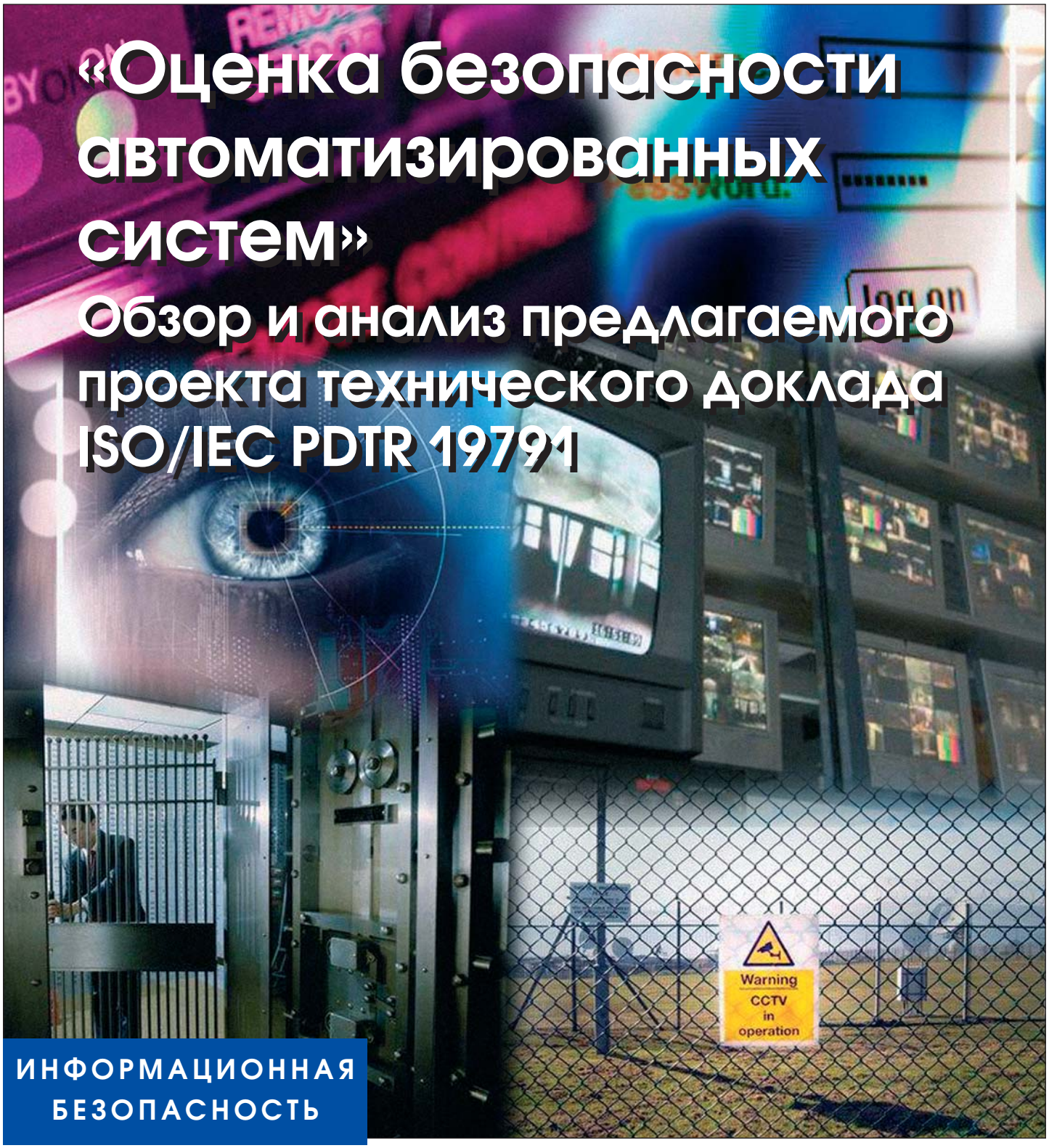
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 7 (146)/2005

«Оценка безопасности автоматизированных систем»

Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 19791



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

«Оценка безопасности автоматизированных систем»

Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 19791

Владимир Галатенко,
доктор физ.-мат. наук,
зав. сектором автоматизации программирования
НИИ системных исследований РАН

СОДЕРЖАНИЕ

Обзор проекта технического доклада ISO/IEC PDTR 19791

Введение

В середине октября 2002 г. на пленарном собрании Подкомитета 27 «Методы и средства обеспечения безопасности» (SC27) совместного Технического комитета 1 «Информационная технология» (JTC1) Международной организации по стандартизации (ISO) было выдвинуто предложение разработать новый стандарт для оценки безопасности автоматизированных систем. Данная инициатива получила поддержку членов подкомитета, в результате появился технический доклад «Security assessment of operational systems». В настоящем обзоре рассматривается вторая редакция проекта технического доклада (2nd Proposed Draft Technical Report, PDTR), опубликованная 17 декабря 2004 г.

Цель данной публикации — дать возможность читателю составить о предлагаемом проекте собственное мнение на основе объективной информации. Оценка проекта, обсуждение его сильных и слабых сторон, рекомендации по исправлению недостатков представлены в отдельном тексте.

Статус проекта

В центральном секретариате ISO проекту был присвоен номер 19791, а статус разрабатываемого документа определен как «Технический доклад типа 2». Это означает, что со временем (хотя и не в ближайшем будущем) текст доклада может быть утвержден в качестве международного стандарта.

Название технического доклада ISO/IEC PDTR 19791 «Security assessment of operational systems», учитывая сложившуюся в руководящих документах ФСТЭК России терминологию, предлагается перевести на русский язык как «Оценка безопасности автоматизированных систем».

В русскоязычном изложении проекта технического доклада везде, где возможно, использовалась терминология, принятая в национальном стандарте ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий», даже если она представлялась не совсем удачной.

Объем и структура технического доклада

Вторая редакция предлагаемого проекта технического доклада насчитывает 170 страниц, 160 из которых составляют нормативную часть. За титульными страницами, оглавлением, предисловием и введением следуют девять разделов, три приложения и библиография.

В разделе 1 описываются цели и рамки проекта 19791. В разделе 2 собраны нормативные ссылки, точнее, одна ссылка — на международный стандарт ISO/IEC 15408:2005 (все части). Раздел 3 содержит термины и определения, раздел 4 — перечень сокращений. В разделе 5 описана структура технического доклада, в разделе 6 — принятый подход, в разделе 7 — расширение существующих в стандарте ISO/IEC 15408 концепций оценки на автоматизированные системы, в разделе 8 — связь с существующими стандартами безопасности. Раздел 9 является руководством по проведению оценки автоматизированных систем.

Приложение A регламентирует структуру и содержание системных профилей защиты и заданий по безопасности. Приложение B содержит перечень системных функциональных требований, приложение C — перечень системных требований доверия к безопасности.

Цели проекта

Основная цель проекта 19791 — расширить международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» (Evaluation Criteria for IT Security), чтобы сделать возможной оценку безопасности систем, находящихся в производственной эксплуатации. Подобное расширение необходимо, поскольку стандарт ISO/IEC 15408 в его нынешнем виде хотя и позволяет специфицировать программно-техническую функциональность безопасности как для продуктов, так и для систем информационных технологий (ИТ), но не охватывает ряд критически важных аспектов действующих, эксплуатируемых (автоматизированных) систем, точные специ-

фикации которых необходимы для эффективного оценивания.

Проект содержит расширенные критерии оценки и рекомендации по оцениванию как программно-технических, так и административных и процедурных аспектов автоматизированных систем (АС). Применение комплексного подхода, охват мер всех уровней, направленных на обеспечение информационной безопасности, равно как и всех этапов жизненного цикла АС — еще одна цель проекта.

Проект ориентирован не только на оценщиков, но и на разработчиков, системных интеграторов и эксплуатационщиков АС, поскольку эти специалисты должны понимать, что требуется для получения положительной оценки.

Технический доклад может стать международным стандартом (и это — одна из целей проекта) после формализации предлагаемых концепций и подходов и получения необходимого опыта их применения. Очевидно, процесс этот длительный и трудоемкий.

Международные стандарты, на которые опирается проект

Базовым для проекта 19791 является международный стандарт ISO/IEC 15408. В нем определен современный понятийный аппарат и подходы к оценке изделий информационных технологий. Общая концепция, выделение функциональных требований и требований доверия к безопасности, формирование заданий по безопасности и профилей защиты — все это важные достижения, которые закрепляются и развиваются в рассматриваемом проекте. Развитие идет по четырем основным направлениям:

- ориентация на оценку действующих автоматизированных систем;
- реализация комплексного подхода к информационной безопасности, охват мер административного и процедурного уровней;
- охват всех этапов жизненного цикла автоматизированных систем;
- декомпозиция сложных систем на домены безопасности.

Международный стандарт ISO/IEC 15408 ориентирован в первую очередь на оценку продуктов информационных технологий. Среда, в которой функционируют или должны функционировать подобные продукты, специфицируется в общем виде, в форме предположений о среде. Действующие автоматизированные системы окружены вполне определенной, конкретной средой, которую можно и нужно учитывать в процессе оценивания безопасности.

Международный стандарт ISO/IEC 15408 ограничен рамками программно-технического уровня информационной безопасности. Для оценки продуктов информационных технологий этого, в принципе, достаточно; для систем, находящихся в производственной эксплуатации, — нет. В рассматриваемом проекте фигурируют функциональные требования и требования доверия к безопасности, относящиеся прежде всего к процедурному, а также к административному уровням информационной безопасности. Считается, что меры программно-технического уровня заимствуются из стандарта ISO/IEC 15408.

Как и в стандарте ISO/IEC 15408, в предлагаемом проекте с мерами и механизмами безопасности (как техническими, так и организационными) ассоциированы соответствующие управляющие меры и механизмы. Например, с техническими средствами разграничения доступа ассоциированы управляющие меры регистрации атрибутов пользователей; с организационными правилами присвоения ролей пользователям ассоциированы административные процедуры управления пользовательскими ролями.

Для обеспечения информационной безопасности продуктов ИТ определяющим является этап разработки, и это нашло отражение в стандарте ISO/IEC 15408. Для действующих систем важны все этапы жизненного цикла, вплоть до выведения из эксплуатации. Это нашло отражение в рассматриваемом проекте.

В международном стандарте ISO/IEC 15408 объект оценки рассматривается как единое целое, с единым набором требований и единой оценкой. Для сложных автоматизированных систем это может оказаться неприемлемым. Целесообразно структурировать сложную систему на домены с разными рисками, требованиями и разной политикой безопасности, что и сделано в рассматриваемом проекте.

Меры безопасности административного и процедурного уровней, включенные в технический доклад, в значительной степени заимствованы из международного стандарта ISO/IEC 17799. Важное отличие, однако, состоит в том, что упомянутый стандарт ориентирован на разработчиков и эксплуатационщиков, а рассматриваемый проект — в первую очередь на оценщиков. Соответственно, положения стандарта ISO/IEC 17799 переформу-

лированы так, чтобы служить критериями оценки безопасности.

Основные понятия, включенные в проект

Поскольку рассматриваемый проект является расширением международного стандарта ISO/IEC 15408, все основные понятия упомянутого стандарта применимы и к проекту 19791. Из вновь введенных понятий выделим следующие.

- Автоматизированная система — информационная система, включая нетехнические аспекты, рассматриваемая в контексте эксплуатационной среды.
- Верификация — процесс оценки, призванный подтвердить, что регуляторы безопасности автоматизированной системы реализованы корректно и эффективно выполняют отведенную им роль.
- Домен безопасности — часть автоматизированной системы, реализующая единый набор политик безопасности.
- Подсистема — набор компонентов автоматизированной системы, способный функционировать отдельно от остальных частей АС.
- Регуляторы безопасности — административные, процедурные и программно-технические регуляторы (то есть защитные механизмы и контрмеры), предназначенные для обеспечения конфиденциальности, целостности и доступности автоматизированной системы и обрабатываемой ею информации. Подразумевается также обеспечение подотчетности, аутентичности, неотказуемости, приватности и надежности — свойств, которые рассматриваются некоторыми авторами как отличные от конфиденциальности, целостности и доступности.
- Уязвимость — дефект или слабое место в проекте или реализации автоматизированной системы (включая регуляторы безопасности), которые могут быть умышленно или неумышленно использованы для вредоносного воздействия на активы организации и/или ее функционирование.

Многие основные понятия проекта 19791 получаются из аналогичных понятий стандарта ISO/IEC 15408 добавлением слов «системный», «система», например: «системный профиль защиты» (СПЗ), «системное задание по безопасности» (СЗБ), «доверие к безопасности системы» (ДБС), «системная функциональность безопасности» (СФБ), «системный объект оценки» (СОО).

Модель автоматизированной системы

Наряду с приведенным выше определением автоматизированной системы, в докладе анализируются важнейшие свойства подобных систем.

Автоматизированные системы по своей природе сложны, они строятся из подсистем, часть из которых уникальны и являются результатом собственных разработок, другие же образованы типовыми продуктами общего назначения от различных производителей. Система в целом может строиться из подсистем системным интегратором, который не выполняет собственных разработок, обеспечивая лишь взаимосвязь и конфигурирование.

Автоматизированные системы взаимодействуют с другими системами и зависят от них. Как правило, автоматизированные системы обладают следующими свойствами:

- находятся под контролем одного владельца;
- строятся для достижения определенных целей и для функционирования в определенном режиме;
- подвержены частым изменениям, как в плане технического устройства, так и в плане эксплуатационных требований;
- состоят из значительного, порой очень большого числа компонентов;
- содержат покупные компоненты с большим числом возможных вариантов конфигурирования;
- оставляют за владельцем выбор баланса между техническими и нетехническими мерами безопасности;
- содержат компоненты с различными уровнями и типами доверия к безопасности.

Оцениваемая автоматизированная система может взаимодействовать с другими АС и/или входить в состав более крупной системы. Системный объект оценки (СОО) включает в себя как технические средства, так и их эксплуатационную среду. Его граница пролегает там, где кончается непосредственный контроль системы. Все остальное рассматривается как внешняя АС.

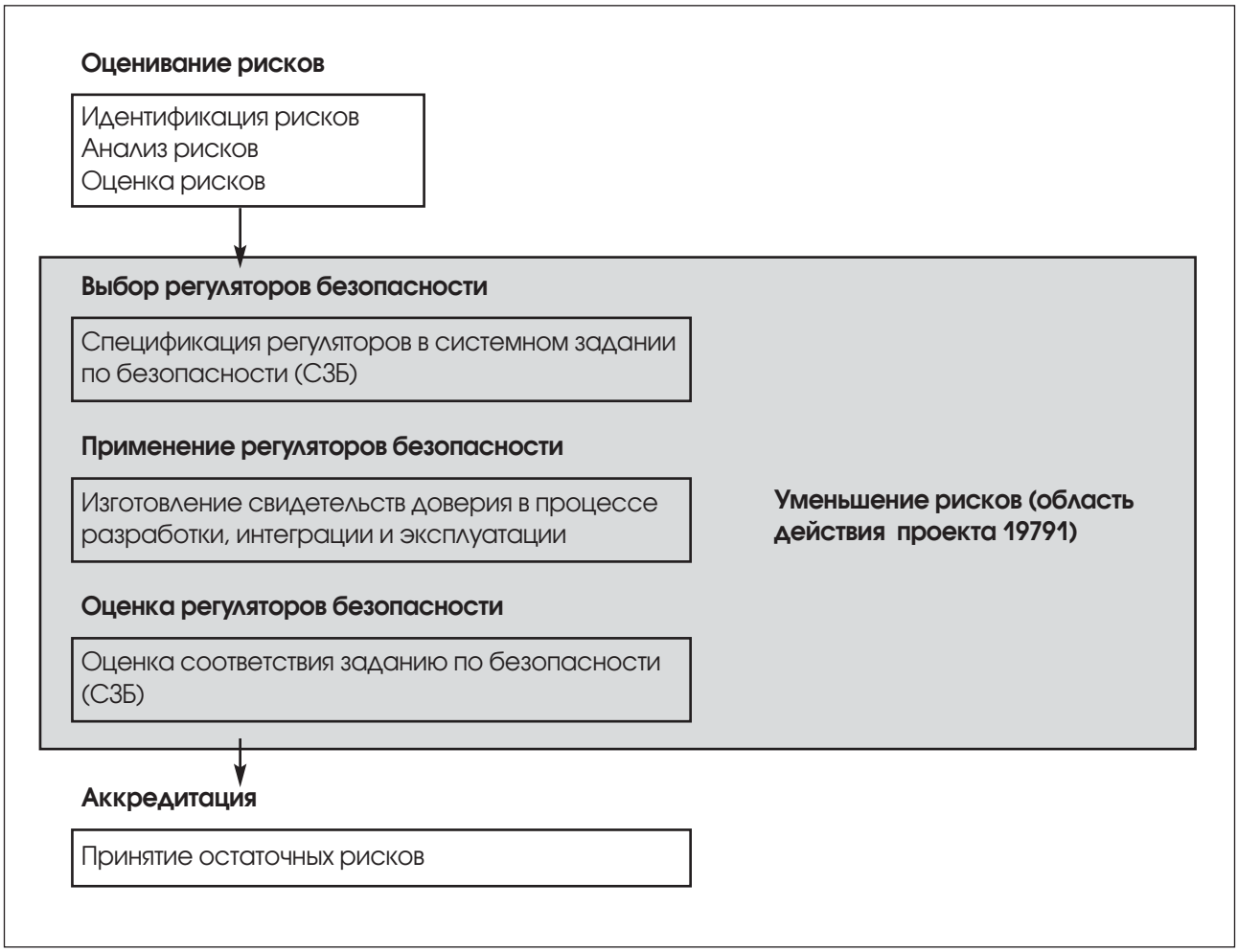


Рис. 1. Процесс формирования режима безопасности автоматизированной системы.

У автоматизированной системы есть множество предоставляемых ею функций, внешние интерфейсы, а также внутренняя структура и внутренние интерфейсы. Каждый компонент может предоставлять одну или несколько функций и быть реализованным в виде одного или нескольких продуктов ИТ.

Автоматизированная система может состоять из нескольких доменов безопасности с различными функциональными требованиями и требованиями доверия к безопасности. Может быть определена общая политика безопасности АС, общие цели и требования безопасности, общая документация. В дополнение возможно существование аналогичного набора для каждого домена безопасности, содержащего специфическую для домена информацию.

В качестве иллюстрации многодоменного СОО в техническом докладе приведена система, построенная в архитектуре клиент/сервер, с использование прикладного и базового программного обеспечения, а также ПО промежуточного слоя. Базовое ПО может быть предварительно сертифицировано в соответствии с требованиями стандарта ISO/IEC 15408, для других компонентов возможно существование отдельных свидетельств доверия к безопасности. Для некоторых компонентов получение подобных свидетельств проблематично, и оценщик должен подходить к ним как к «черному ящику». Это еще один аспект разнородности системных объектов оценки.

Таким образом, в рассматриваемой модели АС делается акцент на сложность подобных систем и разнородность их компонентов, а также на наличие альтернативных способов обеспечения их безопасности — технических и организационных.

Формирование режима безопасности

В предлагаемом проекте принят трехзвенный подход к формированию режима безопасности авто-

матизированных систем. Первый этап состоит в идентификации, анализе и оценке рисков, которым подвержена АС. Второй этап — уменьшение (или ликвидация) рисков путем выбора, применения и оценки регуляторов безопасности. На третьем этапе проводится аккредитация АС, подтверждающая, что остаточные риски допустимы для системы, эксплуатируемой в конкретной реальной среде.

Проект 19791 имеет дело только со вторым из перечисленных этапов (см. рис. 1). В качестве средства достижения цели данного этапа используется оценка безопасности, основанная на модели оценивания технических регуляторов, принятой в стандарте ISO/IEC 15408, но распространенная на регуляторы всех видов.

Несмотря на то, что оценивание рисков находится за рамками предлагаемого проекта, этот процесс должен быть документирован, так как его результаты являются исходными данными для разработки системного задания по безопасности.

Для формирования режима безопасности следует:

- идентифицировать риски, которые необходимо уменьшить или ликвидировать;
- сформулировать цели безопасности для технических, процедурных и административных регуляторов безопасности, призванных снизить все риски до приемлемого уровня;
- выбрать функциональные регуляторы, удовлетворяющие целям безопасности АС;
- определить конкретные, измеримые требования доверия для технических, процедурных и административных регуляторов безопасности, чтобы получить требуемую степень уверенности в способности автоматизированной системы достичь поставленных целей безопасности;
- зафиксировать принятые решения в системном задании по безопасности (СЗБ);
- оценить соответствие реальной автоматизированной системы системному ЗБ;
- периодически проводить переоценку рисков и способности АС этим рискам противостоять.

Безопасность в жизненном цикле автоматизированной системы

Регуляторы безопасности автоматизированной системы должны оцениваться на всем протяжении ее жизненного цикла. В рассматриваемом техническом докладе выделяются четыре этапа жизненного цикла:

- разработка/интеграция;
- ввод в эксплуатацию;
- производственная эксплуатация;
- сопровождение.

В качестве первого шага первого этапа указана идентификация рисков для автоматизированной системы. После того как выявлены недопустимо высокие риски, подлежащие уменьшению или ликвидации средствами безопасности АС, уполномоченное должностное лицо рассматривает ожидаемые остаточные риски и подтверждает их приемлемость.

Второй шаг — проектирование АС, включая определение используемых аппаратных и программных продуктов, поддерживающей инфраструктуры, прикладного программного обеспечения и необходимых технических регуляторов безопасности. Параллельно разрабатывается системное задание по безопасности, в которое включается описание системных требований безопасности, в том числе перечень рисков, которым необходимо противостоять, и целей безопасности, которых необходимо достичь с помощью технических, процедурных и административных регуляторов. Зафиксированный в СЗБ список регуляторов может рассматриваться как форма представления системных целей безопасности.

Уже на первом, самом раннем этапе жизненного цикла АС следует начинать проведение оценки ее безопасности. Это облегчит оценщикам понимание системы и ее предполагаемой эксплуатационной среды, анализ проектной документации и руководств, получение свидетельств доверия к безопасности. В идеале следует оценить все системное ЗБ, чтобы убедиться в отсутствии несоответствий и упущений в требованиях безопасности и предлагаемых регуляторах.

Третий шаг первого этапа — разработка или закупка базового и прикладного программного обеспечения, включая технические регуляторы безопасности, а также системная интеграция, конфигурирование и тестирование разработчиком/интегратором. Параллельно создается инфраструктура безопасности для административного и процедурного уровней, документируются политики, правила и процедуры безопасности, интегрируемые в системный контекст.

Если происходит перестройка существующей автоматизированной системы, то выполняется замена регуляторов безопасности в соответствии с изменившейся средой. Верификационная

деятельность при этом должна быть увязана с масштабом и характером изменений.

За интеграционным тестированием разработчик выполняет тестирование безопасности, чтобы убедиться в выполнении предъявляемых системных требований. Обычно специфические для конкретной организации параметры безопасности (технические, административные и процедурные) могут быть определены до развертывания автоматизированной системы в производственной среде, поэтому разработчик/интегратор может выполнить верификацию регуляторов безопасности уже на первом этапе, до начала этапа ввода в эксплуатацию. Верификация должна подтвердить силу механизмов безопасности и корректность функционирования регуляторов.

Следующий шаг — оценка автоматизированной системы. Это даст владельцу АС независимое подтверждение того, что все риски, фигурирующие в СЗБ, благодаря применению регуляторов безопасности уменьшены до приемлемого уровня. В сертификационном докладе перечисляются все обнаруженные уязвимости и описываются рекомендуемые действия по их устранению. Владелец АС готовит план устранения недостатков. Результаты сертификации системы представляются уполномоченному должностному лицу, определяющему допустимость реальных остаточных рисков для системных активов и процесса функционирования.

Итог первого этапа — получение официального разрешения на ввод системы в эксплуатацию. На втором этапе система устанавливается, развертывается и готовится к использованию.

На этапе производственной эксплуатации выполняется протоколирование, непрерывное отслеживание работы технических, процедурных и административных регуляторов безопасности, обеспечивается обратная связь для корректирующих действий после внесения изменений в АС. Обычно осуществляется мониторинг не всех регуляторов, а только их критически важного подмножества. Кроме того, владелец системы должен располагать средствами управления конфигурацией, администрирования и аудита, которые позволяют получить текущую картину ресурсов АС и их конфигурации.

На этапе сопровождения рассматриваются и анализируются все предлагаемые или сделанные изменения АС, включая изменения политик, правил и процедур. При необходимости выполняется регрессионное тестирование. Если возможно значительное изменение остаточных рисков, то может потребоваться переоценка автоматизированной системы.

Сопровождение завершается выведением системы из эксплуатации, архивированием, ликвидацией или перемещением данных на другие системы. Уполномоченное должностное лицо должно заверить факт успешного завершения работы автоматизированной системы.

Доверие к безопасности автоматизированной системы

Доверие к безопасности автоматизированных систем по своей природе сложнее доверия к безопасности продуктов ИТ, получаемого в результате проведения оценки по стандарту ISO/IEC 15408. Доверие должно быть распространено как на технические, так и на процедурные и административные регуляторы безопасности, для его формирования могут потребоваться действия на всех этапах жизненного цикла АС, а не только на этапе разработки/интеграции. Автоматизированная система может состоять из многих доменов безопасности с различными требованиями доверия.

Сочетание всех перечисленных факторов заставляет предусмотреть новые (по сравнению со стандартом ISO/IEC 15408) действия для оценки доверия к безопасности.

В предлагаемом проекте выделены два аспекта доверия к безопасности: корректность и эффективность. Корректность означает корректную реализацию механизмов безопасности, функционирование в соответствии с документацией, отслеживание постоянной доступности сервисов безопасности. Эффективность означает, что механизмы безопасности противостоят угрозам и уязвимостям и предотвращают неавторизованные действия, такие как обход защитных средств или вмешательство в их работу. И корректность, и эффективность должны поддерживаться на всех этапах жизненного цикла АС.

На этапе разработки/интеграции для проверки корректности необходимо в первую очередь проверить соответствие между рисками и требованиями безопасности, а также между требованиями и контрмерами. Требования должны охватывать все недопустимо высокие риски, а контрмеры — все требования безопасности. Необходимо убедиться в корректности управления конфигурацией контрмер. Следующий шаг — проверка корректности реализации контрмер и их включения в систему без неавторизованных модификаций. Наконец, следует проверить, кор-

ректно ли отражена функциональность контрмер в документации на систему.

Для проверки эффективности на этапе разработки/интеграции следует убедиться, что требования безопасности, включенные в СЗБ, позволяют уменьшить риски до приемлемого уровня. Затем необходимо проанализировать проекты архитектуры системы в целом, ее подсистем и компонентов, а также представления о реализации и концепцию безопасности на предмет согласованности контрмер, распределенных по различным подсистемам и компонентам, и убедиться, что в совокупности эти контрмеры обеспечивают требуемые свойства безопасности АС. Наконец, следует проверить, обладают ли механизмы безопасности достаточной стойкостью и обеспечивают ли они защиту от атак злоумышленников с предполагаемым потенциалом. Для этого необходимо провести анализ уязвимостей и организовать тестирование путем преодоления защиты.

На этапе ввода в эксплуатацию для проверки корректности следует убедиться, что административные и процедурные регуляторы соответствуют требованиям безопасности, а их введение в действие санкционировано уполномоченным должностным лицом. Эффективность заключается в доведении до сведения пользователей АС правил и процедур безопасности и в проведении обучения. Необходимо проконтролировать формальные и содержательные результаты обучения.

Для проверки корректности на этапе эксплуатации следует проводить аудит регистрационной информации, проверять данные о доступе и использовании ресурсов, чтобы убедиться в корректной работе контрмер. Эффективность контролируется аналогичным образом, быть может, с дополнительным проведением опросов пользователей. Следует убедиться в отсутствии несанкционированных действий и недопустимо высоких рисков, в восстановлении безопасных состояний из небезопасных за требуемое время.

На этапе сопровождения необходимо контролировать своевременное выявление проблем, доведение их до сведения должностных лиц, проведение анализа и внесение изменений. Регрессионное тестирование и тестирование путем преодоления защиты должны подтвердить, что измененные регуляторы безопасности функционируют в соответствии со спецификациями и эффективно противостоят рискам.

Проведение оценки безопасности автоматизированной системы

Процесс оценки безопасности автоматизированной системы в предлагаемом проекте подразделяется на три этапа:

- порождение свидетельств для оценивания, включая результаты оценки рисков, спецификацию системного объекта оценки, данные и документацию по разработке, интеграции, эксплуатации и мониторингу АС;
- оценивание, включая сертификацию результатов оценки;
- аккредитация автоматизированной системы.

Все перечисленные действия должны выполняться определенными должностными лицами. Согласно предлагаемому проекту, их роли и обязанности заключаются в следующем.

На первом этапе руководитель организации владельца автоматизированной системы, несущий общую ответственность за информационную безопасность, определяет допустимый уровень рисков и санкционирует действия уполномоченного должностного лица, оценивающего и определяющего допустимость остаточных рисков.

Отдел информационной безопасности разрабатывает политику безопасности организации, определяет обязательные регуляторы, которые должны быть реализованы во всех автоматизированных системах организации.

Владелец системы проводит оценку рисков, определяет задачу безопасности, решаемую автоматизированной системой, готовит системные профили защиты (возможно, в сотрудничестве с владельцами аналогичных систем), санкционирует повторное проведение оценки, исходя из изменений, произведенных в системе и/или эксплуатационной среде, отслеживает состояние системы по непрерывно поступающим данным протоколирования/аудита.

Проектировщик/разработчик/интегратор системы создает или участвует в создании системного задания по безопасности, основываясь на задаче безопасности, сформулированной владельцем системы; порождает свидетельства этапа разработки; помогает владельцу системы уменьшить или устранить уязвимости, выявленные в процессе оценивания.

Специалисты, занимающиеся администрированием, эксплуатацией и сопровождением, помогают разработать системное задание по безопасности; порождают свидетельства этапа эксплу-

атации; помогают владельцу системы уменьшить или устранить уязвимости, выявленные в процессе оценивания.

На этапе проведения оценки оценщик/представитель сертифицирующего ведомства оценивает систему, исходя из требований безопасности, фигурирующих в СЗБ, и делает вывод о способности АС выполнить эти требования в данный момент времени; дает независимую оценку безопасности действующей системы; по мере необходимости проводит переоценку АС после внесения изменений в систему или эксплуатационную среду; сертифицирует результаты оценки; готовит доклад по результатам оценки и сертификации и предоставляет его владельцу системы вместе с рекомендациями, чтобы поддержать аккредитацию АС.

На этапе аккредитации представитель соответствующего ведомства санкционирует использование системы или подтверждает, что ожидаемые остаточные риски находятся в допустимых пределах.

Автоматизированная система должна решать определенную задачу безопасности. В формулировке этой задачи должны быть отражены два аспекта:

- результаты анализа рисков и, в частности, риски, которые необходимо уменьшить или устранить;
- политики безопасности организации, которые система должна проводить в жизнь.

Предлагаемое решение задачи безопасности начинается с выбора целей безопасности. В контексте оценивания АС следует различать три типа целей безопасности:

- цели, достигаемые посредством технических регуляторов, реализуемых в рамках системной функциональности;
- цели, достигаемые посредством административных и/или процедурных регуляторов (политик, процедур и т.п.), реализуемых в эксплуатационной среде АС;
- цели, достигаемые с помощью мер доверия (таких как верификационная деятельность).

В предлагаемом проекте, как и в стандарте ISO/IEC 15408, требования безопасности подразделяются на функциональные и требования доверия. В свою очередь, системная функциональность безопасности (СФБ) включает технические функции безопасности (ТФБ) и организационные функции безопасности (ОФБ). После того как определены требования безопасности, владелец АС может выбрать баланс между техническими и организационными регуляторами безопасности. Технические регуляторы выбираются из арсенала стандарта ISO/IEC 15408 (или вводятся дополнительные компоненты в соответствии с дисциплиной, описанной в приложении А стандарта ISO/IEC 15408-1). Требования к организационным регуляторам (в количестве семи функциональных классов) специфицированы в приложении В предлагаемого проекта.

Организационные требования безопасности должны предъявляться к административным и эксплуатационным процессам и процедурам. Они должны быть описаны в эксплуатационных руководствах, предназначенных для пользователей и операторов. В процессе оценки проверяется, предоставляются ли выбранными организационными функциями безопасности требуемые возможности. Применение организационных регуляторов должно сопровождаться протоколированием, допускающим последующий аудит.

Вообще говоря, требования доверия в том виде, как они сформулированы в стандарте ISO/IEC 15408-3 для технических регуляторов, могут быть применены буквально или легко адаптированы к административным и процедурным регуляторам. Для оценки же автоматизированных систем, обладающих более сложной, по сравнению с продуктами ИТ, структурой, необходимы дополнительные требования доверия. Например, в проектной документации и при тестировании следует принять во внимание общую архитектуру системы и специфику доменов безопасности. Еще одна группа требований доверия необходима для охвата мониторинга работы регуляторов безопасности на этапе эксплуатации и для проверки системных профилей защиты и заданий по безопасности. В приложении С предлагаемого проекта описаны десять новых классов требований доверия.

В рассматриваемом техническом докладе обращается внимание на то, что при проведении оценки в соответствии со стандартом ISO/IEC 15408 требования доверия обычно не выводятся из задачи безопасности, но просто постулируются или выбираются «политическим» решением. При оценивании автоматизированных систем приходится учитывать различия в характере и объеме информации об используемых продуктах ИТ, а также выбранный баланс между техническими и организационными регуляторами безопасности и соответственно выбирать меры доверия. Из этого следует, что цели доверия должны рассматриваться как часть решения задачи безопасности.

Еще один нюанс состоит в том, что для автоматизированных систем, включающих с себя мно-

жество разнообразных продуктов ИТ, приходится учитывать существование множества сред разработки, по крайней мере одна из которых (для системной интеграции и разработки организационных регуляторов) совпадает с эксплуатационной. Это означает, что некоторые требования доверия к безопасности среды разработки оказываются невыполнимыми, а применение других может быть отложено до этапа ввода системы в эксплуатацию.

Задачи, цели и требования безопасности фиксируются владельцем в системном задании по безопасности (СЗБ), структура которого специфицирована в приложении А предлагаемого проекта.

Если владелец стремится сформулировать требования к АС способом, не зависящим от реализации, он может первоначально разработать системный профиль защиты (СПЗ). Обязательные и необязательные части СПЗ специфицированы в том же приложении.

Системное задание по безопасности является основой как документации по средствам безопасности АС, так и оценки этих средств в пределах системного объекта оценки (СОО). Как таковое, оно предоставляет и свидетельство, и информацию, необходимую для проведения оценки. Как и привычное по стандарту ISO/IEC 15408 задание по безопасности, СЗБ может быть проверено на внутреннюю непротиворечивость независимо от СОО.

Последующая оценка СОО может выявить несоответствия между СЗБ и СОО. Например: расхождения между реальной и описанной в СЗБ эксплуатационной средой, между запланированной в СЗБ и реализованной функциональностью безопасности, между реальными и запланированными интерфейсами и их поведением. Владелец АС должен решить, что (задание или система) является правильным, а что следует изменить. По этой причине окончательное заключение о том, что СЗБ является корректным представлением задуманной автоматизированной системы, может быть сделано только после завершения оценивания СОО.

Владелец АС должен предусмотреть регуляторы для поддержки уверенности в том, что результаты оценки автоматизированной системы сохраняют свою годность в процессе эксплуатации АС. С этой целью он может:

- специфицировать административные регуляторы для проведения периодических проверок сопровождения технических регуляторов и действенности регуляторов организационных;
- проводить периодические переоценки АС с акцентом на анализ влияния изменений в требованиях безопасности организации на совокупность технических и организационных регуляторов и на сохранение эффективности применения организационных мер.

Таковы, в соответствии с предлагаемым проектом, основные особенности проведения оценки автоматизированных систем.

Функциональные требования безопасности для автоматизированных систем

Общая характеристика функциональных требований безопасности для АС

Функциональные требования безопасности для автоматизированных систем, включенные в рассматриваемый проект, относятся к организационным (административным и процедурным) регуляторам. Они структурированы по трем характеристикам:

- субъект регулирования (руководство организации, производственные данные, системы ИТ, поддерживающая инфраструктура и т.п.);
- функциональная область (политика безопасности, оценка рисков, протоколирование/аудит и т.п.);
- действие в заданной функциональной области (утверждение политики безопасности, управление рисками в организации, доклад об обнаруженном нарушении безопасности и т.п.).

Субъект регулирования определяет класс функциональных требований, функциональная область — семейство в классе, действие — компонент в семействе.

По сравнению со стандартом ISO/IEC 15408-2 существует четыре отличия в форме описания функциональных требований. Во-первых, в предлагаемом проекте нет иерархических связей между компонентами, поэтому диаграммы в описании семейств, равно как и подразделы «Иерархический» отсутствуют. Во-вторых, все действия по управлению явным образом включены в отдельные компоненты, поэтому в подразделах «Управление» нет необходимости. В-третьих, подзаголовок «Аудит» заменен на «Записи», который лучше отражает процесс сбора необходимых свиде-

тельств функционирования организационных регуляторов. В-четвертых, операция назначения используется более гибко, в ней могут фигурировать идентификаторы документов, описывающих ассоциированные политики, процедуры, правила, требования безопасности и т.п.

В приложении В рассматриваемого проекта содержится описание семи новых, по сравнению со стандартом ISO/IEC 15408-2, классов функциональных требований, включающих следующие двадцать девять семейств:

- класс FOD (администрирование, то есть действия руководства организации):
  - FOD_POL (администрирование политик),
  - FOD_PSN (администрирование персонала),
  - FOD_RSM (администрирование управления рисками),
  - FOD_INC (администрирование управления инцидентами безопасности),
  - FOD_ORG (администрирование организации безопасности),
  - FOD_SER (администрирование сервисных соглашений);
- класс FOS (системы ИТ):
  - FOS_POL (политики для систем ИТ),
  - FOS_CNF (конфигурирование систем ИТ),
  - FOS_NET (сетевая безопасность систем ИТ),
  - FOS_MON (мониторинг систем ИТ),
  - FOS_PSN (управление персоналом систем ИТ),
  - FOS_OAS (эксплуатационные активы систем ИТ),
  - FOS_RCD (протоколирование для систем ИТ);
- класс FOA (пользовательские активы):
  - FOA_PRO (защита конфиденциальности данных),
  - FOA_INF (защита информации в пользовательских активах);
- класс FOB (производственная деятельность):
  - FOB_POL (политики производственной деятельности),
  - FOB_BCN (непрерывность производственной деятельности);
- класс FOP (инфраструктура и оборудование):
  - FOP_MOB (мобильное оборудование),
  - FOP_RMM (съемное оборудование),
  - FOP_RMT (удаленное оборудование),
  - FOP_SYS (системное оборудование),
  - FOP_MNG (управление инфраструктурой);
- класс FOT (сторонние организации):
  - FOT_COM (обязательства сторонних организаций),
  - FOT_MNG (управление взаимодействием со сторонними организациями);
- класс FOM (управление):
  - FOM_PRM (управление параметрами безопасности),
  - FOM_CLS (управление классификацией активов),
  - FOM_PSN (управление должностными обязанностями, связанными с безопасностью),
  - FOM_ORG (управление организацией безопасности),
  - FOM_INC (управление докладами о событиях, связанных с безопасностью).

Чтобы продемонстрировать структуру и стиль описания функциональных требований безопасности для автоматизированных систем в предлагаемом проекте, приведем в качестве примера описание семейства FOD_RSM (администрирование управления рисками).

«B.2.3 Администрирование управления рисками (FOD_RSM)

B.2.3.1 Характеристика семейства

Данное семейство определяет управление рисками как объект администрирования. Оно включает управление рисками, вызванными действиями как самой организации, так и ее партнеров.

B.2.3.2 Ранжирование компонентов

FOD_RSM.1 Управление рисками в пределах организации. Определяются процедуры управления рисками, вызванными действиями самой организации.

FOD_RSM.2 Управление рисками, относящимися к доступу сторонних организаций. Определяются процедуры управления рисками, вызванными доступом сторонних организаций.

B.2.3.3 Записи

Автоматизированная система должна поддерживать и предоставлять для проверки следующие свидетельства.

Для FOD_RSM.1: Описание управления рисками организации с конкретными действиями, определениями и записями об осуществлении управления рисками.

Для FOD_RSM.2: Описание управления рисками при доступе сторонних организаций с конкретными действиями, определениями и записями об осуществлении управления рисками.

B.2.3.4 FOD_RSM.1 Управление рисками в пределах организации

Зависимости: нет зависимостей.

FOD_RSM.1.1 ОФБ должна определять (назначение: процедуры) для управления рисками для перечней инфор-

мации организации и средств обработки информации с учетом тех, кто работает дома, а также других удаленных или мобильных пользователей.
FOD_RSM.1.2 ОФБ должна определять (назначение: требования безопасности) для осуществления управления рисками для автоматизированной системы с учетом производственных процессов и персонала, связанного с АС.

B.2.3.5 FOD_RSM.2 Управление рисками, относящимися к доступу сторонних организаций.
Зависимости: нет зависимостей.
FOD_RSM.2.1 ОФБ должна определять (назначение: процедуры) для управления рисками для перечней информации организации и средств обработки информации, к которым сторонние организации будут иметь доступ, с учетом перечней регуляторов, предназначенных для сторонних организаций, законодательных и нормативных требований, которые должны приниматься во внимание сторонними организациями, а также контрактных обязательств, которые необходимо принимать во внимание организации и ее партнерам.»

Далее следует краткий обзор предложенных в проекте классов функциональных требований безопасности для автоматизированных систем.

Класс FOD: администрирование

Данный класс содержит требования к организационным регуляторам для руководства работой автоматизированной системы. Он состоит из шести семейств.

Семейство FOD_POL (администрирование политик) определяет администрируемые политики безопасности АС. Оно включает определение политики безопасности, комиссии по управлению, поверки управления, а также административных регуляторов нарушений безопасности.

Семейство содержит два компонента — FOD_POL.1 «политика безопасности» и FOD_POL.2 «комиссия по управлению». Первый определяет административные регуляторы, цели и объекты политики безопасности, поверку управления и административные регуляторы нарушений безопасности. Второй — учреждение комиссии по управлению.

Компонент FOD_POL.1 конкретизируется в виде восьми элементов. В качестве характерного примера приведем первый из них.

«FOD_POL.1.1 ОФБ должна определять (назначение: обязательства руководства), включая ясное направление, видимую руководящую поддержку, консультации специалистов по безопасности, поддержку соответствующими ресурсами и интеграцию в процессы продвижения вопросов безопасности.»

Компонент FOD_POL.2 конкретизируется в виде единственного элемента.

Семейство FOD_PSN (администрирование персонала) определяет администрирование персонала в контексте обеспечения безопасности автоматизированной системы. Оно включает определение ролей и обязанностей должностных лиц, определение дисциплинарных акций, содержания персональных контрактов, управление идентификацией пользователей, контроль активов.

В семейство входит единственный компонент — FOD_PSN.1 «роли и обязанности должностных лиц», в котором специфицируются управляющие обязанности, обязанности по выполнению процесса увольнения, юридические нормы и регуляторы безопасности для лиц, работающих в охраняемых областях, формальный процесс наложения дисциплинарных наказаний, требования должностных контрактов и правила заключения соглашений о неразглашении, правила надзора за посетителями, правила определения допустимых областей доступа, правила возврата всех активов организации.

Компонент FOD_PSN.1 конкретизируется в виде двадцати элементов. Пример:

«FOD_PSN.1.19 ОФБ должна определять (назначение: правила), состоящие в том, что все штатные сотрудники, лица, работающие по контракту, а также сотрудники сторонних организаций обязаны возвращать все находящиеся в их распоряжении активы организации по истечении их должностных контрактов.
Примечание. Активы организации включают в себя ранее выпущенное программное обеспечение, корпоративные документы, мобильные вычислительные устройства, кредитные карты, карты доступа, программное обеспечение, справочники и данные, хранящиеся на электронных носителях.»

Описание семейства FOD_RSM (администрирование управления рисками) полностью приведено выше.

Семейство FOD_INC (администрирование управления инцидентами безопасности) определяет управление инцидентами безопасности как объект администрирования. Оно состоит из одного компонента — FOD_INC.1 «инциденты безопасности», — определяющего формальную проце-

дуру доклада об инцидентах, процедуры управления инцидентами и действия по возвращению к нормальной работе.

Среди семи элементов, конкретизирующих этот компонент, выделим следующий.

«FOD_INC.1.4 ОФБ должна определять (назначение: требования безопасности) к действиям по восстановлению нормального функционирования после нарушений безопасности или отказов системы.»

Семейство FOD_ORG (администрирование организации безопасности) определяет действия руководства по организации безопасности, а именно учреждение комиссии по управлению.

Единственный компонент семейства — FOD_ORG.1 «комиссия по управлению» определяет обязанности комиссии.

Обязанности комиссии конкретизируются в единственном элементе FOD_ORG.1.1, который предписывает, в частности, поддерживать инициативы в области информационной безопасности.

Последнее, шестое семейство класса — FOD_SER «администрирование сервисных соглашений» — определяет требования к безопасности сетевых сервисов.

Единственный компонент семейства, поименованный как FOD_SER.1 «соглашения по сетевым сервисам», специфицирует защитные возможности, уровни сервиса и требования к управлению сетевыми сервисами.

Из двух элементов, конкретизирующих данный компонент, приведем второй.

«FOD_SER.1.2 ОФБ должна определять (назначение: требования безопасности) к способности поставщика сетевых услуг оказывать их безопасным образом и оговаривать право организации на проведение аудита.»

Класс FOS: системы ИТ

Этот класс, включающий семь семейств, содержит требования к организационным регуляторам систем ИТ в эксплуатационном контексте.

Семейство FOS_POL (политики для систем ИТ) определяет политики безопасности для систем ИТ в эксплуатационной среде. В него входят: определение требований безопасности, контроль изменений, контроль вредоносного программного обеспечения, политика в области криптографии.

Семейство FOS_POL подразделяется на четыре компонента: FOS_POL.1 «требования безопасности», FOS_POL.2 «политика по отношению к вредоносному ПО», FOS_POL.3 «политика в области криптографии» и FOS_POL.4 «общедоступные системы».

Компонент FOS_POL.1 ведает авторизованным доступом к системам ИТ, системными учетными действиями, идентификацией изменений в системе, их контролем и вводом в эксплуатацию.

Один из аспектов компонента FOS_POL.3 — процедуры управления криптографическими ключами.

Компонент FOS_POL.4 определяет защитные процедуры для общедоступных систем.

Среди элементов, конкретизирующих компонент FOS_POL.1, выделим третий.

«FOS_POL.1.3 ОФБ должна определять (назначение: процедуры) по управлению изменениями программного обеспечения с целью гарантировать установку самых свежих одобренных корректирующих заплат и прикладных коррекций для всего авторизованного ПО.»

Из элементов, конкретизирующих компонент FOS_POL.2, также выделим третий.

«FOS_POL.2.3 ОФБ должна определять (назначение: обязанности) по защите систем от вредоносного ПО, обучению использовать соответствующие защитные средства, докладывать об атаках вредоносного ПО и нейтрализовывать их последствия.»

Последний из элементов, конкретизирующих компонент FOS_POL.3, сформулирован в предлагаемом проекте следующим образом.

«FOS_POL.3.4 СФБ должна предоставлять (назначение: регуляторы), чтобы все криптографические ключи, ассоциированные с зашифрованными архивами или цифровыми подписями, были защищены и при необходимости доступны авторизованным лицам.»

В приведенной формулировке обратим внимание на аббревиатуру «СФБ». Конфиденциальность, целостность и доступность криптографических ключей в общем случае обеспечивается системной функциональностью безопасности, то есть сочетанием технических и организационных средств и мер.

То же справедливо по отношению к элементу FOS_POL.4.1:

«FOS_POL.4.1 СФБ должна предоставлять (назначение: регуляторы) для защиты программного обеспечения, данных и другой информации, требующей высокого уровня целостности, сделанных доступными на общедоступных системах.»

Семейство FOS_CNF «конфигурирование систем ИТ» включает такие аспекты, как разделение среды разработки и эксплуатационной среды и контроль доступа (компонент FOS_CNF.1), а также управление разделяемыми ресурсами и конфигурацией системы (компонент FOS_CNF.2).

Выделим два элемента, конкретизирующие компоненты семейства FOS_CNF.

«FOS_CNF.1.4 СФБ должна предоставлять (назначение: регуляторы) для ограничения доступа персонала ИТ-поддержки к библиотекам исходных текстов программ.»

«FOS_CNF.2.1 ОФБ должна определять (назначение: правила) разделения групп информационных сервисов, пользователей и информационных систем в сети.»

Семейство FOS_NET (сетевая безопасность систем ИТ) обладает особой гибкостью в плане сочетания технических и организационных регуляторов: во всех входящих в него элементах, кроме одного, фигурирует системная функциональность безопасности.

В данное семейство входят два компонента: FOS_NET.1 «сетевые сервисы» (определяет сетевые сервисы и доступ к ним) и FOS_NET.2 «сетевая безопасность» (ведает защитой сетей, безопасностью информации в них, конфиденциальностью и целостностью передаваемых данных).

Приведем определения двух элементов из семейства FOS_NET.

«FOS_NET.1.1 ОФБ должна определять (назначение: правила) для сетей и сетевых сервисов с разрешенным доступом, а также процедуры авторизации для определения того, кто и к каким сетям и сетевым сервисам имеет права доступа.»

«FOS_NET.2.7 СФБ должна предоставлять (назначение: меры) для увязывания прав сетевого доступа с определенными датами и временем суток.»

Семейство FOS_MON (мониторинг систем ИТ) включает определение процессов протоколирования/аудита, юридической поддержки, требований к средствам аудита и сигнализации. В него входят четыре компонента:

- FOS_MON.1 (регистрационные журналы) — определяет требования аудита, управления аудитом, проведение аудита, протоколируемую информацию, регистрацию действий системных администраторов;
- FOS_MON.2 (юридическая поддержка) — предписывает проводить юридические консультации до реализации процедур мониторинга;
- FOS_MON.3 (требования к сигнализации) — определяет установки параметров сигнализации и реагирование на сигналы тревоги.
- FOS_MON.4 (инструменты анализа регистрационных журналов) — определяет инструменты генерации отчетов на основе регистрационной информации.

Приведем формулировки двух элементов из этого семейства.

«FOS_MON.1.5 СФБ должна обеспечивать (назначение: протоколирование) действий системных администратора и оператора. Регистрационные записи должны включать время события или отказа, информацию о событии или отказе, сведения о том, какой системный счет и какой системный администратор или оператор оказались вовлеченными в событие.»

«FOS_MON.3.3 ОФБ должна определять (назначение: правила и процедуры), которые необходимо выполнять в случае получения сигнала тревоги, а также требуемые действия, включая временные ограничения, ответственных лиц и дисциплину докладов.»

Семейство FOS_PSN (управление персоналом систем ИТ) содержит требования к регуляторам для персонала автоматизированных систем. Оно состоит из трех компонентов:

- FOS_PSN.1 (авторизация пользователей) — определяет дисциплину регистрации пользователей, их аутентификации, правила сохранения конфиденциальности аутентификационной информации (такой, например, как пароли);
- FOS_PSN.2 (вредоносное ПО) — определяет обязанности по защите систем от вредоносного ПО;
- FOS_PSN.3 (использование систем) — определяет процедуры терминирования активных сеансов.

В предлагаемом проекте отсутствует конкретизация компонента FOS_PSN.2 в виде одного или нескольких элементов (возможно, это одно из случайных упущений; см. также выше описание элемента FOS_POL.2.3).

Приведем формулировки двух элементов рассматриваемого семейства.

«FOS_PSN.1.5 ОФБ должна определять (назначение: правила) подписания обязательств по предотвращению утери, компрометации или ненадлежащего использования аутентификационной информации, например, обя-

зательство хранить личный пароль в секрете, а пароли рабочей группы разделять только с членами группы.»

«FOS_PSN.2.4 ОФБ должна определять (назначение: правила) не оставлять без присмотра находящиеся в активном состоянии персональные компьютеры, компьютерные терминалы и принтеры, защищать их, когда они не используются, замками, паролями и другими средствами.»

Семейство FOS_OAS (эксплуатационные активы систем ИТ) включает требования к мерам по защите эксплуатационных активов, системных программ, резервных копий и аутентификационной информации. В семейство входят два компонента — FOS_OAS.1 «защита эксплуатационных активов» и FOS_OAS.2 «процедуры резервного копирования».

Компонент FOS_OAS.1 ведает стиранием эксплуатационной информации, контролем доступа, защитой инструментальных средств аудита и безопасным хранением системной документации, критериями принятия новых систем, правилами использования служебных программ, процедурами аутентификации для служебных программ, процедурами изменения эксплуатационного программного обеспечения, запретами на использование неавторизованного ПО, обязанностью применять выпускаемые производителями программные коррекции. Этот компонент конкретизируется в виде семнадцати элементов. Приведем один из них.

«FOS_OAS.1.17 ОФБ должна определять (назначение: процедуры) перехода на новые версии с учетом безопасности этих версий, появления в них новой защитной функциональности или числа и серьезности проблем безопасности в текущей версии.»

Из шести элементов, конкретизирующих компонент FOS_OAS.2, также приведем последний.

«FOS_OAS.2.6 ОФБ должна определять (назначение: требования безопасности) к организации резервного копирования на отдельных системах, чтобы гарантировать выполнение требований планов непрерывности производственной деятельности.»

Семейство FOS_RCD (протоколирование для систем ИТ) устроено совсем просто. Оно определяет хранимые записи о работе систем ИТ и содержит один компонент — FOS_RCD.1 «записи», ведающий защитой важных записей и протоколированием всех предполагаемых или реальных отказов.

Первый из двух элементов, конкретизирующих данный компонент, выглядит следующим образом.

«FOS_RCD.1.1 СФБ должна обеспечивать (назначение: меры) защиты с помощью регуляторов важных для организации записей от утери, разрушения или фальсификации.»

Класс FOA: пользовательские активы

Данный класс, содержащий требования к организационным регуляторам безопасности пользовательских активов автоматизированных систем, состоит из двух семейств.

Семейство FOA_PRO (защита конфиденциальности данных) определяет политику по отношению к пользовательским активам, включая такие аспекты, как конфиденциальность данных, криптография, управление пользовательскими активами, роли и обязанности. Оно состоит из одного пятиэлементного компонента — FOA_PRO.1 «конфиденциальность данных», который определяет защиту персональных данных, правила не использовать базы данных о персонале, содержащие личную информацию, правила получения общедоступной информации в соответствии с законодательными требованиями по защите данных. Определяются также роли и обязанности по защите пользовательских активов, обязанность владельца данных информировать уполномоченное должностное лицо, отвечающее в организации за защиту данных, своих предложениях по защите персональных данных.

Элемент FOA_PRO.1.2 формулируется следующим образом.

«FOA_PRO.1.2 ОФБ должна определять (назначение: правила) не использовать эксплуатационные базы данных, содержащие персональную информацию, для целей тестирования.»

Семейство FOA_INF (защита информации в пользовательских активах) также состоит из одного компонента. Оно определяет защиту данных, процедуры и правила.

Компонент FOA_INF.1 «защита данных» определяет защиту информации и физических носителей, руководства по хранению записей при транспортировке, процедуры получения разрешений на уничтожение записей, безопасность электронных коммуникаций, процедуры обработки, хранения и передачи информации, процедуры снабжения информации метками и обращения с ними.

Из тринадцати элементов, конкретизирующий данный компонент, приведем девятый.

«FOA_INF.1.9 СФБ должна обеспечивать (назначение: регуляторы) предоставления и использования привилегий.»

Класс FOB: производственная деятельность

Этот класс содержит требования к организационным регуляторам безопасности автоматизированных систем как составной части производственной деятельности. Он состоит из двух семейств.

Семейство FOB_POL (политики производственной деятельности) состоит из одного компонента — FOB_POL.1 «требования безопасности», который определяет производственную ценность задействованных информационных активов, требования безопасности отдельных производственных приложений, идентификацию всей информации, относящейся к производственным приложениям, роли и обязанности безопасности для реализации и сопровождения политик безопасности, процедуры для получения гарантий соответствия законодательным нормам на использование материалов.

Характерен четвертый из пяти элементов, конкретизирующих данный компонент.

«FOB_POL.1.4 ОФБ должна определять (назначение: роли и обязанности) и сведения для кандидатов на работу перед их зачислением.»

Семейство FOB_BCN (непрерывность производственной деятельности) также состоит из одного компонента — FOB_BCN.1 «анализ воздействия», определяющего анализ воздействия на непрерывность производственной деятельности, планы обеспечения непрерывности производственной деятельности путем сопровождения или восстановления производственных операций, изоляцию нарушений безопасности, специальный доступ, предоставляемый во время нарушений безопасности.

Последний из десяти элементов, конкретизирующих компонент FOB_BCN.1, формулируется следующим образом.

«FOB_BCN.1.10 ОФБ должна определять (назначение: правила) специального доступа к активам автоматизированной системы во время нарушений безопасности.»

Класс FOP: инфраструктура и оборудование

Данный класс содержит требования к организационным регуляторам безопасности инфраструктуры и оборудования автоматизированных систем. Он состоит из пяти семейств. Все они, кроме последнего, включают по одному компоненту.

Семейство FOP_MOB (мобильное оборудование) определяет требования, роли и обязанности по отношению к мобильному оборудованию, в том числе требования к физической защите, процедуры для соблюдения мер безопасности при использовании мобильных вычислительных устройств в общественных местах, правила использования персональных или собственных вычислительных устройств, правила для оборудования, оставляемого без присмотра.

Единственный компонент семейства FOP_MOB — FOP_MOB.1 «требования безопасности для мобильного оборудования» конкретизируется в виде семи элементов. Приведем формулировку третьего из них.

«FOP_MOB.1.3 СФБ должна обеспечивать (назначение: меры) защиты от рисков, связанных с использованием мобильных вычислительных устройств.»

Семейство FOP_RMM (съемное оборудование) определяет процедуры безопасности для съемного оборудования. В данном случае имеются в виду съемные носители и носители для резервных копий.

Единственный компонент семейства — FOP_RMM.1 «управление резервными носителями». Он определяет процедуры управления съемными компьютерными носителями, процедуры для безопасного выведения из эксплуатации носителей, содержащих информацию ограниченного доступа с учетом степени секретности, процедуры получения разрешений на вынос носителей из организации, процедуры стирания содержимого носителей многоразового использования, процедуры для резервных носителей с резервными копиями, процедуры восстановления.

Последний из пяти элементов, конкретизирующих компонент FOP_RMM.1, формулируется следующим образом.

«FOP_RMM.1.5 ОФБ должна определять (назначение: процедуры) стирания содержимого носителей многоразового использования, которые больше не нужны и должны быть вынесены из организации.»

Семейство FOP_RMT (удаленное оборудование) регламентирует обязанности и процедуры управления и использования удаленного оборудования и процедуры удаленного доступа к производственной информации. Из трех элементов, конкретизирующих единственный компонент се-

мейства FOP_RMT.1 «управление удаленным оборудованием», приведем последний.

«FOP_RMT.1.3 СФБ должна обеспечивать (назначение: меры) для запирания ключами или эквивалентные регуляторы для защиты ПК и терминалов от несанкционированного использования.»

Семейство FOP_SYS (системное оборудование) ведает резервными оборудованием и носителями, правилами хранения вредных или горючих веществ, процедурами проверки поступающих материалов, защитой кабельного хозяйства. Единственный компонент семейства – FOP_SYS.1 «управление системным оборудованием» – конкретизируется в виде одиннадцати элементов. Приведем первый из них.

«FOP_SYS.1.1 ОФБ должна определять (назначение: правила) хранения резервных оборудования и носителей на безопасном расстоянии от основной производственной площадки, чтобы избежать их повреждения в случае аварии на упомянутой площадке.»

Последним, пятым семейством класса FOP является FOP_MNG (управление инфраструктурой). Оно включает два компонента – FOP_MNG.1 «физическая безопасность» и FOP_MNG.2 «средства поддержки электропитания». Первый из них определяет физическую безопасность помещений и инфраструктуры, процедуры использования инфраструктуры обработки информации, ограничения на доступ к областям погрузки/разгрузки, использование инфраструктуры обработки информации, защиту инфраструктуры протоколирования, физическое разделение инфраструктуры обработки информации, контроль доступа к областям, где располагается информация ограниченного доступа. Второй компонент ведает контролем средств поддержки электропитания и использованием резервного генератора.

Приведем пятый и седьмой из шестнадцати элементов, конкретизирующих компонентов FOP_MNG.1.

«FOP_MNG.1.5 ОФБ должна определять (назначение: требования безопасности) к использованию инфраструктуры обработки информации.»

«FOP_MNG.1.7 ОФБ должна определять (назначение: регуляторы) для защиты инфраструктуры протоколирования от внесения несанкционированных изменений и создания эксплуатационных проблем.»

Из четырех элементов, конкретизирующих компонент FOP_MNG.2, приведем последний.

«FOP_MNG.2.4 ОФБ должна определять (назначение: требования безопасности) к расположению аварийных выключателей электропитания вблизи от аварийных выходов из аппаратных, чтобы облегчить быстрое выключение электропитания в случае возникновения аварийной ситуации.»

Класс FOT: сторонние организации

Данный класс содержит требования к организационным регуляторам, относящимся к сторонним организациям. Он включает два семейства – FOT_COM (обязательства сторонних организаций) и FOT_MNG (управление взаимодействием со сторонними организациями). В предлагаемом проекте описано только второе из них, однако в него включены требования к обязательствам сторонних организаций.

Семейство FOT_MNG регламентирует управление взаимодействием со сторонними организациями, обязательства сторонних организаций, политику безопасности, аутсорсинг и требования безопасности. Это семейство включает два компонента – FOT_MNG.1 «аутсорсинг» и FOT_MNG.2 «требования безопасности к взаимодействию со сторонними организациями».

Компонент FOT_MNG.1 «аутсорсинг» определяет план передачи необходимой информации, лицензионные соглашения, права собственности на программный код и права интеллектуальной собственности. Из двух конкретизирующих его элементов приведем второй.

«FOT_MNG.1.2 ОФБ должна определять (назначение: требования безопасности) к лицензионным соглашениям, правам собственности на программный код и правам интеллектуальной собственности, сертификацию качества и правильности выполненной работы, порядок урегулирования ситуации в случае провала сторонней организации, права доступа для проведения аудита качества и правильности сделанной работы, контрактные требования к качеству кода и тестирования перед установкой с целью выявить троянский код, если сторонней организации поручается разработка программного обеспечения.»

Компонент FOT_MNG.2 «требования безопасности к взаимодействию со сторонними организациями» определяет все требования безопасности, вытекающие из работы со сторонними организациями, достаточный общий контроль,

правила не предоставлять доступ к информации организации, управление рисками, являющимися следствием взаимодействия со сторонними организациями.

Данный компонент конкретизируется в виде шести элементов. Приведем четвертый из них.

«FOT_MNG.2.4 ОФБ должна определять (назначение: правила) не предоставлять сторонним организациям доступ к информации организации, если только не установлены соответствующие регуляторы и не подписано соглашение, определяющее границы и условия подключения или доступа и порядок выполнения работ.»

Класс FOM: управление

Данный класс содержит требования к управлению организационными регуляторами. Он состоит из пяти семейств.

Семейство FOM_PRM (управление параметрами безопасности) определяет использование криптографии и полномочий. В него входят два компонента – FOM_PRM.1 «использование криптографии» и FOM_PRM.2 «разделение полномочий».

Компонент FOM_PRM.1 определяет подход к управлению ключами, в том числе методы защиты криптографических ключей и восстановления зашифрованной информации. В предлагаемом проекте он конкретизируется одним, весьма пространным элементом.

«FOM_PRM.1.1 ОФБ должна определять (назначение: требования безопасности) к административному подходу к использованию криптографических регуляторов в организации, подходу к управлению ключами, в том числе к методам защиты криптографических ключей и восстановления зашифрованной информации в случае утери, компрометации или повреждения ключей; роли и обязанности по проведению политики в жизнь; законы и национальные ограничения, которые могут повлиять на использование криптографических технологий в различных странах и на вопросы передачи через границы зашифрованных информационных потоков в политике безопасности организации.»

Компонент FOM_PRM.2 конкретизируется двумя элементами. Приведем формулировку первого из них.

«FOM_PRM.2.1 ОФБ должна определять (назначение: правила) разделения полномочий с целью уменьшить возможности для несанкционированной модификации или ненадлежащего использования активов, разделения инициации события и его санкционирования.»

Семейство FOM_CLS (управление классификацией активов) включает два компонента – FOM_CLS.1 «категорирование» и FOM_CLS.2 «идентификация активов». Компонент FOM_CLS.1 конкретизируется одним элементом.

«FOM_CLS.1.1 ОФБ должна определять (назначение: требования безопасности) к категорированию записей на типы, записи баз данных, журналы транзакций, регистрационные журналы и организационные процедуры, с детальным описанием сроков хранения и носителей для каждого типа.»

Компонент FOM_CLS.2 конкретизируется тремя элементами. Приведем второй из них.

«FOM_CLS.2.2 ОФБ должна определять (назначение: требования безопасности) к составлению и сопровождению описи всех важных активов.»

Семейство FOM_PSN (управление должностными обязанностями, связанными с безопасностью) ориентировано на владельцев активов и администраторов безопасности. Как и предыдущее, оно включает два компонента – FOM_PSN.1 «владение активами» и FOM_PSN.2 «администраторы безопасности». В свою очередь, каждый из компонентов данного семейства конкретизируется одним элементом. Приведем их формулировки.

«FOM_PSN.1.1 ОФБ должна определять (назначение: требования безопасности) к назначению определенного владельца для каждого актива.»

«FOM_PSN.2.1 ОФБ должна определять (назначение: требования безопасности) к назначению специального ответственного администратора для каждого регулятора безопасности.»

Сходным образом устроено семейство FOM_ORG (управление организацией безопасности), ведающее обязанностями и составом комиссии по управлению и включающее компоненты FOM_ORG.1 «обязанности комиссии по управлению» и FOM_ORG.2 «состав комиссии по управлению». Отметим, что для этих компонентов определены зависимости от описанного выше компонента FOD_ORG.1, который, согласно тексту предлагаемого проекта технического доклада, зависит от FOM_ORG.1 и FOM_ORG.2. Приведем формулировки конкретизирующих элементов.

«FOM_ORG.1.1 ОФБ должна определять (назначение: требования безопасности) к тому, что координационная группа обеспечивает согласованность деятельности в области безопасности с политикой безопасности, одобряет конкретные методики и процессы информационной безопасности, отслеживает существенные изменения угроз и уязвимость информационных активов по отношению к угрозам, оценивает адекватность и координирует реализацию специальных регуляторов информационной безопасности для новых систем и сервисов, поощряет видимую поддержку информационной безопасности во всей организации.»

«FOM_ORG.2.1 ОФБ должна определять (назначение: требования безопасности) к тому, что деятельность в области безопасности координируется назначенными представителями руководства и различных частей организации с соответствующими ролями и производственными обязанностями.»

Семейство FOM_INC (управление докладами о событиях, связанных с безопасностью) состоит из одного компонента FOM_INC.1 «доклады об обнаруженных проблемах безопасности», который конкретизируется в виде двух элементов. Приведем второй из них.

«FOM_INC.1.2 ОФБ должна определять (назначение: правила) запрета попыток доказать существование предполагаемой уязвимости путем попыток ее использования.»

Таковы, в общих чертах, функциональные требования безопасности для автоматизированных систем, включенные в предлагаемый проект технического доклада ISO/IEC PDTR 19791.

Требования доверия к безопасности для автоматизированных систем

Общая характеристика требований доверия к безопасности для автоматизированных систем

В приложении С, являющемся нормативной частью предлагаемого проекта технического доклада, определены десять новых по сравнению со стандартом ISO/IEC 15408-3 классов требований доверия, содержащих пятьдесят одно семейство:

- Класс ASP (оценка системного профиля защиты):
  - ASP_INT (введение СПЗ),
  - ASP_CCL (утверждения о соответствии),
  - ASP_ECD (определение дополнительных требований безопасности),
  - ASP_SPD (определение задачи безопасности),
  - ASP_OBJ (цели безопасности),
  - ASP_REQ (требования безопасности),
  - ASP_DMI (введение для домена безопасности),
  - ASP_DMC (утверждения о соответствии для домена безопасности),
  - ASP_DMP (определение задачи безопасности для домена безопасности),
  - ASP_DMO (цели безопасности для домена безопасности),
  - ASP_DMR (требования для домена безопасности);
- Класс ASS (оценка системного задания по безопасности):
  - ASS_INT (введение СЗВ),
  - ASS_CCL (утверждения о соответствии),
  - ASS_ECD (определение дополнительных требований безопасности),
  - ASS_SPD (определение задачи безопасности),
  - ASS_OBJ (цели безопасности),
  - ASS_REQ (требования безопасности),
  - ASS_TSS (краткая спецификация СОО),
  - ASS_DMI (введение для домена безопасности),
  - ASS_DMC (утверждения о соответствии для домена безопасности),
  - ASS_DMP (определение задачи безопасности для домена безопасности),
  - ASS_DMO (цели безопасности для домена безопасности),
  - ASS_DMR (требования для домена безопасности);
- Класс AOD (руководства автоматизированной системы):
  - AOD_OCD (определение конфигурации автоматизированной системы),
  - AOD_ADM (руководство администратора автоматизированной системы),
  - AOD_USR (руководство пользователя автоматизированной системы);
- Класс ASD (архитектурная, проектная и конфигурационная документация автоматизированной системы):

  - ASD_SAD (архитектурный проект автоматизированной системы),
  - ASD_IFS (функциональная спецификация интерфейсов автоматизированной системы),
  - ASD_SSD (проект подсистем автоматизированной системы),
  - ASD_CMP (проект неделимых компонентов автоматизированной системы),
  - ASD_IMP (представление реализации),
  - ASD_COM (концепция безопасности автоматизированной системы);

- Класс AOC (управление конфигурацией автоматизированной системы):
  - AOC_OBM (базовая конфигурация автоматизированной системы),
  - AOC_ECP (оцененные компонентные продукты),
  - AOC_PPC (соответствие профилям защиты),
  - AOC_NCP (неоцененные компонентные продукты);
- Класс AOT (тестирование автоматизированной системы):
  - AOT_FUN (функциональное тестирование автоматизированной системы),
  - AOT_COV (покрытие тестами автоматизированной системы),
  - AOT_DPT (глубина тестирования автоматизированной системы),
  - AOT_IND (независимое тестирование),
  - AOT_REG (регрессионное тестирование);
- Класс AOV (анализ уязвимостей автоматизированной системы):
  - AOV_MSU (неправильное применение автоматизированной системы),
  - AOV_SOF (стойкость функций безопасности действующего COO),
  - AOV_VLA (анализ уязвимостей);
- Класс AOL (поддержка жизненного цикла автоматизированной системы):
  - AOL_DVS (идентификация мер безопасности автоматизированной системы);
- Класс ASI (установка и поставка системной функциональности безопасности):
  - ASI_AWA (отработка навыков),
  - ASI_CMM (уведомление),
  - ASI_SIC (проверка производственной совместимости);
- Класс ASO (записи в автоматизированной системе):
  - ASO_RCD (записи функционирования организационных регуляторов),
  - ASO_VER (верификация организационных регуляторов),
  - ASO_MON (мониторинг организационных регуляторов).

Между девятью новыми классами требований доверия к безопасности, определенными в предлагаемом проекте, и классами, описанными в стандарте ISO/IEC 15408-3, существуют очевидные параллели: ASP является модификацией APE (оценка профиля защиты) для автоматизированных систем, ASS – ASE (оценка задания по безопасности), AOD – AGD (руководства), ASD – ADV (разработка), AOC – ACM (управление конфигурацией), AOT – ATE (тестирование), AOV – AVA (оценка уязвимостей), AOL – ALC (поддержка жизненного цикла), ASI – ADO (поставка и эксплуатация). И только класс ASO можно считать по-настоящему новым, не имеющим аналога в стандарте ISO/IEC 15408-3.

В соответствии с целью рассматриваемого проекта, новые требования доверия к безопасности охватывают весь жизненный цикл автоматизированных систем. На этапе разработки/интеграции применимы компоненты семейств AOL_DVS, ASD_IMP, ASD_SSD, ASD_CMP, ASD_IFS, ASD_SAD, ASD_COM, AOD_USR, AOD_ADM, AOD_OCD.

Этап ввода в эксплуатацию охватывается компонентами семейств AOC_OBM, AOC_ECP, AOC_PPC, AOC_NCP, AOT_FUN, AOT_COV, AOT_DPT, AOV_MSU, AOV_SOF, ASI_AWA, ASI_CMM, ASI_SIC, ASO_RCD, ASO_VER, AOT_IND.

На этапе производственной эксплуатации применимы компоненты семейств AOD_USR, AOD_ADM, AOD_OCD, AOC_OBM, AOC_ECP, AOC_PPC, AOC_NCP, AOV_MSU, ASI_AWA, ASI_CMM, ASI_SIC, ASO_RCD, ASO_VER, ASO_MON.

Наконец, этап сопровождения обслуживается компонентами семейств AOV_MSU, AOV_VLA и AOT_REG.

По традиции, идущей от стандарта ISO/IEC 15408-3, классы ASP и ASS стоят особняком, хотя требования класса ASS можно отнести к этапу разработки/интеграции. В предлагаемом проекте отсутствует какая-либо связь между новыми требованиями и определенными в стандарте ISO/IEC 15408-3 оценочными уровнями доверия.

По сравнению со стандартом ISO/IEC 15408-3 в предлагаемом проекте технического доклада имеются два отличия в форме описания требований доверия к безопасности.

Во-первых, элементы действий разработчика переименованы в элементы действий разработчика/интегратора, чтобы отразить тот факт, что

автоматизированная система может строиться системным интегратором, отличным от разработчика компонентов и продуктов, использованных в АС, и оба они (и разработчик, и интегратор) могут сотрудничать при изготовлении и поставке необходимых свидетельств. Во-вторых, в некоторых случаях за изготовление свидетельств отвечает руководство АС, поэтому в соответствующих семействах элементы действий по предоставлению свидетельств идентифицированы как действия руководителей.

Ниже представлен краткий обзор предложенных в проекте 19791 классов требований доверия к безопасности для автоматизированных систем.

Класс ASP: оценка системного профиля защиты

Оценка системного профиля защиты (СПЗ) требуется для того, чтобы продемонстрировать, что СПЗ является обоснованным и внутренне непротиворечивым и, если он выведен из одного или нескольких СПЗ или пакетов, он является их корректным представлением. Перечисленные свойства необходимы, чтобы СПЗ можно было использовать как основу последующих оценок СОО.

Данный класс включает одиннадцать семейств. В общем и целом он аналогичен классу APE (оценка профиля защиты) из стандарта ISO/IEC 15408 3, а отличия от упомянутого класса объясняются различиями в структуре ПЗ и СПЗ. Этим отличиям мы и уделим основное внимание.

Важнейшее отличие СПЗ от ПЗ состоит в том, что СПЗ включает общую часть, применимую к АС в целом, а также части, специфичные для отдельных доменов безопасности. Требования первых шести семейств рассматриваемого класса (ASP_INT, ASP_CCL, ASP_ECD, ASP_SPD, ASP_OBJ, ASP_REQ) обслуживают общую часть, а пять остальных (ASP_DMI, ASP_DMC, ASP_DMP, ASP_DMO, ASP_DMR) — отдельные домены.

Семейство ASP_INT (введение СПЗ) предназначено для описания системного объекта оценки в повествовательном стиле на четырех уровнях абстракции:

- идентификатор СПЗ/СОО;
- обзор СОО;
- описание СОО;
- организация доменов безопасности.

Оценка введения СПЗ необходима для демонстрации того, что СПЗ и СОО правильно идентифицированы, что СОО корректно описан на четырех уровнях абстракции и что эти четыре описания согласованы между собой.

Данное семейство состоит из одного компонента — ASP_INT.1 «введение СПЗ». Из конкретизирующих его элементов приведем следующие.

«ASP_INT.1.1D Разработчик/интегратор должен представить введение ПЗ.»

«ASP_INT.1.4C Обзор СОО должен обобщать использование и основные особенности безопасности СОО.»

«ASP_INT.1.6C Обзор СОО должен идентифицировать все внешние автоматизированные системы, требующиеся для функционирования СОО.»

«ASP_INT.1.9C Описание СОО должно содержать описание организации созданных доменов безопасности и их идентификаторы, а также физический масштаб и границы каждого домена.»

Цель семейства ASP_CCL (утверждения о соответствии) — определить обоснованность различных утверждений о соответствии, а именно:

- утверждений о соответствии «Общим критериям»;
- утверждений о соответствии системному профилю защиты;
- утверждений о соответствии профилям защиты;
- утверждений о соответствии пакетам требований.

Приведем один из элементов, конкретизирующих единственный компонент семейства — ASP_CCL.1 «утверждения о соответствии».

«ASP_CCL.1.2D Разработчик/интегратор должен представить обоснование утверждений о соответствии.»

Дополнительными называются требования безопасности, основанные не на компонентах из стандарта ISO/IEC 15408 или данного технического доклада, а на дополнительных компонентах, определенных автором СПЗ. Оценка определения дополнительных компонентов, регламентируемая семейством ASP_ECD, нужна для того, чтобы убедиться в их ясности, недвусмысленности и необходимости, то есть в том, что они не могут быть естественным образом выражены с использованием существующих компонентов.

Вновь ограничимся цитированием одного из элементов, конкретизирующих единственный компонент семейства.

«ASP_ECD.1.5C Дополнительные компоненты должны состоять из измеримых и объективных элементов, таких что

соответствие или несоответствие этим элементам может быть доказано.»

Семейство ASP_SPD (определение задачи безопасности) служит для оценки данного в СПЗ определения задачи безопасности, решаемой системным объектом оценки, его эксплуатационной средой и средой разработки. Один из элементов содержания и представления свидетельств, конкретизирующих единственный компонент семейства, сформулирован в предлагаемом проекте следующим образом.

«ASP_SPD.1.2C Все риски должны быть описаны в терминах угроз и уязвимостей. Для каждой угрозы должен быть описан ее агент, актив и вредоносное действие.»

Цели безопасности — это сжатое изложение предполагаемого ответа на задачу безопасности, сформулированную средствами семейства ASP_SPD. Оценка целей безопасности, регламентируемая семейством ASP_OBJ, требуется для того, чтобы доказать, что цели безопасности адекватно и полно отвечают постановке задачи безопасности, что разделение этой задачи между СОО, его средой разработки, эксплуатационной средой и внешними автоматизированными системами ясно определено, и что цели безопасности внутренне непротиворечивы.

Приведем несколько фрагментов из описания единственного компонента семейства.

«Зависимости: ASP_SPD.1 Определение задачи безопасности»

«ASP_OBJ.1.8C Изложение целей безопасности должно определять цели безопасности для внешних автоматизированных систем.»

Цель семейства ASP_REQ (требования безопасности) — удостовериться в том, что требования безопасности ясны, недвусмысленны и каноничны. Данное семейство включает два компонента. ASP_REQ.1 охватывает фиксированные требования безопасности, ASP_REQ.2 — требования, выведенные из целей безопасности СОО, среды разработки и эксплуатационной среды.

Приведем формулировку одного из элементов, конкретизирующих компонент ASP_REQ.2 «производные требования безопасности».

«ASP_REQ.2.7C Обоснование требований безопасности должно демонстрировать, что системная функциональность безопасности отвечает всем целям безопасности для СОО и эксплуатационной среды.»

Следующие пять семейств класса ASP:

- ASP_DMI (введение для домена безопасности),
- ASP_DMC (утверждения о соответствии для домена безопасности),
- ASP_DMP (определение задачи безопасности для домена безопасности),
- ASP_DMO (цели безопасности для домена безопасности),
- ASP_DMR (требования для домена безопасности)

ориентированы на отдельные домены безопасности, для каждого из которых в системном профиле защиты формулируются специфические задача, цели и требования безопасности. В общем и целом требования к рассматриваемым разделам СПЗ аналогичны требованиям к общей части СПЗ, с естественной модификацией некоторых аспектов.

Например, в семействе ASP_DMI (введение для домена безопасности) фигурируют следующие четыре уровня абстракции:

- идентификатор домена безопасности;
- обзор домена безопасности;
- описание домена безопасности;
- взаимосвязь с другими доменами безопасности.

Класс ASS: оценка системного задания по безопасности

Данный класс аналогичен рассмотренному выше классу ASP с заменой аббревиатуры «СПЗ» на «СЗБ» и другими более содержательными, но также естественными изменениями. (Несомненно, так же считали и авторы рассматриваемого проекта технического доклада, поскольку даже дефекты в описании этих классов общие.)

Наиболее существенным отличием класса ASS от ASP является присутствие дополнительного семейства — ASS_TSS (краткая спецификация СОО). Назначение краткой спецификации — дать потенциальным потребителям системного объекта оценки общее представление о том, как разработчик/интегратор предполагает обеспечивать требуемые системную функциональность безопасности и доверие к безопасности системы. Оценка краткой спецификации СОО необходима для установления того, что вся системная функциональность безопасности освещена должным образом, и что краткая спецификация согласована с другими повествовательными описаниями СОО.

Приведем формулировку одного из элементов, конкретизирующих единственный компонент семейства.

«ASS_TSS.1.2C В краткой спецификации СОО должно быть описано, как в СОО представлена каждая из требуемых мер доверия к безопасности системы.»

Класс AOD: руководства автоматизированной системы

Цель данного класса требований доверия – оценить адекватность документации, описывающей интеграцию и эксплуатацию автоматизированной системы. Подобная документация ориентирована как на интеграторов АС, доверенных администраторов и неадминистративных пользователей, неправильные действия которых способны оказать вредоносное влияние на защитное поведение и характеристики автоматизированной системы, так и на обычных пользователей, от неправильных действий которых может пострадать способность автоматизированной системы обеспечивать требуемые защитные возможности для собственных данных этих пользователей.

Руководства пользователя и администратора содержат информацию, относящуюся к технологическим аспектам автоматизированной системы, а также к организационным процессам в АС.

Таким образом, деятельность по применению требований класса AOD тесно связана с процессами и процедурами, определенными организационными требованиями безопасности.

Приведем фрагмент описания класса AOD.

«С.4.2 Замечания по применению
Все требования к ОФБ, определенные в СЗБ, относящиеся к требуемому поведению персонала, должны быть описаны в соответствующем руководстве автоматизированной системы.
Режим сопровождения, однопользовательский режим и любой специальный режим функционирования, в который система переходит после ошибки или исключительной ситуации, должен быть идентифицирован и рассмотрен на предмет последствий и контекста для поддержания безопасности функционирования.
Руководство администратора должно определять следующие аспекты:

- *функции и привилегии, которые должны контролироваться;*
- *типы регуляторов, требуемые для этих целей;*
- *причины для подобного контроля.*

Предупреждающие сообщения должны освещать ожидаемые эффекты, возможные побочные эффекты и возможное взаимодействие с другими функциями и привилегиями.
Руководство должно описывать администрирование автоматизированной системы как целого в дополнение к администрированию отдельных продуктов и подсистем. В комплект документации должно входить не только руководство по администрированию прикладных программ, но и по администрированию всей автоматизированной системы.»

Класс AOD состоит из трех семейств.

Цель определения конфигурации автоматизированной системы, контролируемой семейством AOD_OCD, – специфицировать относящиеся к безопасности конфигурационные параметры, поддерживающие интеграцию компонентов автоматизированной системы и позволяющие функциям безопасности АС реализовывать и проводить в жизнь концепцию безопасного функционирования и ассоциированные политики.

Семейство AOD_OCD состоит из двух компонентов – AOD_OCD.1 «определение конфигурации автоматизированной системы» и AOD_OCD.2 «верификация определения конфигурации автоматизированной системы». Приведем формулировку одного из элементов, конкретизирующих оба компонента.

«AOD_OCD.1.2C Руководство по конфигурированию должно описывать использование параметров безопасности, конфигурируемых СОО, для реализации и проведения в жизнь системных политик безопасности.»

Второй компонент отличается от первого одной дополнительной зависимостью (от AOD_OCD.1) и одним дополнительным элементом:

«AOD_OCD.2.2E Оценщик должен независимо проверить применение конфигурационных параметров, определенных в руководстве по конфигурированию.»

Аналогичную структуру имеют также семейства AOD_ADM (руководство администратора автоматизированной системы) и AOD_USR (руководство пользователя автоматизированной системы).

Руководство администратора автоматизированной системы предназначено для применения лицами, ответственными за конфигурирование, сопровождение и администрирование СОО способами, корректными по отношению к регуляторам безопасности. Политика безопасности, процедуры, правила, обязанности и другие требования безопасности, определенные эксплуатационными требованиями и предназначенные для применения администратором, должны быть описаны в этом руководстве. Руководство администратора автоматизированной системы призвано помочь администраторам разобраться в регуляторах безопасности, как технических, так и организацион-

ных, предоставляемых СОО и требующих от администратора выполнения действий, критичных для безопасности, и в функциях, предоставляющих критичную для безопасности информацию.

Приведем формулировку элемента, специфичного для компонента AOD_ADM.2 (аналогичный элемент присутствует в семействе AOD_USR).

«AOD_ADM.2.2E Оценщик должен независимо проверить применение инструкций, присутствующих в руководстве администратора, путем (выбор: бесед с персоналом, выборки фрагментов руководства администратора, (назначение: другими методами)).»

Класс ASD: архитектурная, проектная и конфигурационная документация автоматизированной системы

Назначение данного класса — оценить принятые архитектурные, проектные и конфигурационные решения, чтобы убедиться в их достаточности и полноте в плане выполнения функциональных требований, предъявляемых к автоматизированной системе. Средством оценки служит анализ представленной документации, освещающей эти решения. Еще одна цель класса — проверить, отражают ли архитектура, проект и конфигурация автоматизированной системы требования безопасности, которые предъявляются к различным подсистемам и компонентам АС.

В класс ASD входят шесть семейств требований доверия к безопасности. Цель семейства ASD_SAD (архитектурный проект автоматизированной системы) — детальное изучение свойств безопасности, встроенных в АС, в терминах ее структуры (подсистем, компонентов, внешних автоматизированных систем), взаимосвязей (интерфейсов, межсоединений, потоков данных и управления) и назначения (прослеживание связей с концепцией безопасного функционирования и требованиями безопасности для АС) и получение различной степени доверия к безопасности различных частей автоматизированной системы. Эта информация служит базой для понимания и выполнения и других аспектов оценивания АС, таких как выработка стратегии, планов и процедур тестирования автоматизированной системы.

Более точно архитектурный проект отражает следующие аспекты автоматизированной системы:

- определение подсистем, составляющих АС;
- распределение функциональности по этим подсистемам;
- распределение степеней доверия к этим подсистемам;
- внутренние и внешние интерфейсы подсистем и функциональность, обеспечиваемая через определенные интерфейсы;
- взаимосвязь подсистем и проходящие по межсоединениям информационные потоки;
- внешние автоматизированные системы (среда), интерфейсы и взаимосвязи АС с ними;
- информационные потоки между АС и внешними автоматизированными системами.

Семейство состоит из одного компонента. Один из элементов, конкретизирующих этот компонент, формулируется следующим образом.

«ASD_SAD.1.6C Описание архитектуры должно описывать механизмы самозащиты организационных регуляторов на должном уровне, соответствующем результатам анализа рисков.»

Семейство ASD_IFS (функциональная спецификация интерфейсов автоматизированной системы) имеет дело с описаниями функций безопасности АС в том виде, как они представлены на специфицированных интерфейсах, и поведения АС, видимого на этих интерфейсах.

Из элементов, конкретизирующих единственный компонент семейства, приведем следующий.

«ASD_IFS.1.2C Функциональная спецификация интерфейсов должна быть внутренне непротиворечивой.»

Семейство ASD_SSD имеет дело с проектом подсистем автоматизированной системы, цель которого как свидетельства — предоставить описание следующих аспектов:

- подсистемы;
- распределение функциональности безопасности между этими подсистемами;
- интерфейсы подсистем и функциональность, предоставляемая посредством специфицированных интерфейсов;
- взаимосвязь подсистем;
- потоки сообщений между подсистемами;
- составные компоненты подсистем.

Приведем формулировку одного из элементов, конкретизирующих единственный компонент семейства.

«ASD_SSD1.4C Проект подсистем должен идентифицировать все аппаратное и программное обеспечение, в том числе встроенное, требуемое системной функциональностью безопасности, отведенной подсистемам.»

Назначение проекта неделимых компонентов автоматизированной системы как свидетельства (обслуживается семейством ASD_SSD) – предоставить описание следующих аспектов:

- распределение функциональности безопасности между компонентами;
- интерфейсы неделимых компонентов;
- функциональность, предоставляемая посредством специфицированных интерфейсов компонентов;
- ссылки на детальное описание требований к компонентам, проектную и справочную документацию, если таковая существует.

Один из элементов, конкретизирующих единственный компонент семейства, формулируется следующим образом.

«ASD_SSD.1.7C Проект компонентов должен являться точной и полной реализацией функциональных требований безопасности автоматизированной системы.»

Назначение семейства ASD_IMP (представление реализации) -поддержать оценку критичной функциональности АС, разработанной исключительно для целей интеграции компонентов в автоматизированную систему. Примеры объектов применения данного семейства – интегрирующие программы или процедуры завершения работы АС.

Таким образом, в контексте семейства ASD_IMP критичная функциональность автоматизированной системы – это не функциональность, присутствующая в компонентах в том виде, как они были построены или оценены, однако при проведении оценки автоматизированной системы может потребоваться переоценка некоторых ранее оцененных частей компонентов в конкретной конфигурации или среде, идентифицированной до или в ходе оценки АС.

Приведем формулировку одного из элементов, конкретизирующих единственный компонент семейства.

«ASD_IMP1.3C Представление реализации должно описывать функциональность безопасности, обеспечиваемую интеграцией компонентов, в терминах конкретных требований к конфигурации.»

Концепция безопасности автоматизированной системы, обслуживаемая семейством ASD_COM, описывает политики безопасности, свойства и характеристики АС в том виде, как они предоставляются и проводятся в жизнь в поддержку производственных функций. В число аспектов концепции безопасности автоматизированной системы входят:

- концепция управления информационными потоками по межсоединениям в пределах АС;
- концепция управления информационными потоками по соединениям с внешними автоматизированными системами;
- концепция управления локальным и удаленным доступом к АС;
- концепция управления доступом к ресурсам АС на основе правил контроля доступа;
- концепция режимов работы АС и управления операциями, специфичными для определенных режимов.

В семейство ASD_COM входит единственный компонент, один из элементов которого выглядит следующим образом.

«ASD_COM.1.4C Документированная эксплуатационная политика АС должна идентифицировать системные средства управления локальным и удаленным доступом к АС.»

Можно видеть, что класс ASD является аналогом класса ADV из стандарта ISO/IEC 15408-3, однако довольно отдаленным.

Класс AOC: управление конфигурацией автоматизированной системы

Цель управления конфигурацией (УК) в процессе оценки состоит в обеспечении доверия к тому, что оценщик имеет дело с корректными версиями всех компонентов автоматизированной системы для всех прочих действий по оценке. Следовательно, оно применяется к мерам в среде разработки и интеграции, а не в эксплуатационной среде. После развертывания и интеграции АС оцененная система управления конфигурацией остается в среде разработки и интеграции. Управление конфигурацией может применяться к оцененным и неоцененным продуктам, входящим в состав АС.

Класс AOC предоставляет нетехнические меры, позволяющие персоналу, отвечающему за безопасность, управлять защитными аспектами АС и ее конфигурацией в процессе эксплуатации и контролировать изменения в АС, связанные с ее функциональностью безопасности. Управление конфигурацией безопасности определяет и описывает:

- компоненты АС в том виде, как они определены в конфигурации разработки;

- интеграционную конфигурацию АС, включающую специализированную функциональность для обеспечения интероперабельности;
- эксплуатационную конфигурацию, определяющую установки параметров для эксплуатационной конфигурации компонентов.

Требования класса АОС направлены также на то, чтобы убедиться в наличии политик и процедур контроля изменений и в их эффективном применении в АС, включая ограничения доступа для контроля изменений. Четыре семейства, входящие в класс АОС, определяют процессы и процедуры, позволяющие персоналу, отвечающему за безопасность, решать, что входит в конфигурацию АС, прослеживать и сопровождать АС и каждый из критически важных компонентов, входящих в состав АС в различных конфигурациях. Конфигурационные определения включают аспекты разработки, интеграции, эксплуатации и непрерывности функционирования.

Семейство АОС_ОВМ (базовая конфигурация автоматизированной системы) определяет оцененную конфигурацию АС и ее защитные компоненты, а также средства, с помощью которых планы и процедуры управления конфигурацией безопасности прослеживают базовую конфигурацию и контролируют вносимые в нее изменения. Семейство идентифицирует и прослеживает как технические, так и организационные регуляторы, связанные с функциями безопасности АС и их взаимосвязями.

Семейство АОС_ОВМ, аналогично представленному выше семейству AOD_OCD, содержит два иерархически связанных компонента — АОС_ОВМ.1 «базовая конфигурация автоматизированной системы» и АОС_ОВМ.2 «верификация базовой конфигурации автоматизированной системы». Приведем формулировку одного из элементов, конкретизирующих оба компонента.

«AOC_OBM.1.3D Система УК должна выдавать текущую базовую конфигурацию автоматизированной системы.»

Семейство АОС_ECP (оцененные компонентные продукты) определяет пакет требований доверия к требованиям к эксплуатационным параметрам для компонентов АС, построенных из ранее оцененных продуктов. При создании автоматизированной системы из компонентов-продуктов необходимо специфицировать требуемый уровень доверия, исходя из производимых действий по разработке и интеграции. Если используются готовые коммерческие продукты, то обычно в каких-либо специальных действиях по разработке для данной АС нет нужды. Следовательно, доверие может быть обеспечено произведенной ранее оценкой и сертификацией продукта, например, наличием формального сертификата соответствия ОУД4.

Семейство имеет стандартную для данного класса организацию. Приведем формулировку одного из элементов, конкретизирующих оба иерархически связанных компонента.

«AOC_ECP.1.2C Должны быть приведены формулировка результатов оценки или независимый сертификационный отчет и ЗБ для оцененных ранее продуктов.»

Семейство АОС_РРС (соответствие профилям защиты) определяет требования доверия для соответствия конкретному ПЗ. В качестве свидетельства должен быть представлен сертификационный отчет, включающий применимое ЗБ. В эксплуатационной среде компоненты-продукты могут иметь конкретные значения эксплуатационных параметров, которые должны быть корректно определены.

Приведем формулировку одного из общих элементов, относящихся к действиям разработчика/интегратора.

«AOC_PPC.1.2D Разработчик/интегратор должен специфицировать эксплуатационные параметры для каждого компонента-продукта.»

Элемент, специфичный для компонента АОС_РРС.2 «верификация соответствия профилям защиты», формулируется следующим образом.

«AOC_PPC.2.2E Оценщик должен подтвердить, что условия эксплуатации, описанные в формулировке результатов оценки или в независимом сертификационном отчете об оцененных продуктах, соответствуют требованиям эксплуатационной среды автоматизированной системы.»

Семейство АОС_NCP (неоцененные компонентные продукты) определяет пакет требований доверия к требованиям к эксплуатационным параметрам для компонентов АС, построенных из неоцененных продуктов. Для производственных прикладных программ, разработанных специально для данной автоматизированной системы, на этапе разработки могут быть получены те же свидетельства доверия, что требуются для оценки продуктов.

Приведем формулировку элемента, специфичного для компонента АОС_NCP.2 «верификация неоцененных компонентных продуктов».

«AOC_NCP.2.2E Оценщик должен произвести оценку и подтвердить, что продукты удовлетворяют требуемым пакетам доверия в эксплуатационной среде автоматизированной системы.»

Класс AOT: тестирование автоматизированной системы

Назначение класса AOT состоит в проверке того, что компоненты автоматизированной системы после установки, интеграции и конфигурирования в соответствии с архитектурным и конфигурационным свидетельствами, удовлетворяют функциональным требованиям безопасности, специфицированным в СЗБ, и позволяют эффективно проводить в жизнь концепцию безопасного функционирования АС.

Архитектурная, интеграционная и проектная документация АС помогает планировать и осуществлять тестирование. Чтобы достичь целей тестирования, необходимо убедиться, что системная функциональность безопасности сконфигурирована в соответствии со спецификациями, протестирована на предмет соответствия архитектурным и проектным свидетельствам путем выборочного выполнения тестов разработчика/интегратора, и провести независимое тестирование подмножества СФБ.

Класс AOT включает пять семейств.

Семейство AOT_FUN (функциональное тестирование автоматизированной системы), являющееся аналогом семейства ATE_FUN из стандарта ISO/IEC 15408-3, ориентировано на разработчика, который должен продемонстрировать, что все функции безопасности исполняются в соответствии со спецификациями. Требуется, чтобы разработчик выполнил тестирование и предоставил тестовую документацию.

Функциональное тестирование, выполняемое разработчиком и/или интегратором, устанавливает, что СФБ демонстрирует свойства, необходимые для удовлетворения функциональных требований ПЗ/ЗБ.

Приведем формулировку одного из элементов, конкретизирующих единственный компонент семейства — AOT_FUN.1 «функциональное тестирование».

«AOT_FUN.1.3D Разработчик/интегратор должен представить анализ уровня детализации тестирования интегрированных регуляторов безопасности.»

Семейство AOT_COV (покрытие тестами автоматизированной системы) аналогично семейству ATE_COV из стандарта ISO/IEC 15408-3. Оно состоит из двух иерархически связанных компонентов — AOT_COV.1 «свидетельство покрытия» и AOT_COV.2 «строгий анализ покрытия».

Компонент AOT_COV.1 включает в себя аналоги элементов, конкретизирующих два компонента семейства ATE_COV — ATE_COV.1 и ATE_COV.2. Пример:

«AOT_COV.1.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием СФБ в функциональной спецификации и тестами, идентифицированными в тестовой документации.»

Семейство AOT_DPT (глубина тестирования автоматизированной системы) является практически полным аналогом семейства ATE_DPT из стандарта ISO/IEC 15408-3. То же справедливо для пары семейств AOT_IND (независимое тестирование) и ATE_IND.

Семейство AOT_REG (регрессионное тестирование) специфично для предлагаемого проекта технического доклада, но построено по стандартной схеме. Цель регрессионного тестирования — демонстрация выполнения функций безопасности в соответствии со спецификациями после некоторых изменений компонентов, конфигурации и эксплуатационной среды автоматизированной системы.

Приведем формулировку одного из элементов, конкретизирующих единственный компонент семейства.

«AOT_REG.1.3D Разработчик/интегратор должен представить анализ уровня детализации регрессионного тестирования.»

Класс AOV: анализ уязвимостей автоматизированной системы

Цель деятельности по оценке уязвимостей — выявить допускающие использование дефекты и слабости в автоматизированной системе, сконфигурированной и реализованной для намеченной среды. Для достижения этой цели разработчик/интегратор и оценщик выполняют анализ с учетом информации, предоставленной потребителем; кроме того, оценщик осуществляет тестирование.

Естественно, анализ уязвимостей тесно связан с действующими политикой безопасности автоматизированной системы, процедурами, мерами физической безопасности и безопасности персонала, инфраструктурой безопасности, спо-

собными эффективно нейтрализовать любые уязвимости АС. Стойкость функций безопасности автоматизированной системы охватывает аспекты (преимущественно свойственные человеку) регуляторов безопасности, дающие уверенность в том, что АС остается защищенной, а любые нарушения могут быть эффективно нейтрализованы.

Класс AOV включает три семейства.

Семейство AOV_MSU (неправильное применение автоматизированной системы) аналогично семейству AVA_MSU из стандарта ISO/IEC 15408-3, причем связь между ними по сути та же, что и между рассмотренными выше семействами AOT_COV и ATE_COV. Компонент AOV_MSU.1 «экспертиза руководств автоматизированной системы» включает в себя аналоги элементов, конкретизирующих два компонента семейства AVA_MSU – AVA_MSU.1 и AVA_MSU.2. Пример:

«AOV_MSU.1.2D Разработчик должен документировать анализ руководств.»

Семейство AOV_SOF (стойкость функций безопасности действующего СОО) – практически полный аналог семейства AVA_SOF из стандарта ISO/IEC 15408-3. То же справедливо для пары семейств AOV_VLA (анализ уязвимостей) и AVA_VLA.

Класс AOL: поддержка жизненного цикла автоматизированной системы

Назначение класса AOL состоит в оценке адекватности процедур, применяемых на этапах интеграции и эксплуатации автоматизированной системы. Эти процедуры включают меры безопасности, использовавшиеся на всем протяжении разработки (интеграции) АС, модель жизненного цикла, использованную интегратором, а также инструментарий, применявшийся интегратором на всем протяжении жизненного цикла автоматизированной системы.

Единственное семейство данного класса, AOL_DVS (идентификация мер безопасности автоматизированной системы), является близким, хотя и не полным аналогом семейства ALC_DVS из стандарта ISO/IEC 15408-3, и охватывает меры безопасности при разработке АС. Разработчик должен обеспечить конфиденциальность и целостность своих материалов.

В семейство входят два компонента – AOL_DVS.1 «идентификация мер безопасности» и AOL_DVS.2 «верификация мер безопасности». Приведем формулировку одного из элементов, конкретизирующих первый компонент и помеченных в предлагаемом проекте как управляющий.

«AOL_DVS.1.1M Разработчик/интегратор должен представить документацию по безопасности разработки.»

Класс ASI: установка и поставка системной функциональности безопасности

В процессе установки необходимо сформировать и узаконить структуру управления безопасностью, назначение которой – пропаганда и внедрение в организации политики безопасности и осведомленности в вопросах безопасности. Руководители должны явным образом продвигать и поддерживать в организации меры безопасности, активно участвовать в их реализации. К числу действий руководителей принадлежит формулирование целей безопасности, удовлетворяющих производственным требованиям, а сами действия должны быть интегрированы в соответствующие производственные процессы. Другие действия руководителей – формулирование, пересмотр и одобрение политики безопасности, обеспечение ясной, видимой руководящей поддержки, в том числе поддержки политики безопасности путем выработки и реализации программ повышения осведомленности и проведения тренировок персонала. В организации должен быть также назначен ответственный за информационную безопасность.

Кроме того, необходимо подтвердить адекватность процедур, использовавшихся для конфигурирования автоматизированной системы как при установке, так и при обычном запуске.

Класс ASI содержит три семейства.

Семейство ASI_AWA (отработка навыков) требует от руководителей организации проведения тренировок как средства обучения персонала ролям и обязанностям безопасности для ведения производственной деятельности с помощью автоматизированной системы. Семейство состоит из двух компонентов – ASI_AWA.1 «отработка навыков» и ASI_AWA.2 «верификация отработки навыков». Приведем формулировку одного из элементов, конкретизирующих первый компонент.

«C10.2.3.1 Элементы действий руководителей
ASI_AWA.1.1M Руководители должны организовать отработку навыков в рамках формального процесса внедрения, предназначенного для освоения (выбор: всех организационных регуляторов, (назначение: организацион-

ные регуляторы)) и их требований (выбор: до, в течение (назначение: отрезок времени), периодически (назначение: период времени)), предоставления персоналу доступа к активам автоматизированной системы.»

Семейство ASI_CMM (уведомление) требует, чтобы руководители располагали средствами доведения до сведения персонала руководств по автоматизированной системе, определяющих и специфицирующих для соответствующих должностных лиц системную функциональность и политику безопасности, их роли и обязанности.

Структура данного семейства аналогична структуре предыдущего, а компоненты именуются как ASI_CMM.1 «информирование» и ASI_CMM.2 «верификация информирования». Приведем формулировку элемента действий руководителей.

«ASI_CMM.1.1M Руководители должны довести информацию о (выбор: всех СФБ, (назначение: отдельных СФБ) до сведения всех должностных лиц, затрагиваемых организационными регуляторами) до предоставления им доступа к активам автоматизированной системы.»

Семейство ASI_SIC (проверка производственной совместимости) является средством контроля установки и запуска системного объекта оценки. Установка и запуск СОО должны быть реализованы и выполнены корректно и эффективно в соответствии с политикой безопасности автоматизированной системы.

В рамках стандартной структуры семейств данного класса приведем формулировку элемента, помеченного в предлагаемом проекте как элемент действий руководителей.

«ASI_SIC.1.1M Разработчик/интегратор должен документировать процедуры, необходимые для получения уверенности в том, что компоненты и интерфейсы, входящие в состав СОО, особенно относящиеся к унаследованным, могут быть запущены и взаимодействовать безопасным образом.»

Класс ASO: записи в автоматизированной системе

Данный класс требований доверия к безопасности не имеет аналога в стандарте ISO/IEC 15408 3. Он специфичен для автоматизированных систем, подверженных непрерывным изменениям и модификациям. Составными частями процессов изменения и модификации являются запросы на изменения, сервисные пакеты, любые применимые программные коррекции, а также специализированные требования интероперабельности или совместимости, выдвигаемые при добавлении новых или изменении существующих внутренних и внешних интерфейсов.

Класс ASO включает три семейства, которые определяют, как корректно и эффективно управлять системной функциональностью безопасности в процессе эксплуатации системы. Основная цель функционирования системной безопасности — иметь возможность убедиться в том, что автоматизированная система работает безопасным образом, без нарушений политик безопасности АС. Еще одна цель — определить действия, предпринимаемые, если происходят события, связанные с безопасностью. Данный класс дает уверенность в выполнении необходимых действий по обнаружению, записи и реагированию на события, возможно, являющиеся нарушениями политики безопасности автоматизированной системы.

Семейства класса ASO определяют административные средства мониторинга и верификации организационных регуляторов.

Семейство ASO_RCD (записи функционирования организационных регуляторов) отвечает за записи функционирования системной функциональности безопасности. Организационные регуляторы должны быть реализованы и функционировать корректно и эффективно в соответствии с политикой безопасности автоматизированной системы.

Семейство включает два компонента — ASO_RCD.1 «запись функционирования организационных регуляторов» и ASO_RCD.2 «верификация записи функционирования».

Приведем формулировку одного из элементов, конкретизирующих оба компонента семейства.

«ASO_RCD.1.2C Записи должны содержать дату и время, ответственное лицо, целевые организационные регуляторы и результаты операции.»

Семейство ASO_VER (верификация организационных регуляторов) предоставляет средства для верификации организационных регуляторов во время их функционирования. Семейство состоит из двух компонентов — ASO_VER.1 «верификация организационных регуляторов» и ASO_VER.2 «независимая верификация организационных регуляторов». Один из элементов, конкретизирующих оба компонента, формулируется следующим образом.

«ASO_VER.1.1M Руководители должны проверить, что (выбор: все организационные регуляторы или (назначение:

организационные регуляторы)) установлены и функционируют корректно и эффективно.»

Основная цель семейства ASO_MON (мониторинг организационных регуляторов) — дать возможность убедиться в том, что организационные регуляторы работают безопасным образом, без нарушений политик безопасности АС. Кроме того, семейство определяет действия, предпринимаемые при внесении изменений в автоматизированную систему.

Семейство включает два компонента — ASO_MON.1 «мониторинг организационных регуляторов руководителями» и ASO_MON.2 «верификация мониторинга организационных регуляторов». Один из элементов действий руководителей формулируется следующим образом.

«ASO_MON.1.2M Руководители должны отслеживать изменения в предоставлении сервисов, включая сопровождение или улучшение политик безопасности, процедур и регуляторов с учетом критичности затрагиваемых производственных систем и процессов, а также переоценку рисков.»

На этом мы завершаем обзор требований доверия к безопасности для автоматизированных систем, включенных в предлагаемый проект технического доклада.

Системные профили защиты и задания по безопасности

В приложении А предлагаемого проекта технического доклада определяются структура и содержание системных профилей защиты и заданий по безопасности. Фактически эта структура и требования к содержанию были рассмотрены выше, поскольку они отражены в структуре и требованиях классов доверия к безопасности автоматизированных систем ASP и ASS. Кратко отметим основные различия между системными профилями и заданиями из предлагаемого проекта и их аналогами из стандарта ISO/IEC 15408.

Важнейшим структурным отличием является присутствие в системных документах частей, описывающих домены безопасности и требования к ним. Далее, введение в системных документах соответствует совокупности введения и описания объекта оценки в стандартном задании по безопасности, описание задачи безопасности — спецификации среды безопасности ОО.

Из содержательных отличий системных документов главным является ориентация на более крупные и сложнее организованные совокупности компонентов, учет не только ИТ-аспектов как в плане требований, так и в плане применяемых регуляторов, но и учет конкретной эксплуатационной среды с конкретными рисками вместо общих предположений о среде.

Заключение

Как показывает сделанный обзор, предлагаемый проект технического доклада ISO/IEC PDTR 19791 — крупный, богатый новыми идеями документ, развивающий и дополняющий подход, зафиксированный в международном стандарте ISO/IEC 15408, применительно к действующим автоматизированным системам. Тщательное изучение этого документа, внимательное отношение к нему необходимы уже на нынешней, ранней стадии развития проекта 19791.

Анализ проекта технического доклада ISO/IEC PDTR 19791

О концептуальном базисе оценочных стандартов информационной безопасности

Анализируя концептуальный базис оценочных стандартов информационной безопасности, необходимо осветить три основных аспекта:

- для чего производится оценка безопасности;
- что оценивается;
- как оценивается.

Цели оценки безопасности

Оценка безопасности может преследовать две цели: формальную и содержательную. Формальная цель состоит в выполнении законодательных, нормативных и технических требований, предъявляемых к организациям определенной ведомственной принадлежности, выполняющим определенные функции, хранящим, обрабатывающим и передающим данные определенного характера. Кроме того, эти требования предъявляются также и к изделиям информационных технологий (ИТ), используемым в упомянутых организациях для выполнения соответствующих функций.

Как правило, достижение формальной цели требует умеренных материальных и интеллектуальных затрат. Требования безопасности широко известны и длительное время (несколько лет) применяются в неизменном виде. Известно, как эти требования выполнить (в какой архитектуре и из каких продуктов строить информационную систему (ИС)), понятно, по какой методике проводится оценка и как к ней подготовиться. Наконец, результаты оценки действуют долго (несколько лет).

Длительное время концептуальным базисом оценочных стандартов информационной безопасности, используемых в формальных целях, служили положения «Оранжевой книги» [3] и их интерпретация для сетевых конфигураций [4]. В России многие важные, в значительной степени оригинальные положения были сформулированы в руководящих документах Гостехкомиссии России (см., например, [5], [6], [7], [8]).

Таким образом, к достоинствам существовавшей системы оценки и лежащих в ее основе стандартов следует отнести стабильность, обозримость, реализуемость, простоту интерпретации результатов. Главный недостаток — неясность соотношения между (зафиксированной) формальной и (непрерывно меняющейся) реальной безопасностью сложных современных ИС.

Если оставить в стороне формальный аспект, то (добровольную, содержательную) оценку следует рассматривать как элемент формирования и поддержания режима реальной информационной безопасности, точнее, как важную составляющую процесса управления безопасностью. На верхнем уровне этот процесс специфицирован в стандарте BS 7799-2:2002 [9].

Современной базой содержательной (а также, в значительной степени, и формальной) оценки безопасности информационных технологий служит международный стандарт ISO/IEC 15408 ([10], [11], [12]) и ассоциированная с ним методология (ISO/IEC 18045 [13]). Анализ стандарта и методологии проведения оценки можно найти, например, в книге [14]. Здесь мы выделим такие достоинства концептуальных основ стандарта ISO/IEC 15408, как гибкость, учет современного уровня информационных технологий, а также широту спектра, высокий уровень детализации и параметризованность требований безопасности. Стандарт ISO/IEC 15408 можно представлять себе как весьма обширную, тщательно проработанную библиотеку функциональных требований и требований доверия к безопасности.

Перечисленные достоинства стандарта ISO/IEC 15408 на практике оборачиваются серьезными проблемами. Во-первых, проведение оценки для четвертого оценочного уровня доверия (ОУД4) занимает около года, а «несжимаемый минимум» (см. третью часть технического доклада ISO/IEC DTR 15443 [15], [16], [17]) составляет шесть месяцев при стоимости услуг испытательной лаборатории (это только часть расходов) порядка $150 — 200 тыс. У стандарта ISO/IEC 15408 и предлагаемого проекта ISO/IEC PDTR 19791 общий концептуальный базис, поэтому нет оснований полагать, что оценка безопасности автоматизированных си-

стем (АС), выполняемая по критериям ISO/IEC PDTR 19791, окажется менее длительной или дорогостоящей.

Если целью оценки является получение конкурентных преимуществ, например, для нового защитного продукта, то длительность оценки и ее высокая стоимость делают достижение этой цели проблематичным. Кроме того, согласно букве закона, результаты оценки действительны только в момент выдачи заключения.

По взаимному соглашению «срок годности» заключения увеличили до шести месяцев, но все равно это очень мало. На практике автоматизированная система по производственным причинам просто не может оставаться неизменной в течение года, как не остаются неизменными риски и угрозы безопасности. В результате полученная после длительных, дорогостоящих испытаний оценка безопасности АС оказывается не вполне адекватной.

Во-вторых, в заключении по результатам оценки на основе стандарта ISO/IEC 15408 фигурируют не только цели безопасности, но и разного рода ограничения, требования к среде и т.п. Интерпретация результатов оценки может быть довольно сложной, и не всегда можно понять, будет ли соответствовать предполагаемое применение оцененной конфигурации защитного продукта. Из-за этого заключение с результатами оценки превращается скорее в рекламу компании-производителя успешно оцененного продукта; в технические детали и производители, и потенциальные клиенты предпочитают не вдаваться (см., например, [18]).

Если рассматривать оценку как элемент управления информационной безопасностью, то обратная связь не должна слишком запаздывать, иначе она в значительной степени теряет смысл. Стоимость оценки также должна быть приемлемой, иначе этот элемент окажется непригодным для практического управления (равно как и для получения конкурентных преимуществ, даже с учетом тиражности защитного продукта).

В этом плане система сертификации, основанная на семействе спецификаций CMM, оказывается более привлекательной. Согласно приведенным в [17] данным, сертификация одного проекта на одной производственной площадке на соответствие требованиям SSE-CMM (международный стандарт ISO/IEC 21827 [19]) обходится примерно в тысячу человеко-часов или, в денежном выражении, — в $100 тыс. Оценка каждого дополнительного проекта по той же методике обойдется заказчику в $10 тыс., что, несомненно, вполне приемлемо.

Объект оценки

У информационной безопасности три основные составляющие — люди, технологии и процессы, — совокупность которых в общем случае и является (или, по крайней мере, должна являться) объектом оценки. Оцениваются такие качества персонала, как квалификация, осведомленность в вопросах безопасности и лояльность, проверяется зрелость технологий и отсутствие уязвимостей, организация производственных процессов и управление ими.

Несмотря на формальные декларации пригодности международного стандарта ISO/IEC 15408 для оценки любых изделий ИТ (продуктов и систем), можно считать общепризнанным фактом ориентацию данного стандарта на оценку продуктов ИТ. (Это и послужило основанием для учреждения проекта ISO/IEC 19791.) В свою очередь, при оценке продуктов ИТ по стандарту ISO/IEC 15408 основной упор делается на технологии; процессы производства продуктов ИТ оцениваются фрагментарно, в некоторых требованиях доверия к безопасности; характеристики персонала не оцениваются вовсе. Заметим, что в стандарте ISO/IEC 15408 и технологический аспект оценивается не полностью; в работе [20] как существенный недостаток отмечено отсутствие в стандарте ISO/IEC 15408 архитектурных требований.

Ключевым для повышения качества, сокращения сроков и стоимости оценки является вопрос накопления и многократного использования знаний. В этом отношении оценка конечного продукта практически ничего не дает. Гораздо эффективнее оценивать и сертифицировать процессы и решения, начиная с ранних стадий жизненного цикла изделий ИТ. Имеются в виду типовые угрозы и риски, задания по безопасности и профили защиты, архитектурные связки, протоколы взаимодействия и т.д. Безопасная система может быть построена только на основе типовых, апробированных решений; индивидуальные проекты чреваты концептуальными, практически неустранимыми просчетами.

Требования безопасности базового уровня зафиксированы в стандарте [21]. К этой же категории можно отнести рекомендации [22]. В стандарте ISO/IEC 15408 и предлагаемом проекте ISO/IEC PDTR 19791 упоминание о каких-либо базовых уровнях отсутствует. Так, в проекте технического доклада ISO/IEC PDTR 19791 предполагается, что для автоматизированной системы производится анализ рисков, формулируется задача безопасности, а предметом оценки по сути является качество решения этой задачи. К сожалению,

подобное основание для оценки безопасности — слишком зыбко. Возможных угроз и рисков — тысячи, проанализировать их исчерпывающим образом, достоверно оценить вероятность реализации и наносимый ущерб не представляется возможным. Неадекватность описания объекта оценки оказывается неизбежной, что, очевидно, снижает значимость самой оценки.

Развивая положение о накоплении и использовании знаний, задачу безопасности, равно как и ее решения на всех уровнях абстракции, следует формулировать инкрементальным образом : это некая (большая, сложная, но заранее детально исследованная и поддерживаемая в актуальном состоянии) базовая сущность плюс обозримая часть, специфичная для конкретного объекта оценки.

В любом случае, однако, автоматизированная система является более естественным объектом оценки, чем продукт ИТ. Она функционирует в конкретной среде, под воздействием конкретных (хотя и непрерывно множащихся) рисков и угроз, поэтому вместо, как правило, не очень внятных, расплывчатых предположений о среде, характерных для документов на основе стандарта ISO/IEC 15408, в описании АС как объекта оценки присутствует существенно больше конкретики, что делает оценку безопасности более значимой.

При оценке безопасности автоматизированных систем необходимо рассматривать такие этапы жизненного цикла, как эксплуатация и сопровождение, что и сделано в предлагаемом проекте ISO/IEC PDTR 19791. Таким образом, в число оцениваемых сущностей вошли процессы, а сам подход к безопасности, по сравнению со стандартом ISO/IEC 15408 стал более комплексным, охватывающим административный и процедурный уровни, что необходимо и для формирования реальной информационной безопасности, и для ее реальной оценки.

Персонал как таковой, и в частности системные и сетевые администраторы (точнее, характеристики персонала), не являются объектом оценки в рамках проекта ISO/IEC PDTR 19791. (Требуется лишь обучение персонала и доведение до него необходимых сведений в соответствии с должностными обязанностями.) Это — общая беда информационных технологий, когда программистом, администратором или специалистом по безопасности может быть любой человек, независимо от его образования и квалификации. В то же время, квалифицированное администрирование — один из важнейших компонентов информационной безопасности автоматизированных систем, систематическое изложение требований к которому в предлагаемом проекте ISO/IEC PDTR 19791, к сожалению, отсутствует.

Проведение оценки

Вопрос «как оценивать?» не менее важен, чем вопросы «для чего оценивать?» и «что оценивать?». Прежде всего, когда речь идет о доверии к безопасности изделия ИТ, можно оценивать не только само это изделие, но и процессы его производства (проектирования, разработки и реализации) и эксплуатации. Как показывает опыт применения семейства стандартов CMM (и в частности приведенные выше данные о длительности и стоимости проведения оценки), оценивание процессов оказывается более эффективным, если, конечно, зрелость этих процессов достаточно высока для того чтобы обеспечить предсказуемость и повторяемость результатов, то есть состоятельность оценки.

В предлагаемом проекте ISO/IEC PDTR 19791 оценка процессов присутствует, но не автоматизированные системы оцениваются посредством процессов их изготовления, эксплуатации и сопровождения, а скорее процессы, ассоциированные с АС, оцениваются как (статичные) изделия. О какой-либо шкале зрелости процессов и о продвижении по этой шкале, как, например, в стандарте ISO/IEC 21827, речь не идет. На наш взгляд, это является недостатком предлагаемого проекта, поскольку если уровень информационной безопасности не повышать, на практике он будет понижаться.

Оценка процессов проводится своими, в значительной степени нетехническими методами, такими, например, как беседы с соответствующими должностными лицами и специалистами. Формально эти методы фигурируют в предлагаемом проекте (беседы с персоналом указаны в качестве одного из вариантов действий оценщика при проверке некоторых требований доверия к безопасности), но им явно отведена второстепенная роль, а основной упор по-прежнему сделан на оценку конечного продукта. Вообще, требования доверия к безопасности в предлагаемом проекте отличаются от аналогичных требований в стандарте ISO/IEC 15408 существенно меньше, чем функциональные, и меньше, чем необходимо для учета различий автоматизированной системы и продукта ИТ как объектов оценки.

Оценка процессов может стать ключевым элементом еще одного способа уменьшения запаз-

дывания оценки — совмещения во времени этапов разработки, реализации, интеграции автоматизированной системы и ее оценки. Получение предварительной, промежуточной оценки таким способом могло бы явным образом фигурировать в предлагаемом проекте.

В соответствии с предлагаемым проектом ISO/IEC PDTR 19791, при проведении оценки проверяется качество решения задачи безопасности. Если вернуться к положению о накоплении и многократном использовании знаний, к оценке безопасности можно подойти и с других позиций, проверяя, выстроена ли защита в соответствии с современными представлениями о корректных и эффективных решениях. При этом задача безопасности учитывается лишь косвенно, как фактор, влияющий на множество рассматриваемых решений. Именно такой подход представлен в «Оранжевой книге», построенной на основе формальной модели безопасности и возможных методов ее реализации. На наш взгляд, он имеет право на существование и в настоящее время, особенно если стремиться к сокращению длительности и стоимости оценки. В критериях оценки могут фигурировать упоминавшиеся выше стандартные архитектурные связки (служащие, например, для защиты внутренней сети и демилитаризованной зоны от внешних угроз и включающие средства межсетевого экранирования и активного аудита), и это не будет реальным ограничением гибкости, поскольку реализовать данный элемент защиты по-другому на современном уровне не представляется возможным. (Взгляды на архитектуру безопасности, конечно, не остаются неизменными, но меняются они не чаще, чем пересматриваются действующие стандарты.)

Важным достоинством предлагаемого проекта, оказывающим существенное положительное влияние на проведение оценки (как первичной, так и особенно повторной) является возможность структурирования автоматизированной системы на (относительно независимые) домены безопасности, по отношению к которым, вообще говоря, выдвигаются разные функциональные требования и требования доверия. Очевидно, что к оценке демилитаризованной зоны и серверного сегмента внутренней сети нужно подходить поразному; предлагаемый проект явным образом поддерживает это.

Возможность структуризации АС на домены безопасности и подсистемы поддержана требованиями безопасности внешних и внутренних интерфейсов, что также следует отнести к существенным достоинствам предлагаемого проекта, упрощающим оценку автоматизированных систем со сложной внутренней организацией и многофункциональными внешними связями.

Внутренние недостатки предлагаемого проекта технического доклада

В данной работе анализируется вторая редакция предлагаемого проекта технического доклада ISO/IEC PDTR 19791. Нет ничего удивительного в том, что эта редакция оказалась довольно сырой, с многочисленными опечатками и внутренними несоответствиями, поэтому мы в первую очередь попытаемся сосредоточиться на наиболее принципиальных моментах, сводя к минимуму мелочные придирки.

Функциональные требования безопасности, включенные в предлагаемый проект технического доклада, на наш взгляд, весьма удачны, в то время как требования доверия нуждаются в существенной переработке. В представленном виде они слишком мало отличаются от требований аналогичной направленности из стандарта ISO/IEC 15408, недостаточно отражают специфику автоматизированных систем. Например, класс AOL (поддержка жизненного цикла автоматизированной системы) состоит лишь из одного семейства — AOL_DVS (идентификация мер безопасности автоматизированной системы), что, разумеется, не позволяет поддерживать должный уровень доверия к безопасности на этапах эксплуатации и сопровождения.

Класс требований доверия ASO (записи в автоматизированной системе) специфицирует требования к протоколированию и аудиту для системной функциональности безопасности и, как аналог класса FAU (аудит безопасности) из стандарта ISO/IEC 15408, должен быть перенесен в число классов функциональных требований.

По заявлению авторов, в предлагаемом проекте технического доклада представлены методология, процесс и требования оценки безопасности автоматизированных систем. Действительно, в разделах 6 и 9 описан рекомендуемый подход к оценке безопасности АС, в приложениях B и C — требования безопасности. Однако едва ли правильно смешивать в одном документе столь разные аспекты оценки безопасности. Предпочтительнее, следуя примеру стандарта ISO/IEC 15408, вынести методологию в отдельный документ (ISO/IEC 18045). Кроме того, наивно полагать, что

на 20 с небольшим страницах (суммарный объем разделов 6 и 9) можно адекватно представить методологию и процесс оценки такой сложной сущности, как автоматизированная система, включающая не только технические, но и организационные элементы. Вопрос оценки организационных регуляторов безопасности явно нуждается в более детальном рассмотрении, поскольку для них весьма непросто обеспечить такие фундаментальные свойства, как объективность и повторяемость результатов оценки. В частности, целесообразно формализовать и конкретизировать проведение оценки статистическими методами.

В плане общей структуры предлагаемый проект технического доклада кажется поставленным с ног на голову. Разделы, составляющие основной текст, заполнены весьма пространными, но довольно очевидными рассуждениями по поводу отличий автоматизированных систем от продуктов ИТ (среди которых выделены сложная внутренняя структура и конкретная эксплуатационная среда), а также расширений предлагаемого проекта по сравнению со стандартом ISO/IEC 15408 (в первую очередь — более полный охват жизненного цикла и рассмотрение административного и процедурного уровней информационной безопасности). Собственно предлагаемые, новые требования безопасности, составляющие суть проекта 19791, вынесены в приложения (естественно, нормативные, обязательные). На наш взгляд, структура технического доклада должна быть переработана так, чтобы общие рассуждения были вынесены в информационно-справочные приложения (как это сделано, например, в стандартах ISO/IEC 15408 и ISO/IEC 21827), а требования безопасности — включены в основной текст.

Основной текст изобилует повторами, даже в пределах одного раздела. Например, в пунктах 6.1 и 6.6 сходным (но не совпадающим) образом описаны типичные свойства автоматизированной системы. На наш взгляд, подобные повторы следует устранить.

Из многочисленных упущений технического характера упомянем оборванную в середине формулировку элемента FOD_POL.1.2, неправильное указание в начале раздела C.1 количества классов требований доверия к безопасности (в предлагаемом проекте введено десять, а не девять новых классов доверия), опечатки в таблице C.1 (вместо AOC_CPP должно быть AOC_PPC, вместо AOD_SIC — ASI_SIC и т.п.). Вообще, при подготовке приложения C, вероятно, слишком часто использовалась технология «copy & paste» без редактирования скопированных фрагментов. Впрочем, не вызывает сомнений, что отмеченные технические недостатки легко исправить, и это наверняка будет сделано в новой редакции.

Возможные расширения набора требований безопасности

Имеется довольно много формальных и фактических стандартов, относящихся к управлению информационной безопасностью, и в частности к оцениванию безопасности информационных систем и продуктов ИТ. Их обзор, сравнение и анализ возможности совместного использования стали предметом технического доклада ISO/IEC DTR 15443 ([15], [16], [17]). Очевидно, необходимо, чтобы по крайней мере стандарты, разработанные в рамках одного ведомства (например, ISO), были согласованы между собой и допускали совместное применение стандартизованным способом. Важно рассмотреть, какие положения одного из самых популярных стандартов — SSE-CMM (ISO/IEC 21827, [19]) целесообразно учесть при продолжении работы над проектом ISO/IEC PDTR 19791.

В стандарте ISO/IEC 21827 фигурирует одиннадцать групп процессов, относящихся к разработке системных средств безопасности. Мы выделим следующие группы:

- оценка уязвимостей;
- построение доказательств доверия;
- координация безопасности;
- обеспечение необходимых данных о безопасности.

Согласно стандарту ISO/IEC 21827, оценка уязвимостей подразумевает выполнение следующих действий:

- выбор методов, средств и критериев, посредством которых уязвимости в безопасности систем, функционирующих в определенной среде, идентифицируются и характеризуются;
- идентификация уязвимостей;
- сбор данных, относящихся к свойствам идентифицированных уязвимостей;
- оценка уязвимостей системы и совокупной уязвимости, являющейся следствием конкретных уязвимостей и комбинации этих уязвимостей;
- мониторинг непрерывных изменений в наборе системных уязвимостей и в их характеристиках.

Хотелось бы подчеркнуть принципиальные различия в подходе к анализу уязвимостей в стандарте ISO/IEC 15408 (семейство требований доверия AVA_VLA) и проекте ISO/IEC PDTR 19791 (семейство AOV_VLA) с одной стороны, и в стандарте ISO/IEC 21827 — с другой. В первом случае доминирует статический подход, цель которого — доказать отсутствие уязвимостей, допускающих практическое использование. Во втором случае наличие уязвимостей не вызывает сомнений; их нужно непрерывно отслеживать, систематизировать их свойства и выбирать контрмеры в зависимости от этих свойств. Для продуктов ИТ статический подход к оценке уязвимостей можно оправдать и принять; для автоматизированных систем — нет. Для АС предпочтителен динамический подход в духе SSE-CMM.

(Выводы о сравнительных достоинствах и недостатках различных стандартов зачастую основываются на интерпретации этих документов, на субъективной расстановке акцентов. В принципе, в элементе FOD_POL.1.3 при желании можно найти эквивалент перечисленных выше действий по оценке уязвимостей, но, на наш взгляд, проект ISO/IEC PDTR 19791 только выиграет, если важные положения из разряда подразумеваемых или домысливаемых перейдут в разряд явно сформулированных.)

В процессе построения доказательств доверия по стандарту ISO/IEC 21827 фигурируют следующие действия:

- идентификация целей доверия к безопасности;
- определение стратегии получения доверия к безопасности, увязанной с идентифицированными целями;
- идентификация и контроль свидетельств доверия к безопасности;
- анализ свидетельств доверия к безопасности;
- предоставление доказательств доверия к безопасности, демонстрирующих выполнение потребностей заказчика.

Для проекта ISO/IEC PDTR 19791 идентификация целей доверия к безопасности — нетривиальный момент. В стандарте ISO/IEC 15408 фигурируют оценочные уровни доверия. Соответственно, в качестве цели (пусть и формальной) может быть провозглашено достижение определенного оценочного уровня. В предлагаемом проекте ISO/IEC PDTR 19791 оценочные уровни не упоминаются, поэтому не очевидно, какая совокупность требований доверия должна быть выполнена для конкретной автоматизированной системы. Значит, действия по идентификации целей доверия к безопасности следует явным образом специфицировать.

Очень важен и такой момент, как выбор стратегии достижения цели. Наличие стратегического уровня при планировании процессов формирования и поддержания информационной безопасности автоматизированных систем не предусмотрено проектом ISO/IEC PDTR 19791. Лишь в элементе FOD_ORG.1.1 в числе функций комиссии по управлению фигурирует выработка стратегии организации в области информационной безопасности; но необходимы и более частные стратегии, разрабатываемые не только упомянутой комиссией. И разумеется, обязательно должна быть выработана и документирована стратегия развития автоматизированной системы в целом, а не только ее компонентов, реализующих защитную функциональность.

Координация действий в области информационной безопасности важна на всех уровнях — от стратегического планирования до администрирования сервисов безопасности. Необходимо определить цели, взаимосвязи и механизмы для координации, поощрять и облегчать координацию. Требований, включенных в элемент FOM_ORG.1.1, на наш взгляд, недостаточно.

Обеспечение данных о безопасности, необходимых системным архитекторам, проектировщикам, разработчикам, интеграторам, администраторам и пользователям для принятия обоснованных решений, включает такой важнейший элемент, как рассмотрение альтернатив. Документ с анализом и ранжированием альтернативных решений целесообразно включить в число обязательных свидетельств, предоставляемых разработчиком/интегратором и подвергающихся периодической ревизии. Доведение данных до всех заинтересованных лиц — один из важных аспектов координации действий в области информационной безопасности.

На наш взгляд, целесообразно дополнить семейство ASD_SAD (архитектурный проект автоматизированной системы) требованиями выполнения общепризнанных архитектурных принципов, таких как эшелонированность обороны, разнообразие защитных средств, отсутствие одиночных точек отказа. Без архитектурной поддержки доверие к безопасности не может быть обеспечено.

Заключение

Проблема оценки информационной безопасности автоматизированных систем, несомненно, является крайне важной и актуальной. Современный

подход к оценке безопасности информационных технологий зафиксирован в международном стандарте ISO/IEC 15408. В силу перечисленных причин учреждение проекта ISO/IEC PDTR 19791 представляется весьма своевременным, а выбранное в нем стратегическое направление на развитие стандарта ISO/IEC 15408 — вполне оправданным.

Не вызывает сомнений, что работа над проектом предстоит длительная, но уже подготовленный вариант технического доклада находится на довольно высоком уровне. В нем, по сравнению со стандартом ISO/IEC 15408, обеспечен более полный охват мер безопасности и этапов жизненного цикла оцениваемых систем, удачно выбраны и определены основные понятия и функциональные требования безопасности. Меры доверия к безопасности, на наш взгляд, сформулированы менее удачно, но и здесь есть качественное ядро.

Оценка безопасности сложных систем по необходимости сложна, как сложна и проблема сокращения сроков и стоимости оценки. Некоторых результатов можно добиться организационными мерами, приблизив начало оценки к началу разработки/интеграции системы, выбрав для оценки только наиболее критичные подсистемы АС, и т.п. Но принципиальный эффект может дать только накопление и многократное использование знаний, упреждающая оценка и стандартизация решений, фиксируемых на ранних этапах разработки систем, стандартизация процессов разработки/интеграции/эксплуатации, смещение акцентов при проведении оценки с продуктов на процессы.

На наш взгляд, уже сейчас можно планировать проведение научно-исследовательских работ по оценке информационной безопасности автоматизированных систем на основе предлагаемого проекта технического доклада ISO/IEC PDTR 19791. Это может быть, например, параллельная оценка, проводимая одновременно с оценкой по действующим руководящим документам Гостехкомиссии России. Сопоставление двух оценок позволило бы наглядно продемонстрировать сильные и слабые стороны предлагаемого проекта, наметить пути его совершенствования. Еще одно перспективное направление деятельности — проведение оценки силами системного интегратора, совмещение во времени этапов интеграции и оценки, получение не просто действующей, но и уже оцененной автоматизированной системы.

Литература

1. Обзор предлагаемого проекта технического доклада ISO/IEC PDTR 19791 «Оценка безопасности автоматизированных систем»
2. Information technology — Security techniques — Security assessment of operational systems. — ISO/IEC 2nd PDTR 19791, 2004-12-17.
3. Department of Defense Trusted Computer System Evaliation Criteria. — DoD 5200.28-STD, December 26, 1985.
4. National Computer Security Center. Trusted Network Interpretation. — NCSC-TG-005, 1987.
5. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. — Москва, 1992.
6. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — Москва, 1992.
7. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — Москва, 1992.
8. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — Москва, 1997.
9. British Standard. Information security management systems — Specification with guidance for use. — British Standards Institution, BS 7799-2:2002.
10. Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. — ISO/IEC 15408-1:2005.
11. Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements. — ISO/IEC 15408-2:2005.
12. Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements. — ISO/IEC 15408-3:2005.
13. Information technology — Security techniques — Methodology for IT Security Evaluation. — ISO/IEC 18045:2005.

14. Галатенко В.А. Стандарты информационной безопасности. Под ред. академика РАН В.Б. Бетелина. — М.: ИНТУИТ.РУ, 2004, 328 с.
15. Information technology — Security techniques — A Framework for IT Security Assurance. Part 1: Overview and Framework. — ISO/IEC 1st DTR 15443-1, 2003-06-11.
16. Information technology — Security techniques — A Framework for IT Security Assurance. Part 2: Assurance Methods. — ISO/IEC DTR 15443-2, 2004-02-26.
17. Information technology — Security techniques — A Framework for IT Security Assurance. Part 3: Analysis of Assurance Methods. — ISO/IEC 4th WD 15443-3, 2004-04-21.
18. Hearn J. Does the Common Criteria Paradigm Have a Future?. — IEEE Security & Privacy, 2004, January/February, pp. 64-65.
19. Information technology — System Security Engineering — Capability Maturity Model (SSE-CMM). — ISO/IEC 21827:2002.
20. Бетелин В.Б., Галатенко В.А. Информационная (компьютерная) безопасность с точки зрения технологии программирования. — Труды 4-й Ежегодной конференции консорциума ПрМ «Построение стратегического сообщества через образование и науку». — М.: МГУ, 2001, с. 38-44.
21. IT Baseline Protection Manual: New. — Bundesamt fur Sicherheit in der Informationstechnik, Germany, 2004, 2377 pp.
22. Recommended Security Controls for Federal Information Systems. NIST Special Publication SP 800-53, Second Public Draft. — U.S. Department of Commerce, NIST, September, 2004.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**