УДК 621.382, 26

ОСНОВНЫЕ ПРИНЦИПЫ ОЦЕНКИ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ

О.В. Трубиенко@, к.т.н., зав. кафедрой
С.И. Журавлев, к.т.н., доцент
В.И. Сороковиков, преподаватель
Д.В. Набатов, аспирант
А.А. Худяков, преподаватель
А.В. Крылов, преподаватель

Московский технологический университет (МИРЭА),
Институт комплексной безопасности и специального приборостроения, Москва, 107996 Россия
Автор для переписки, e-mail: trubienko_ov@mgupi.ru

В статье рассмотрены и проанализированы основные принципы, гарантирующие безопасность программного обеспечения (ПО), используемого при эксплуатации информационных систем. Данные принципы сопоставлены с требованиями Общих критериев для определения того, насколько эти принципы совпадают с современными направлениями в области безопасности информации. Рассмотрены преимущества информационного моделирования с использованием подходов Общих критериев (ОК). Информационное моделирование является удобным и наглядным средством для представления требований ОК. Схемы информационного моделирования в статье показывают движение информации в ИТ и среду безопасности информации (угрозы, политики безопасности информации). Классифицированные, иерархические и взаимоувязанные требования ОК позволяют в полной мере описывать любые документы ОК (профили защиты, задания по безопасности) схемами информационного моделирования.

Ключевые слова: программное обеспечение, принципы обеспечения безопасности, система проверки безопасности ПО, потенциальные скрытые ошибки программного обеспечения, Общие критерии.

BASIC PRINCIPLES OF ESTIMATION OF SOFTWARE SAFETY AND PROSPECTS OF THEIR DEVELOPMENT

O.V. Trubienko,
S.I. Zhuravlev,
V.I. Sorokovikov,
D.V. Nabatov,

A.A. Khudyako,
A.V. Krylov

Moscow Technological University (MIREA),
Moscow, 107996 Russia
Institute of Integrated Security and Special Instrumentation
@Corresponding author e-mail: trubienko_ov@mgupi.ru

The article describes and analyzes the basic principles of security software used in the operation of information systems. These principles are compared with the requirements of the Common Criteria (CC) for determining whether these principles coincide with the contemporary trends in the field of information security. Benefits of information modeling also considered using the Common Criteria approach. Information Modeling - a convenient and intuitive way for filing requirements CC. Schemes of information modeling in the article show the movement of information in the IT and information security environment (threats, information security policy). Classified, hierarchical and interrelated requirements CC allow you to fully describe any documents CC (protection profiles, security target) schemes of information modeling.

Keywords: principles on security software, security audit system, potentially hidden software errors, Common Criteria.

Введение

В современных условиях трудно переоценить необходимость повышения безопасности программного обеспечения (ПО). В быту мы часто сталкиваемся с устройствами, в которых программное обеспечение работает неустойчиво. Можно привести множество примеров, когда, например, в сотовых телефонах ПО функционирует со сбоями (у одного из авторов на телефоне, созданном компанией NOKIA, постоянно «зависает» операционная система Windows, что приводит к отключению телефона). Это, безусловно, влияет на потребительскую ценность подобных продуктов информационных технологий (ИТ), однако, если ненадежное ПО используется в атомной промышленности, энергетике, в военных отраслях или на иных критически важных объектах, то значимость обеспечения безопасности ПО возрастает [1]. К безопасности информации таких объектов предъявляются особые требования [1], [2].

С целью повышения безопасности информации в статье предлагается использовать моделирование процессов в ИТ для определения «узких мест» в них, а также иных возможных уязвимостей, не прибегая к дорогостоящим натурным испытаниям [2].

Наиболее представительно и показательно такое моделирование в области защиты информации можно продемонстрировать с использованием Общих критериев (между-

[1]Руководящий документ ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

[2]Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 14 марта 2014 г. № 31 г. Москва «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

народный стандарт ISO/IEC 15408). Для обоснования выбора Общих критериев (ОК) в качестве основы для информационного моделирования авторы провели сравнительный анализ некоторых современных тенденций (принципов обеспечения безопасности ПО) в области защиты информации и требований ОК. Сравнение проведено с учетом моделей на основе ОК [3], а также некоторых руководящих документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) России, основанных на применении ОК[3], [4], [5].

Сопоставление принципов безопасности ПО с требованиями современных систем обеспечения безопасности

Для проведения исследования по сопоставлению некоторых современных показателей защищенности ПО с требованиями ОК наиболее представительные подходы обеспечения безопасности ПО выбраны из литературы [4–11]. Данные показатели приведены в таблице в столбце 3 «Современные принципы обеспечения безопасности ПО», а наименования требований ОК – в столбцах 1 и 2.

Анализ данных, представленных в таблице, показывает, что выбранные авторами принципы (третий столбец), с одной стороны, недостаточны в сравнении с ОК, но, с другой стороны, расширяют требования ОК. Однако гибкость принципов ОК состоит в том, что ОК не ограничиваются какими-либо правилами и могут включать любые расширения требований, а в основу ОК положены базовые требования, описывающие основные архитектурные особенности современных информационных технологий.

Таким образом, результаты проведенного авторами исследования говорят об очевидной показательности и представительности ОК для того, чтобы их использовать в основе информационного моделирования. Тот факт, что требования ОК классифицированы, также добавляет уверенности в перспективности ОК как хорошей основы для информационного моделирования.

Возможности и перспективы применения Общих критериев

Международный стандарт ISO/IEC 15408 (русский аутентичный аналог ГОСТ Р ИСО/МЭК 15408)[6] состоит из трех частей:

- первая часть описывает концепцию применения ОК;
- во второй части рассмотрены функциональные требования безопасности для ИТ;
- в третьей части стандарта представлены требования доверия к безопасности, описывающие меры, которые должны быть выполнены для того, чтобы изделия ИТ могли безопасно функционировать; эти меры связаны с безопасным проектированием изделия ИТ, безопасной разработкой, тестированием, поставкой, инсталляцией и т.д., а также требуют проведения испытаний изделия ИТ и подготовки документов – свидетельств разработки, испытаний и оценки изделия ИТ.

---

[3]Требования к средствам антивирусной защиты. Утверждены 20 марта 2012 г. Федеральной службой по техническому и экспортному контролю России.

[4]Требования к системам обнаружения вторжений. Утверждены 6 декабря 2011 г. Федеральной службой по техническому и экспортному контролю России.

[5]Требования к средствам доверенной загрузки. Утверждены 27 сентября 2013 г. Федеральной службой по техническому и экспортному контролю России.

[6]ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

В Общих критериях существуют такие понятия, как профиль защиты (ПЗ) и задание по безопасности (ЗБ). ПЗ и ЗБ – это документы, в которых описаны требования к объекту оценки (к некоторому изделию ИТ). В ПЗ в наиболее общем виде предъявляются требования для типа изделия, а в ЗБ в подробном виде описываются конкретные требования для конкретного изделия ИТ.

Авторы предлагают описывать ПЗ и ЗБ в виде информационных моделей, основанных на известной методологии *Integrated DEFinition (IDEF)*.

Сопоставление основных принципов обеспечения безопасности ПО и требований доверия к безопасности (ТДБ) из ОК по наивысшему 7-му оценочному уровню доверия к безопасности (ОУД7)

Общие критерии		**Современные принципы обеспечения безопасности ПО**
Классы ТДБ из ОК (с их краткими именами)	**Компоненты ТДБ из ОК**	
1	**2**	**3**
ACM: Управление конфигурацией (УК)	Полная автоматизация УК	Статистический учет и ведение системных журналов во всех процессах разработки ПО с целью контроля технологической безопасности
	Расширенная поддержка УК с поэтапным контролем разработок	Последовательная многоуровневая фильтрация программных модулей – процедура осуществляется в процессе создания модулей с применением функционального дублирования разработок и поэтапного контроля
	Охват УК инструментальных средств разработки	Использование только сертифицированных и выбранных в качестве единых инструментальных средств разработки программ для новых технологий обработки информации и перспективных архитектур вычислительных систем
ADO: Поставка и эксплуатация	Предотвращение модификации при поставке	–
	Процедуры установки, генерации и запуска	–
ADV: Разработка	Формальная функциональная спецификация	–
	Формальный проект верхнего уровня	–
	Структурированная реализация функций безопасности	Достижение технологической безопасности ПО в процессе его разработки – обеспечивается за счет реализации процедур и мероприятий
	Минимизация сложности	Достаточность защищенности программ – отражает необходимость поиска наиболее эффективных и надежных мер безопасности при одновременной минимизации их стоимости
	Полуформальный проект нижнего уровня	–
	Формальная демонстрация соответствия спецификации	–
	Формальная модель политики безопасности объекта оценки	Заблаговременность разработки средств обеспечения безопасности и контроля производства ПО – заключается в предупредительном характере мер обеспечения технологической безопасности работ в интересах недопущения снижения эффективности системы безопасности процесса создания ПО
AGD: Руководства	Руководства администратора	Документируемость технологии создания программ – подразумевает разработку пакета нормативно-технических документов по контролю программных средств на наличие преднамеренных дефектов
	Руководство пользователя	

1	2	3
ALC: Поддержка жизненного цикла	Достаточность мер безопасности	Планируемость применения средств безопасности программ – предполагает перенос акцента на совместное системное проектирование ПО и средств его безопасности, планирование их использования в предполагаемых условиях эксплуатации
	Измеримая модель жизненного цикла	–
	Соответствие всех частей объекта оценки стандартам реализации	–
ATE: Тестирование	Строгий анализ покрытия тестами	–
	Тестирование на уровне реализации	Регламентация технологических этапов разработки ПО – включает упорядоченные фазы промежуточного контроля, спецификацию программных модулей и стандартизацию функций и формата представления данных
	Упорядоченное функциональное тестирование	Обеспечение технологической безопасности на этапах стендовых и приемосдаточных испытаний за счет реализации процедур и мероприятий
	Полное независимое тестирование	–
AVA: Оценка уязвимостей	Систематический анализ открытых каналов нарушения безопасности	Обоснованность средств обеспечения безопасности ПО - заключается в глубоком научно-обоснованном подходе к принятию проектных решений по оценке степени безопасности, прогнозированию угроз безопасности, всесторонней априорной оценке показателей средств защиты
	Анализ и тестирование опасных состояний	Автоматизация средств контроля управляющих и вычислительных программ – обеспечивается проверкой и поиском на наличие в ПО преднамеренных дефектов
	Оценка стойкости функций безопасности	Гибкость управления защитой программ – требует от системы контроля и управления обеспечением безопасности ПО способности к диагностированию, опережающей нейтрализации, оперативному и эффективному устранению возникающих угроз
	Стойкость алгоритмов шифрования	–
Это требование нужно отнести ко всем перечисленным выше требованиям ОК		Комплексность обеспечения безопасности ПО – предполагает рассмотрение проблемы безопасности информационно-вычислительных процессов с учетом всех структур КС, возможных каналов утечки информации и несанкционированного доступа к ней, времени и условий их возникновения, комплексного применения организационных и технических мероприятий
–		Блокирование несанкционированного доступа соисполнителей и абонентов государственных и негосударственных сетей связи, подключенных к стендам для разработки программ
–		Типизация алгоритмов, программ и средств информационной безопасности – обеспечивается информационной, технологической и программной совместимости на основе максимальной их унификации по всем компонентам и интерфейсам
–		Централизованное управление базами данных проектов ПО и администрирование технологии их разработки – обеспечивается жестким разграничением функции, ограничением доступа в соответствии со средствами диагностики, контроля, защиты

Предлагаемые особенности моделирования процессов обеспечения безопасности информации следующие. Каждый прямоугольник в модели означает некое действие в процессе функционирования моделируемой системы или в нашем случае это может быть описание действий с информационными потоками, необходимых для реализации того или иного требования по безопасности. Далее каждый прямоугольник может декомпозироваться, представляя некоторые поддействия со своими взаимосвязями. Таким образом, моделирование состоит из процессов декомпозиции действий и объединяющих их связей до необходимого уровня.

На рис. 1 приведена диаграмма информационной модели (в данном случае для системы защиты персональных данных), а вся модель показывает всю среду безопасности для данной системы и, кроме того, всю среду функционирования через моделирование потоков данных (бизнес-процессов) – чего нет в Общих критериях.

В модели на входе в любой прямоугольник (его левая сторона) стрелочкой указан поток информации, с которым будет производиться какое-либо действие, указанное в прямоугольнике. Информационная стрелка может входить в прямоугольник и сверху: в таком случае информация является управляющей для данного действия и может не обрабатываться соответствующим действием, а использоваться для осуществления этого действия. В качестве управляющих потоков для действия в прямоугольнике используется информация о предположениях, политиках и угрозах, указанная стрелками, которые входят в прямоугольник сверху. На выходе прямоугольника (его правая сторона) представлены выходящие стрелки, определяющие информацию на выходе. Связи на входе и на выходе между прямоугольниками являются зависимостями между требованиями, которые также предусматриваются стандартом ISO/IEC 15408. Кроме того, зависимости определяют информационные потоки в системе.

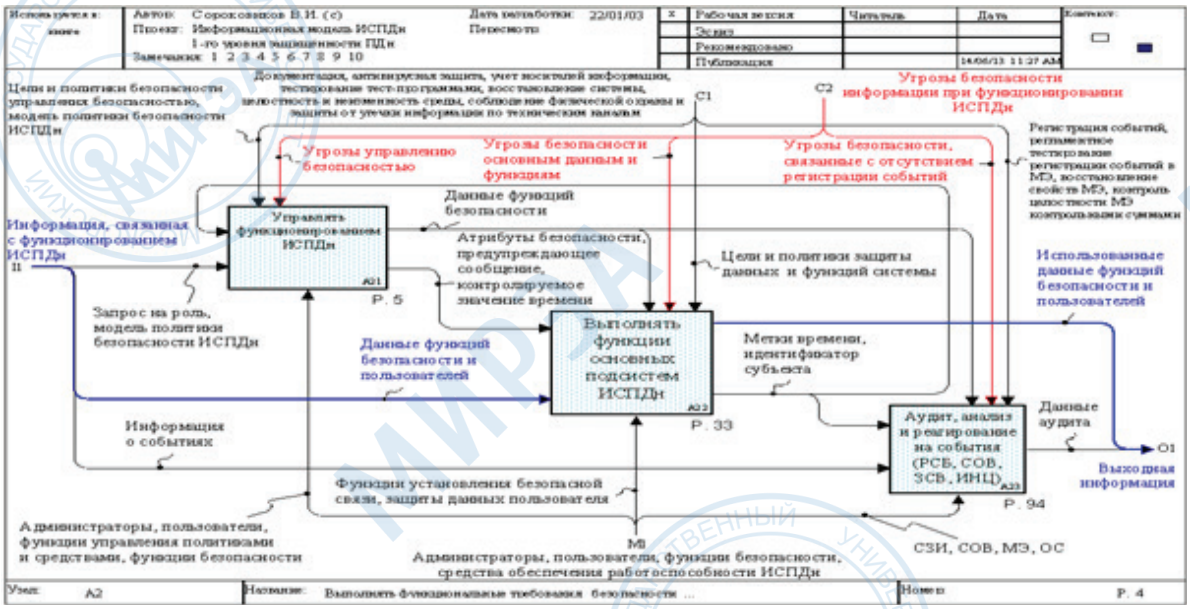

Рис. 1. Пример диаграммы информационной модели.

Методика моделирования безопасности изделий ИТ [3], основанная на вышеизложенном подходе и применении методологии IDEF, позволяет наглядно описывать и даже проектировать системы безопасности. Предлагаемая методика основана на описании всех наиболее значимых аспектов безопасности изделий ИТ в виде взаимосвязанной информационной модели.

Кроме информации из Общих критериев, информационное моделирование позволяет рассмотреть все аспекты среды функционирования объекта оценки. Моделирование более наглядно, представительно, а разрабатываемые модели более удобны в работе, чем обычная текстовая информация. На рис. 2 показано, как модели отражают в себе требования профилей защиты и заданий по безопасности на основе Общих критериев.

На основе предлагаемого моделирования [3], фактически заменяя дорогие натурные испытания испытаниями на моделях, удобно создавать киберполигоны для сборки моделей больших систем из моделей отдельных технологий, проводить их исследования на надежность, живучесть, осуществлять выявление «узких мест». Такой киберполигон будет удобен, например, для обучения студентов и для отработки учебно-тренировочных средств в области обеспечения информационной безопасности.

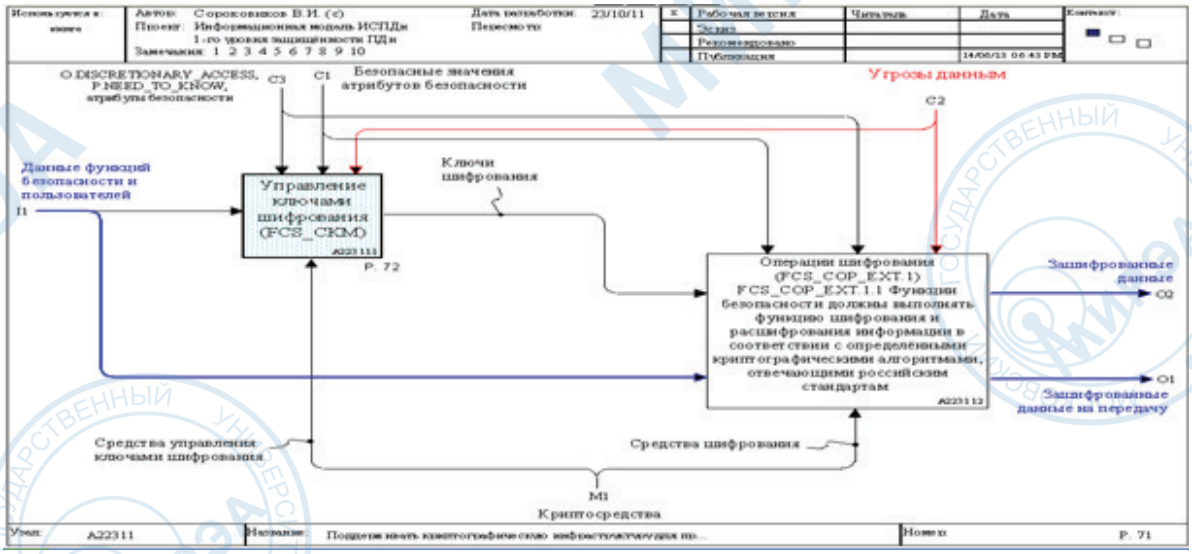

Рис. 2. Пример диаграммы информационной модели, в которой отражены требования Общих критериев.

Заключение

Информационное моделирование является значимым и удобным средством для представления информации. Схемы, представленные в статье, несут в себе более воспринимаемую специалистом информацию, чем если бы она была описана в текстовом виде. Они показывают движение информации в ИТ и среду безопасности информации (угрозы, политики безопасности информации), а также являются более информационно-емкими, наглядными и представительными. Классифицированные, иерархические и взаимоувязанные требования Общих критериев легко описываются схемами информационного моделирования (можно сказать, что просто предназначены для этого). Гибкость ОК и их ориентированность на архитектуры современных ИТ обобщает опыт работы в области безопасности информации и предоставляет возможность для перспективного развития этого опыта. ОК – не только гибкий аппарат обеспечения безопасности информации, охватывающий большинство принципов современных ИТ, но и удобная платформа для мо-

делирования ИТ. Моделирование основ ИТ на базе ОК позволит применять модульный принцип для моделирования и предъявления требований безопасности информации для сложных ИТ.

Литература:

1. Набатов Д.В. Информационное сопровождение программного обеспечения // Научная перспектива. 2015. № 6. С. 14–19.

2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М.: Горячая линия – Телеком, 2013. 339 с.

3. Сороковиков В.И. Моделирование процессов обеспечения безопасности в операционных системах. М., 2009. 268 с.

4. Кияев В., Граничин О. Безопасность информационных систем. М.: Национальный Открытый Университет «ИНТУИТ», 2016. 192 с.

5. Мэйволд Э. Безопасность сетей. М.: Национальный Открытый Университет «ИНТУИТ», 2016. 572 с.

6. Скрипник Д.А. Общие вопросы технической защиты информации. М.: Национальный Открытый Университет «ИНТУИТ», 2016. 425 с.

7. Загинайлов Ю.Н. Основы информационной безопасности. М.: Директ-Медиа, 2015. 105 с.

8. Долозов Н.Л., Гультяева Т.А. Программные средства защиты информации. Новосибирск: НГТУ, 2015. 63 с.

9. Лапонина О.Р. Протоколы безопасного сетевого взаимодействия. М: Национальный Открытый Университет «ИНТУИТ», 2016. 462 с.

10. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации. М.: Директ-Медиа, 2015. 253 с.

11. Информационная безопасность и защита информации на железнодорожном транспорте: учебник / под ред. А.А. Корниенко. М: УМЦ ЖДТ (Маршрут), 2014. 440 с.