жизненного цикла зависит от условий, в которых ИС создается и функционирует. Стандарт ISO/IEC 12207:2008 в большинстве случаев берется за основу при проектировании и анализе модели жизненного цикла ИС различных областей применения.

Модель жизненного цикла ИС представляет собой структуру, содержащую этапы, действия и задачи, которые реализуются в ходе разработки, функционирования и сопровождения программного обеспечения в течение всего жизненного цикла ИС: от определения требований к ИС до завершения ее использования. Определение требований к ИС является важным, например, также для ИС автомобиля семейства ВАЗ-2110, в частности для ИС бортового компьютера типа ШТАТ, контроллера типа BOSH M 1.5.4 двигателя внутреннего сгорания, системы круиз-контроля, противоугонной, охранной систем автомобиля типа ALLIGATOR.

При проектировании модели жизненного цикла ИС с противодействием НСД используется серия международных стандартов, регламентирующих жизненный цикл программного обеспечения. Модели, определяемые данными стандартами, являются взаимосвязанными, но решают совершенно разные задачи и характеризуются принципиально различными подходами к их построению.

Можно выделить две основные формальные модели жизненного цикла ИС БВУ с противодействием атакам инсайдера: каскадную (последовательную) и спиральную (итерационную). В каскадной модели переход на следующий этап проектирования происходит только тогда, когда успешно завершен предыдущий этап. В спиральной модели этапы выполняются циклически, результатом чего является реализация технических решений с помощью прототипов ИС. Каждый виток спирали характеризует фрагмент создания ИС, в нем задаются цели, характеристики проекта и определяется качество работы по проектированию защитных механизмов [2–4].

На рис. 1 приведена каскадная модель жизненного цикла ИС с усовершенствованным этапом (блок 3) разработки механизмов защиты ИС БВУ от НСД. В блоке 1 указан этап предпроектного анализа, создания исходной информационной базы, технического задания, технических условий (a_i — элементы множества исходной информационной

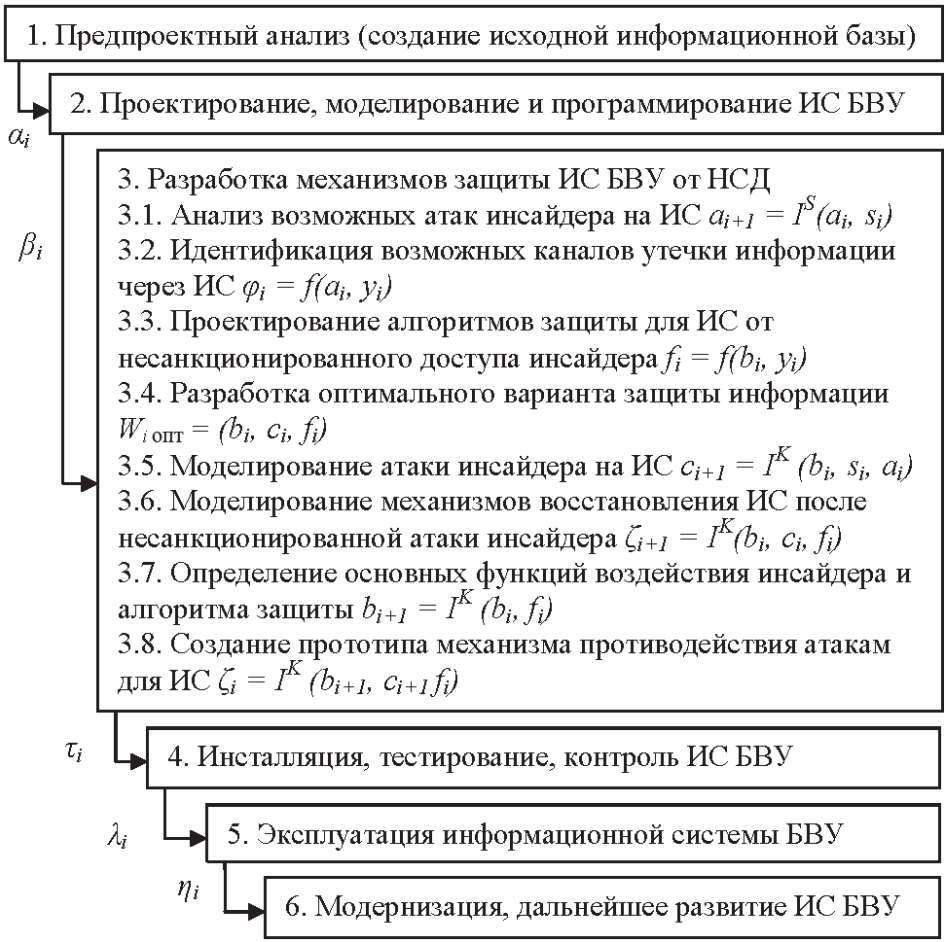

Рис. 1. Каскадная модель жизненного цикла ИС с противодействием НСД инсайдера для БВУ

базы); в блоке 2 представлен этап проектирования, моделирования и программирования ИС БВУ. В блоке 3 приведен обобщенный алгоритм разработки механизма защиты ИС БВУ от НСД. Указанный алгоритм включает в себя следующие этапы: анализ возможных атак инсайдера (a_{i+1}) на ИС; идентификацию возможных каналов утечки информации (φ_i) из ИС БВУ; проектирование алгоритмов защиты (f_i) для ИС от НСД инсайдера; разработку оптимального варианта защиты информации ($W_{i\,\text{опт}} = (b_i, c_i, f_i)$); моделирование атаки инсайдера на ИС; моделирование механизмов восстановления ИС после несанкционированной атаки инсайдера; определение основных функций воздействия инсайдера и алгоритма защиты; создание прототипа механизма противодействия атакам для ИС. Элементы β_i, τ_i, λ_i, η_i множества соответствующих промежуточных информационных баз формируются и транслируются в последующие этапы 2–6 каскадной модели (см. рис. 1).

Предпроектный анализ включает в себя формирование информационной, функциональной модели БВУ, создание исходной информационной базы. При проектировании ИС разрабатываются проектное решение и план реализации проекта. Разработка ИС заключается в создании программного кода, моделировании процессов защиты информации, моделировании НСД к ИС БВУ, тестировании системы защиты на основе проектных спецификаций. Интеграция и тестирование ИС проводятся на завершающем этапе разработки и последующей инсталляции ИС в БВУ. Может потребоваться дальнейшая модернизация ИС для обеспечения безопасности информации при возможных изменениях условий противодействий НСД, например при появлении новых каналов НСД. На каждом этапе формируется завершенный набор проектной документации и элементов β_i, τ_i, λ_i, η_i множества соответствующих промежуточных информационных баз для дальнейшей разработки ИС.

Каскадная модель жизненного цикла ИС с усовершенствованным этапом (блок 3, см. рис. 1) разработки механизмов защиты ИС БВУ от НСД может быть использована для решения инженерных задач, в том числе связанных с обеспечением безопасности информационной базы.

При разработке авторской программы защиты типа Auto Security Mobile v.1.0 (ASM v.1.0) от НСД и атак инсайдера для бортового компьютера, охранной и противоугонной системы автомобиля семейства ВАЗ-2110 была использована каскадная модель, адаптированная к условиям обеспечения защиты информации. Отличительными элементами по сравнению с известным вариантом каскадной модели являются усовершенствованный этап (блок 3, см. рис. 1) разработки защиты и модифицированные промежуточные информационные базы в виде множеств β_i, τ_i, λ_i, η_i для основных этапов 2–6 жизненного цикла ИС БВУ.

На рис. 2 приведен алгоритм разработки и выбора оптимального варианта защиты от атак инсайдера при моделировании жизненного цикла ИС БВУ. Алгоритм включает в себя: анализ возможных атак $a_{i+1} = I^S(a_i, s_i)$ (I^S — зависимость возможных атак a_{i+1} от параметров функционирования ИС, a_i — аппаратный модуль, на который направлена атака инсайдера, s_i — программный модуль, на котором выполняется НСД); идентификацию каналов утечки информации $\varphi_i = f(a_i, y_i)$ (f — нелинейная зависимость идентифицируемых каналов φ_i утечки информации от параметров аппаратных модулей, a_i и y_i — устройства интерфейса аппаратной части БВУ (бортового компьютера, контроллера двигателя внутреннего сгорания, микроконтроллера круиз-контроля и контроллера противоугонного модуля автомобиля)); алгоритмы защиты для ИС $f_i = f(b_i, y_i)$ (f — линейная зависимость выходных функций f_i от параметров b_i — входных воздействий инсайдера при НСД

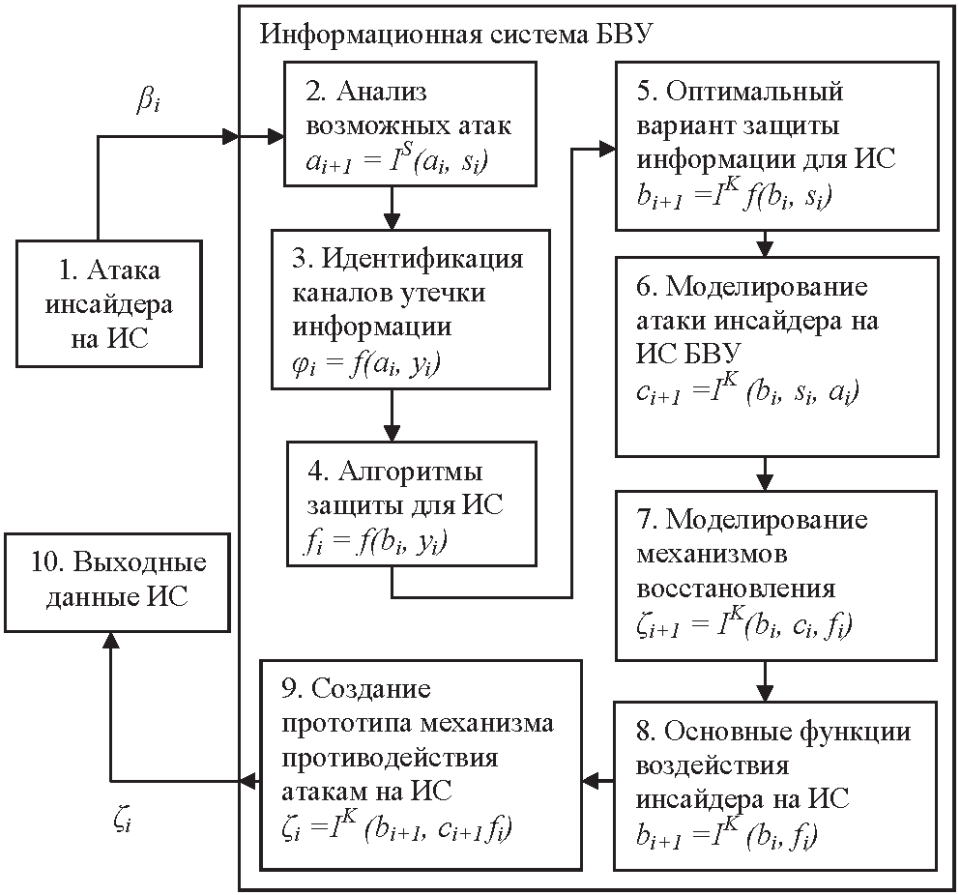

Рис. 2. Алгоритм разработки и выбора оптимального варианта защиты от атак инсайдера при моделировании жизненного цикла информационных систем бортовых встраиваемых устройств

и устройств интерфейса y_i портов аппаратной части БВУ); разработку оптимального варианта защиты информации для ИС $b_{i+1} = I^K f(b_i, s_i)$ (I^K — математическая зависимость информационных процессов b_{i+1} защиты информации для ИС от параметров входных воздействий b_i инсайдера при НСД и программных модулей s_i ИС); моделирование атаки инсайдера на ИС БВУ $c_{i+1} = I^K(b_i, s_i, a_i)$ (I^K — регрессионная зависимость информационных процессов c_{i+1} при НСД от входных воздействий b_i инсайдера, программных модулей s_i и аппаратных модулей a_i ИС); создание прототипа механизма противодействия атакам на ИС $\zeta_i = I^K(b_{i+1}, c_{i+1}, f_i)$ (I^K — зависимость параметров входных воздействий b_i от информационных процессов ζ_i при НСД от контрольных параметров информационных процессов b_{i+1} защиты информации, параметров информационных процессов c_{i+1} при атаке инсайдера и выходных функций f_i интерфейса (портов) аппаратной части БВУ); ζ_i — основные функции воздействия инсайдера на ИС

$b_{i+1} = I^K(b_i, f_i)$ (I^K — зависимость параметров входных воздействий от информационных параметров b_i и выходных функций f_i интерфейса); моделирование механизмов восстановления $\zeta_{i+1} = I^K\ (b_i, c_i, f_i)$ (I^K — функция параметров входных воздействий от информационных параметров ζ_i при атаках инсайдера).

Каскадная модель жизненного цикла ИС с усовершенствованным этапом 3 (см. рис. 1) разработки механизмов защиты ИС БВУ от НСД и модифицированными промежуточными информационными базами для основных этапов жизненного цикла позволяет решить задачу обеспечения безопасности.

Недостатком усовершенствованного варианта каскадной модели жизненного цикла ИС БВУ является то, что процесс создания ИС недостаточно интегрируется в каскадную схему, поэтому возникают потребности в переходе к предыдущим этапам в целях улучшения параметров разработки, ранее принятых решений, выборе оптимального варианта защиты от НСД и отсутствии возможности межэтапных корректировок. Устранение указанного недостатка может быть выполнено при использовании расширенной модели с промежуточным контролем выполняемых этапов, операций и анализа результата моделирования (рис. 3).

Модель жизненного цикла ИС БВУ с промежуточным контролем может быть представлена как самостоятельная так же, как вариант каскадной модели. Модель с промежуточным контролем характеризуется повышенной надежностью, расширенным периодом разработки и межэтапными корректировками [5].

В процессе апробации стандартной каскадной модели жизненного цикла ИС БВУ на базе охранной системы ALLIGATOR для автомобиля семейства ВАЗ-2110 (проектирование программы ASM v.1.0) выявлены определенные недостатки. В частности, при идентификации новых информационных каналов и видов атак инсайдера при использовании стандартной каскадной модели достаточно сложно вносить соответствующие изменения в разрабатываемую программную часть ASM v.1.0. Это объясняется тем, что необходимое сопоставление итоговых результатов можно выяснить только после завершения этапов проектирования. Для снижения отрицательного эффекта данного недостатка была использована спиральная модель жизненного цикла (ИС с программной частью ASM v.1.0).

В спиральной модели жизненного цикла имеется возможность корректировки этапов непосредственно во время разработки ИС БВУ и проектирования на любом этапе создания ИС вне зависимости от завершения предыдущих этапов [6]. Каждый виток спиральной модели означает формирование варианта ИС. Для обеспечения организации

Рис. 3. Модель жизненного цикла ИС с промежуточным контролем с противодействием НСД на этапе разработки

оптимального варианта защиты информации в спиральной модели жизненного цикла дополнительно сформирована спираль 3-го этапа разработки ИС БВУ. В данной спиральной модели усовершенствован этап (блок 3, рис. 4) разработки защиты и модифицированы промежуточные информационные базы в виде множеств β_i, τ_i, λ_i, η_i для основных этапов 2–5 жизненного цикла ИС БВУ.

При использовании спиральной модели ИС с указанными отличиями от стандартной спиральной модели определяли процессы инсталляции, тестирования, контроля, сопровождения ИС БВУ с противодействием НСД. При таком подходе инсталляция происходит фактически непрерывно. При этом число ошибок в процессе инсталляции ИС в БВУ сводится к минимуму. Итерационное проектирование (ряд по-

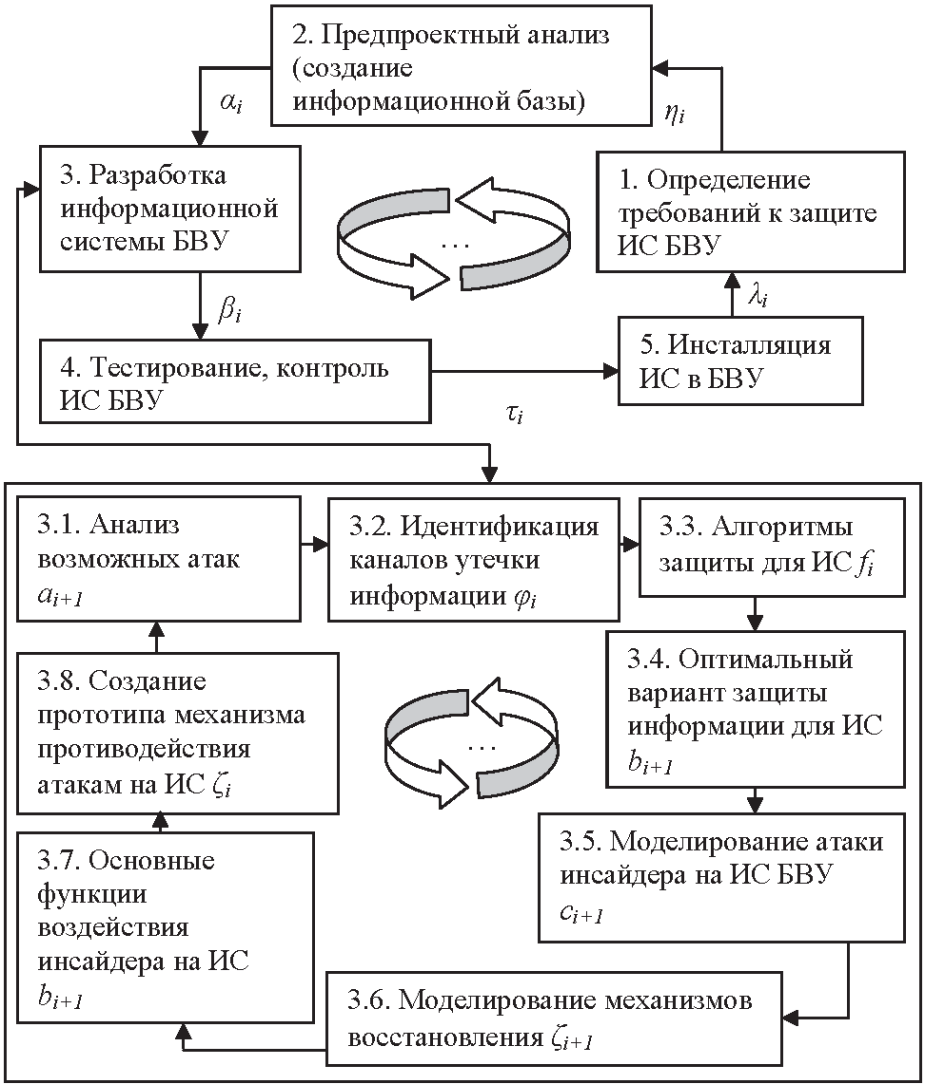

Рис. 4. Спиральная модель жизненного цикла ИС бортовых встраиваемых устройств с противодействием НСД

вторений операции, использующей результат предыдущей аналогичной операции) обеспечивает возможность внесения изменения на любом этапе разработки, упрощая повторное использование компонентов и механизмов защиты при дальнейшей разработке ИС с противодействием атакам инсайдера. Итерационное проектирование способствует идентификации ранее разработанных модулей ИС, что необходимо для упрощения поэтапного анализа проектирования [8]. Анализ проекта после проведения нескольких начальных итераций позволяет выявить общие многократно используемые компоненты, которые на последующих итерациях будут совершенствоваться и модернизироваться.

Рассмотренные модели разработки ИС с противодействием атакам инсайдера позволяют выбрать модель ИС для конкретного БВУ, а именно ИС для бортового компьютера, контроллера двигателя внутреннего сгорания, системы круиз-контроля и противоугонной системы автомобиля.

Множество m вариантов моделей жизненного цикла программной части ASM v.1.0 $A = \{a_1, a_2, \ldots, a_m\}$ рассмотрено применительно к ИС с противодействием НСД для бортового компьютера ШТАТ автомобилей семейства ВАЗ-2110. Различные модели жизненного цикла ИС БВУ имеют равнозначные требования к основным этапам по времени выполнения и стоимости работ. Особыми требованиями при выборе оптимальной модели жизненного цикла для ИС БВУ являлись: итерационное свойство этапов разработки (возможность возврата к предыдущему этапу работ), структура (определяемая технологическими особенностями разработки и техническими условиями эксплуатации ИС БВУ), риски (возможность снижения рисков на этапе проектирования ИС БВУ), логика (логическая последовательность действий механизмов защиты от атак инсайдера и основных алгоритмов работы ИС БВУ).

Модели могут быть охарактеризованы по четырем требованиям (критериям): C_1 — итерация к предыдущему этапу проектирования; C_2 — структура алгоритмов защиты; C_3 — риски при программной части ASM v.1.0; C_4 — логическая последовательность действий от атак инсайдера.

В качестве критерия оценки (C) ИС БВУ может быть рассмотрено нечеткое множество [7]

$$C = \{\mu_C(a_1)/a_1; \mu_C(a_2)/a_2; \ldots; \mu_C(a_m)/a_m\},$$

где $\mu_C(a_1) \in [0, 1]$ — оценка варианта a_1 по критерию C, которая характеризует степень соответствия варианта требованию, определенному критерием C.

Рассмотрим n требований C_j, $j = \overline{1, n}$, при этом считаем, что вариант удовлетворяет требованию C_1 и $C_2 \ldots$ и C_n. Тогда правило для выбора наилучшего варианта модели ИС с противодействием НСД может быть записано в виде пересечения соответствующих множеств:

$$D = C_1 \cap C_2 \cap \ldots \cap C_n.$$

Операции пересечения нечеткого множества соответствует операция min, выполняемая над функциями принадлежности:

$$\mu_D(a_j) = \min_{j=1,n} \mu_{C1}(a_j), \quad j = \overline{1, m}. \tag{1}$$

В качестве лучшего выбирается вариант a^*, имеющий наибольшее

значение функции принадлежности:

$$\mu_D(a^*) = \underset{j=1,m}{\max}\, \mu_D(a_j). \qquad (2)$$

На основе экспертной оценки, выполненной группой специалистов в области проектирования, эксплуатации ИС и обучения персонала, получены следующие усредненные данные, характеризующие степень соответствия заданным требованиям (техническое задание, технико-экономическое обоснование, технические условия) к программной части ASM v.1.0 для ИС БВУ:

$$C_1 = \{0{,}9/a_1;\ 0{,}7/a_2;\ 0{,}8/a_3\};\ C_2 = \{0{,}8/a_1;\ 0{,}9/a_2;\ 0{,}6/a_3\};$$

$$C_3 = \{0{,}7/a_1;\ 0{,}8/a_2;\ 0{,}9/a_3\};\ C_4 = \{0{,}8/a_1;\ 0{,}6/a_2;\ 0{,}7/a_3\}.$$

В соответствии с правилом выбора модели жизненного цикла получено

$$D = \{\min(0{,}9;\ 0{,}8;\ 0{,}7;\ 0{,}8/a_1);\ \min(0{,}7;\ 0{,}9;\ 0{,}8;\ 0{,}6/a_2);$$

$$\min(0{,}8;\ 0{,}6;\ 0{,}9;\ 0{,}7/a_3)\} = \{0{,}7/a_1;\ 0{,}6/a_2;\ 0{,}6/a_3\}.$$

Дальнейшая разработка и выбор оптимальной модели жизненного цикла программной части ASM v.1.0 проведены по мультипликативному показателю качества, который вычисляется путем умножения частных показателей с учетом их весовых коэффициентов:

$$Q = \prod_{j=1}^{m} \overline{q_j}^{w_j}. \qquad (3)$$

Расчет мультипликативного показателя (3) свидетельствует о том, что наилучшим вариантом является спиральная модель жизненного цикла ИС БВУ с усовершенствованным этапом разработки защиты и модифицированными промежуточными информационными базами:

$$a_1 = \{0{,}9;\ 0{,}8;\ 0{,}7;\ 0{,}8\}.$$

Анализ моделей жизненного цикла ИС БВУ на примере программной части ASM v.1.0 показывает, что спиральная модель с усовершенствованным этапом разработки защиты и модифицированными промежуточными информационными базами является предпочтительной при разработке ИС с противодействием НСД для бортового компьютера типа ШТАТ. Таким образом, в каждом отдельном случае проектирования и инсталляции ИС в БВУ можно найти оптимальную (предпочтительную) модель жизненного цикла ИС.

Для противодействия атакам инсайдера может быть определено достаточное число решений. Например, Антивирус Касперского®Mobile предназначен для защиты на базе операционных систем от вредо-

носного программного обеспечения инсайдера. Также в качестве примера можно рассмотреть систему для защиты информации от НСД типа СТРАЖ NT, которая предназначена для комплексной защиты информационных ресурсов от атак инсайдера при работе в автоматизированных ИС на базе ПК. Указанные системы защиты актуальны при использовании на ПК и в корпоративных сетях. Однако предотвратить НСД, например в бортовом компьютере автомобиля семейства ВАЗ-2110, с помощью таких систем защиты не представляется возможным, так как программные и аппаратные части ПК и бортового встраиваемого устройства имеют различия в программно-аппаратной части. Разработанный программный модуль ASM v.1.0 с механизмом защиты информационной системы от атак инсайдера может быть интегрирован в ИС бортового компьютера типа ШТАТ, тем самым дополняя его функциональность и расширяя его возможность противодействия НСД.

Проведенные по уравнениям (1)–(3) расчеты показывают эффективность сформированного алгоритма выполнения этапа разработки и выбора оптимального варианта защиты с противодействием атакам инсайдера на ИС БВУ при моделировании ее жизненного цикла на основе спиральной модели.

Спиральная модель с усовершенствованным этапом разработки варианта защиты и модифицированными промежуточными информационными базами позволяет решить задачу обеспечения безопасности с модификацией на каждой стадии итерации и корректировкой этапов непосредственно во время разработки ИС БВУ. Одновременно могут корректироваться критические параметры эффективности разработки оптимального варианта защиты, что в случае каскадной модели доступно только перед инсталляцией ИС в БВУ. При итерационном подходе для спиральной модели имеется возможность совершенствования процесса разработки в конце каждой итерации; это позволяет оценивать, что должно быть модифицировано в процессе проектирования, и выполнять модернизацию на следующей итерации. Каскадная модель может быть использована для решения инженерных задач, связанных с обеспечением безопасности ИС БВУ.

При разработке авторской программы защиты от атак инсайдера Auto Security Mobile v.1.0 для бортового компьютера типа ШТАТ и охранной системы автомобиля семейства ВАЗ-2110 была использована спиральная модель с расширением модуля (этапа) проектирования разработки в части механизмов с противодействием атакам инсайдера и модифицированными промежуточными информационными базами. Данная модель оказалась более эффективной по времени и затратам ресурсов алгоритмизации и программирования по сравнению с каскадной моделью жизненного цикла ИС БВУ.

СПИСОК ЛИТЕРАТУРЫ

1. Генералов Д. Н., Шлегель О. А. Идентификация скрытых каналов утечки информации при инсталляции инсайдера в мобильное устройство // Вестник Поволжского государственного университета сервиса. Серия "Экономика". – 2009. – № 6.
2. Скотт Ф. У. Принципы проектирования и разработки программного обеспечения: Учебный курс MCSD: Пер. с англ. – М.: ТД "Русская редакция", 2000. – 608 с.
3. Уокер Ройс. Управление проектами по созданию программного обеспечения. – М.: Изд-во "Лори", 2002. – 424 с.
4. Huskamp J. C. Covert communications channels in timesharing systems / J.C. Huskamp // Technical Report Ph.D. Thesis, University of California, Berkley, California, 1978.
5. Генералов Д. Н. Математическое моделирование процессов защиты информации для мобильных устройств // Всеросс. науч.-техн. конф. "Современные сервисные технологии. Научные исследования аспирантов и молодых ученых". – Самара: Изд-во РГУТИС, 2009.
6. Ерохина Л. И., Шлегель О. А., Молясы М., Рекуч В. Синергетика и динамические экономические математические модели // Синергетика природных, технических и социально-экономических систем: Сб. статей Междунар. науч.-техн. конф. Ч. II. – Тольятти: Изд-во ТГУС, 2007. – 175 с.
7. Molasy M. Transfer and processing, coding of industrial / Marian Molasy, L. Erokhina, O. Shlegel, A. Shlegel, M. Molasy // SYSTEMS, Journal of Transdisciplinary Systems Science. – 2007 Wroclaw University of Technology, Poland. – Vol. 12. No. 3.

Статья поступила в редакцию 24.08.2009

Дмитрий Николаевич Генералов родился в 1986 г., окончил в 2009 г. Поволжский государственный университет сервиса (ПВГУС). Аспирант ПВГУС. Автор 36 научных работ в области информационных технологий и систем в автостроении, приборостроении.

D.N. Generalov (b. 1986) graduated from the Povolzh'e State University of Service (town Togliatti) in 2009. Post-graduate of the Povolzh'e State University of Service. Author of 36 publications in the field of information technologies and systems in automobile building and instrument engineering.

Олег Александрович Шлегель родился в 1953 г., окончил в 1974 г. Тольяттинский государственный университет (ТГУ). Д-р техн. наук, профессор, зав. кафедрой "Прикладная математика и информатика" Поволжского государственного университета сервиса. Автор более 300 научных работ в области прикладной математики, информационных технологий и систем в авто- и приборостроении.

O.A. Shlegel' (b. 1953) graduated from the Togliatti State University in 1974. D. Sc. (Eng.), professor, head of "Applied Mathematics and Information Technology" department of the Povolzh'e State University of Service (town Togliatti). Author of more than 300 publications in the field of applied mathematics, nformation technologies and systems in automobile building and instrument engineering.

Николай Николаевич Пыркин родился в 1962 г., окончил в 1985 г. Тольяттинский государственный университет (ТГУ). Преподаватель кафедры “Прикладная математика и информатика” Поволжского государственного университета сервиса. Автор трех научных работ в области информационных технологий, моделирования социально-экономических и технических систем.

N.N. Pyrkin (b. 1962) graduated from the Togliatti State University in 1985. Lecturer of “Applied Mathematics and Information Technology” department of the Povolzh’e State University of Service (town Togliatti). Author of 3 publications in the field of information technologies, simulation of social-economical and technical systems.

Вниманию авторов

В журнале “Вестник МГТУ им. Н.Э. Баумана. Серия “Приборостроение” публикуются материалы по следующим основным направлениям:

- дифференциальные уравнения, динамические системы и оптимальное управление (математика);
- механика систем (механика);
- электромеханика и электрические аппараты (электротехника);
- приборостроение, метрология и информационно-измерительные приборы и системы;
- информатика, вычислительная техника и управление;
- навигация и управление воздушным движением (транспорт);
- электроника;
- радиофизика;
- оптика;
- лазерная физика.