# ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП И СИСТЕМ УПРАВЛЕНИЯ КРИТИЧЕСКИ ВАЖНЫМИ ОБЪЕКТАМИ

***Артамонов Владимир Афанасьевич***

Традиционно при рассмотрении вопросов безопасности информационных технологий прежде всего, как правило, рассматриваются государственные автоматизированные системы (ГАС), банковские технологии, безопасность корпоративных систем, защита персональных данных и другие традиционные объекты, подлежащие информационной защите. Однако мир меняется, и, соответственно, появляются новые вызовы и угрозы, в частности кибервойны и кибертерроризм. Все чаще объектами таких атак являются объекты жизнеобеспечения – энергетика, транспорт, связь, водоснабжение и канализация, трубопроводные системы, а также различного рода автоматизированные системы управления технологическими процессами (АСУ ТП), то, что относится к так называемой «критически важной инфраструктуре».

Не вдаваясь в историю возникновения кибервойн, отметим лишь тот факт, что человечество начало отсчет нового времени деструктивного информационного воздействия на критически важные объекты (КВО) с 2010 года, после атаки на иранские ядерные центрифуги с помощью вредоносного вируса Stuxnet, причем поражению критически важных объектов подвержены прежде всего системы управления на базе так называемых SCADA-систем.

***SCADA*** *(аббр. от англ. supervisory control and data acquisition – диспетчерское управление и сбор данных) — программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления.*

Значение термина SCADA претерпело изменения вместе с развитием технологий автоматизации и управления технологическими процессами. В 80-е годы под SCADA-системами чаще понимали программно-аппаратные комплексы сбора данных реального времени. С 90-х годов термин SCADA больше используется для обозначения только программной части человеко-машинного интерфейса АСУ ТП.

На информационном ресурсе [1] приведен отчет по безопасности SCADA-систем NSS Labs' Vulnerability Threat Report. По данным отчета, уязвимость таких инфраструктур, как системы энергоснабжения, водоснабжения, телекоммуникации или транспортной инфраструктуры, с 2010 года выросла на 600%. В отчете также говорится о существенном росте уязвимости оборудования и системного обеспечения в промышленности. К тому же исследование показало, что многие SCADA-системы слишком несовременны или устарели вовсе.

Ключевые данные из отчета:

- Количество обнаруженных слабых мест снижалось на протяжении пяти лет, пока не выросло на 12% в 2012 году.
- Более чем 90% выявленных уязвимостей имеют средний либо высокий уровень опасности, соответственно, 9% из них, найденных в 2012 году, – это уязвимости с чрезвычайно высоким уровнем опасности (с показателем CVSS выше 9,9), к тому же не являются сложными для исследования или взлома.
- В среднем 1% производителей несут ответственность за 31% выявленных уязвимостей в год.
- Только один из 10 главных производителей уменьшил количество выявленных уязвимостей в 2012 году по сравнению со средним показателем десяти предыдущих лет.
- Количество найденных уязвимостей в операционных системах от Microsoft и Apple существенно снизилось в 2011, 2012 годах на 56% и 53% соответственно.

***МАИТ*** *– Международное научное общественное объединение «Международная академия информационных технологий». Зарегистрировано в ООН под товарным знаком (брендом) IAIT.*

• Количество найденных уязвимостей в системах промышленного контроля (**ICS/SCADA)** возросло в шесть раз с 2010 по 2012 год.

В отчете показано, что выявленные в 2012 уязвимости повлияли на состав производителей: более чем 2600 продуктов от 1330 разных производителей имеют известные уязвимости. Но интересно, что 73% из них – это производители, от которых не было уведомлений об уязвимостях на протяжении последних нескольких лет. Из исследования видно, что общая картина продолжает меняться, в зоне риска оказываются новые производители, так как все время появляются новые технологии, а с ними и новые опасности. Другое важное обстоятельство вытекает из интересных результатов по измерению уровня сложности произведения успешной атаки на промышленные системы, когда злоумышленник уже получил к ним доступ. Результат показал, что отношение уязвимостей с низким уровнем сложности атаки снизилось с 90% в 2000 году до 48% в 2012 году. Тем временем в этот период количество слабых мест со средним уровнем сложности атаки выросло до 2431, с 5 до 47% в 2012 году. Количество уязвимостей с высоким уровнем сложности атаки в последние десять лет оставалось стабильным, со средним показателем в 4%.

Ну и основное заключение таково, что главной проблемой SCADA-систем является то, что они не были приспособлены для подключения к Интернету. Принципиальные вопросы в системах защиты не были продуманы при их разработке.

Из всего изложенного вытекает главный вывод – ***ключ решения проблем безопасности АСУ ТП критически важных объектов любого государства лежит в достижении им той или иной степени «цифрового суверенитета»***. Для достижения этой цели необходимо решение как минимум триединой задачи: ***разработка законодательной и нормативной базы, создание методологии проектирования и анализа безопасности АСУ ТП КВО, производство доверенных продуктов и систем информационных технологий, из которых будут создаваться системы управления этими КВО.***

## ПОЛИТИКА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КВО

Проблема безопасности АСУ ТП и КВО не нова в мировой практике: чем более развито государство в экономическом и технологическом отношении, чем более информационные технологии и Интернет проникли в инфраструктуру управления отраслями и страной в целом, тем чувствительней для него деструктивные воздействия на его киберпространство.

Не рассматривая опыт ведущих в экономическом и технологическом отношении стран, заметим, что, в общем- то, вся правовая и нормативная база, регламентирующая данный вид деятельности, зиждется на практическом опыте, так называемой ***best practics***, носит характер прямых рекомендаций и не предполагает какого-либо варьирования в части оптимизации построения структур АСУ ТП КВО, в том числе на базе SCADA-систем. Желающих более подробно исследовать международный опыт в данной сфере отсылаем к всестороннему и детализированному обзору А. Лукацкого [2].

Теперь вернемся к опыту РФ как флагмана построения и эксплуатации подобных систем на постсоветском пространстве. За неполное десятилетие начиная с 2005 года постепенно начали выстраивать нормативно-правовую базу создания систем управления КВО:

- Совет Безопасности РФ. 08.11.2005 «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий»;
- «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);

- «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007);
- Совет Безопасности РФ. 08.08.2013. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации».

Последний документ является обобщающим, разработан в целях реализации ***Стратегии национальной безопасности РФ до 2020 года*** и ставит своей целью снижение до минимально возможного уровня рисков от несанкционированного вмешательства в функционирование АСУ ТП. Риск ориентированный подход определяет политику государства, что должно быть сделано на национальном уровне в целях снижения рисков от несанкционированного вмешательства в функционирование АСУ ТП КВО РФ.

Для более целенаправленного понимания дальнейшего изложения материала приведем основные определения данного документа.

Основные понятия, используемые в ***Основных направлениях***:

*а) критически важный объект инфраструктуры Российской Федерации (далее – критически важный объект)* – объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно – территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок;

*б) автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации (далее – автоматизированная система управления КВО)* – комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам Российской Федерации, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий (далее – тяжкие последствия);

*в) критическая информационная инфраструктура Российской Федерации (далее – критическая информационная инфраструктура)* – совокупность автоматизированных систем управления КВО и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий;

*г) компьютерная атака* – целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях;

*д) безопасность автоматизированной системы управления КВО* – состояние автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (далее – штатный режим функционирования) при проведении в отношении ее компьютерных атак;

*е) безопасность критической информационной инфраструктуры* – состояние элементов критической информационной инфраструктуры и критической информационной инфраструктуры в целом, при котором проведение в отношении ее компьютерных атак не влечет за собой тяжких последствий.

Кроме того, документ предусматривает:

- Создание единой государственной системы обнаружения и предупреждения компьютерных атак (централизованная, иерархическая, территориально распределенная структура).
- Формирование «сил обнаружения и предупреждения компьютерных атак».
- Обеспечение разрешительного характера деятельности (лицензирование и сертификация), при этом в задачах по развитию указывается на оптимизацию законодательства в части лицензирования.

**КЛЮЧ РЕШЕНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ АСУ ТП КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ЛЮБОГО ГОСУДАРСТВА ЛЕЖИТ В ДОСТИЖЕНИИ ИМ ТОЙ ИЛИ ИНОЙ СТЕПЕНИ «ЦИФРОВОГО СУВЕРЕНИТЕТА».**

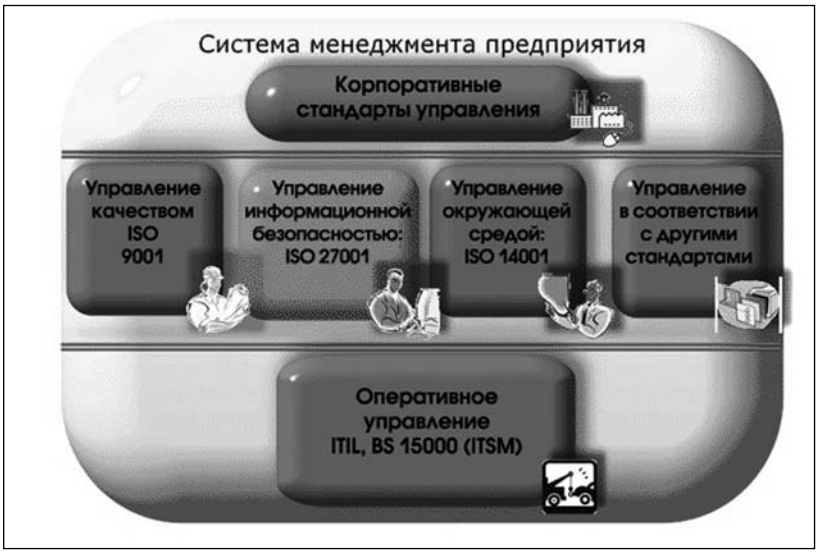


Рис.1. Место СУИБ критичной инфраструктуры в общей системе менеджмента предприятием

- Исключение/ограничение прохождения информационного обмена АСУ КВО по территории иностранных государств.
- Множество задач на разработку систем управления информационной безопасности (СУИБ), оценку защищенности и внедрение специализированных информационных систем, а также импортозамещение (использование доверенных продуктов и систем ИТ).

## МЕСТО СУИБ В ОБЩЕЙ СИСТЕМЕ МЕНЕДЖМЕНТА КРИТИЧЕСКИ ВАЖНЫМ ОБЪЕКТОМ

Основным движущим механизмом СУИБ является периодический анализ рисков информационной безопасности. Высшее руководство организации (КВО) также вовлекается в процесс управления СУИБ посредством принятия решений на основе результатов анализа рисков, результатов внутренних аудитов и других механизмов СУИБ. С точки зрения процессов управления СУИБ входит в общую систему менеджмента организации и предоставляет дополнительные механизмы управления в части обеспечения защиты критичной инфраструктуры (рис. 1).

Одной из наиболее ответственных и сложных задач, решаемых в процессе создания СУИБ, следует назвать проведение анализа рисков информационной безопасности в отношении активов организации в выбранной области деятельности КВО и принятие высшим руководством решения о выборе мер противодействия выявленным рискам.

В процессе анализа рисков проводятся:

- идентификация всех активов в рамках выбранной области деятельности;
- определение ценности идентифицированных активов;
- идентификация угроз и уязвимостей для идентифицированных активов;
- оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;
- выбор критериев принятия рисков;
- подготовка плана обработки рисков.

Выполнение всех указанных задач обычно осуществляется в соответствии с разрабатываемой процедурой анализа рисков, в которой определена методология и отражены организационные аспекты каждой из задач.

## ОЦЕНКА БЕЗОПАСНОСТИ АСУ ТП КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

При рассмотрении нормотворческой деятельности уполномоченных органов (регуляторов) РФ в сфере ИБ АСУ ТП КВО подспудно возникал вопрос оценки безопасности. Чем руководствоваться разработчику, заказчику или аудитору таких сложных инфраструктур, как КВО, при оценке безопасности автоматизированных систем на всех этапах жизненного цикла. Существует два подхода к проблеме оценки ИБ – это использование собственных национальных нормативных правовых методик и рекомендаций и учет мирового опыта на основе международных стандартов.

В феврале 2014 года стал доступен общественности проект долгожданного нормативного документа ФСТЭК, подводящего итог нормотворческой деятельности «регуляторов» РФ: «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Несмотря на столь длинное название, документ лаконичен, как боевой приказ, всеобъемлющ, как армейский устав, прост и безотказен в работе, как автомат Калашникова, и после утверждения сыграет важную роль в ранжировании и сертификации российских АСУ ТП по уровням защищенности и аттестации КВО по соответствующим показателям. Но что делать с КВО, сфера деятельности которых носит

трансграничный характер, а соответствующие субъекты производственных отношений являются транснациональными корпорациями или находятся в юрисдикции субъектов международного права? Это трубопроводные системы всех уровней, линии ЛЭП, коммуникации, транспортные системы и т. п. На этот случай существуют международные стандарты по оценке безопасности, сертификации и аттестации подобных объектов и не только их. Не будем утомлять читателя опытом сертификации и аттестации продуктов и систем ИТ в развитых странах на предмет информационной безопасности в технологической сфере, скажем лишь, что в США существует как минимум четыре таких системы, из них две базируются на международных стандартах.

Давайте с этих позиций перейдем к анализу оценки защищенности на основании международных стандартов. Главными нормативными документами для анализа защищенности продуктов и систем ИТ являются стандарты ISO/IEC 15408 [3,4,5], более известные как «Общие критерии». К этой серии тесно примыкает стандарт ISO/IEC 18045 [6], более известный как «Методология оценки». Первая редакция этих стандартов датирована 1999 годом, и по мере того как нарабатывалась практика применения этого «метастандарта», выпускались более поздние версии, последняя датирована 2008 годом. Вместе с тем в РФ прямым введением выпущена серия стандартов аналогичного содержания под общим титулом «ГОСТ Р ИСО/МЭК 15408».

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 оценки безопасности.

Международный стандарт ISO/IEC 15408 ограничен рамками программно-технического уровня информационной безопасности. Для оценки продуктов информационных технологий этого, в принципе, достаточно; для систем АСУ ТП, проектируемых и находящихся в производственной эксплуатации, – нет. Международной организации по стандартизации (ISO) Российской Федерацией было предложено разработать новый стандарт для оценки безопасности автоматизированных систем. Данная инициатива получила поддержку членов подкомитета 27 «Методы и средства обеспечения безопасности» (SC27), совместного Технического комитета 1 «Информационная технология» (JTC1), в результате появился технический доклад (технический проект) Security assessment of operational systems[7]. С учетом сложившейся в руководящих документах ФСТЭК России терминологии рекомендуется переводить название этого проекта на русский язык как «Оценка безопасности автоматизированных систем».

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 автоматизированных систем, находящихся в производственной эксплуатации, или вновь проектируемых (модернизируемых) систем. 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, но не охватывает ряд критически важных аспектов действующих, эксплуатируемых автоматизированных систем (АС), точные спецификации которых необходимы для проведения эффективной оценки.

Проект содержит расширенные критерии оценки и рекомендации по оцениванию как программно-технических, так и административных и процедурных аспектов автоматизированных систем, в том числе SCADA-систем и АСУ ТП КВО. Применение комплексного подхода, охват всех мер , 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 лиц, занимающихся эксплуатацией АС, поскольку эти специалисты должны понимать, что требуется для получения положительной оценки безопасности АС.

Автоматизированные системы имеют сложную природу, состоят из нескольких подсистем, часть из которых уникальны и являются результатом собственных разработок, другие же образованы типовыми продуктами общего назначения от различных производителей. Система в целом может быть построена (создана, состоять) 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;
- создаются 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 количества компонентов;
- содержат покупные компоненты, в том числе продукты и системы

ИТ с множеством 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.

У автоматизированной системы есть множество 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 проекте принят трехзвенный подход к формированию режима безопасности автоматизированных 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,

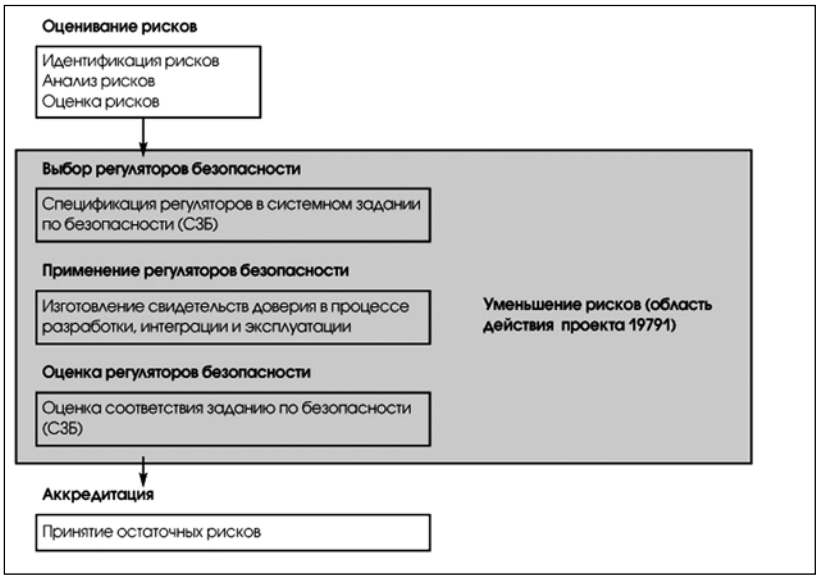


Рис. 2. Формирование режима безопасности АС

подтверждающая, что остаточные риски допустимы для системы, эксплуатируемой в конкретной реальной среде.

Процесс формирования режима безопасности АС представлен на рисунке 2. В качестве средства достижения цели используется оценка безопасности, основанная на модели оценивания технических регуляторов, принятой в стандарте ISO/IEC 15408, но ее действие распространяется 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.

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 указана идентификация рисков для автоматизированной системы. После того как выявлены недопустимо высокие риски, подлежащие

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.

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– разработка или закупка базового и прикладного программного обеспечения, в том числе 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.

Четвертый 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 идет подготовка к ее использованию.

На этапе производственной эксплуатации выполняются 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 предполагаемые или внесенные изменения АС, в том числе 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 документально подтвердить успешное завершение работы автоматизированной системы.

В проекте содержится описание семи новых, которых нет в стандарте ISO/IEC 15408-2 *классов функциональных требований*, включающих двадцать девять семейств:

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

В проекте технического доклада определены также десять новых, не поименованных в в стандарте ISO/IEC 15408-3 *классов требований доверия*, содержащих пятьдесят одно семейство:

- ***Класс ASP*** (оценка системного профиля защиты):
  1. *ASP_INT* (введение СПЗ);
  2. *ASP_CCL* (утверждения о соответствии);
  3. *ASP_ECD* (определение дополнительных требований безопасности);
  4. *ASP_SPD* (определение задачи безопасности);
  5. *ASP_OBJ* (цели безопасности);
  6. *ASP_REQ* (требования безопасности);
  7. *ASP_DMI* (введение для домена безопасности);
  8. *ASP_DMC* (утверждения о соответствии для домена безопасности);
  9. *ASP_DMP* (определение задачи безопасности для домена безопасности);
  10. *ASP_DMO* (цели безопасности для домена безопасности);
  11. *ASP_DMR* (требования для домена безопасности).
- ***Класс ASS*** (оценка системного задания по безопасности):
  1. *ASS_INT* (введение СЗБ);
  2. *ASS_CCL* (утверждения о соответствии);
  3. *ASS_ECD* (определение дополнительных требований безопасности);
  4. *ASS_SPD* (определение задачи безопасности);
  5. *ASS_OBJ* (цели безопасности);
  6. *ASS_REQ* (требования безопасности);
  7. *ASS_TSS* (краткая спецификация СОО);
  8. *ASS_DMI* (введение для домена безопасности);
  9. *ASS_DMC* (утверждения о соответствии для домена безопасности);
  10. *ASS_DMP* (определение задачи безопасности для домена безопасности);
  11. *ASS_DMO* (цели безопасности для домена безопасности);
  12. *ASS_DMR* (требования для домена безопасности).
- ***Класс AOD*** (руководства автоматизированной системы):
  1. *AOD_OCD* (определение конфигурации автоматизированной системы);
  2. *AOD_ADM* (руководство администратора автоматизированной системы);

**НА ЭТАПЕ СОПРОВОЖДЕНИЯ РАССМАТРИВАЮТСЯ И АНАЛИЗИРУЮТСЯ ВСЕ ПРЕДПОЛАГАЕМЫЕ ИЛИ ВНЕСЕННЫЕ ИЗМЕНЕНИЯ АС, В ТОМ ЧИСЛЕ ПОЛИТИК, ПРАВИЛ И ПРОЦЕДУР. ПРИ НЕОБХОДИМОСТИ ВЫПОЛНЯЕТСЯ РЕГРЕССИОННОЕ ТЕСТИРОВАНИЕ.**

ДЛИТЕЛЬНОЕ ВРЕМЯ КОНЦЕПТУАЛЬНЫМ БАЗИСОМ ОЦЕНОЧНЫХ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИСПОЛЬЗУЕМЫХ В ФОРМАЛЬНЫХ ЦЕЛЯХ, СЛУЖИЛИ ПОЛОЖЕНИЯ «ОРАНЖЕВОЙ КНИГИ».

3. *AOD_USR* (руководство пользователя автоматизированной системы).

- ***Класс ASD*** (архитектурная, проектная и конфигурационная документация автоматизированной системы):
  1. *ASD_SAD* (архитектурный проект автоматизированной системы);
  2. *ASD_IFS* (функциональная спецификация интерфейсов автоматизированной системы);
  3. *ASD_SSD* (проект подсистем автоматизированной системы);
  4. *ASD_CMP* (проект неделимых компонентов автоматизированной системы);
  5. *ASD_IMP* (представление реализации);
  6. *ASD_COM* (концепция безопасности автоматизированной системы).
- Класс AOC (управление конфигурацией автоматизированной системы):
  1. *AOC_OBM* (базовая конфигурация автоматизированной системы);
  2. *AOC_ECP* (оцененные компонентные продукты);
  3. *AOC_PPC* (соответствие профилям защиты);
  4. *AOC_NCP* (неоцененные компонентные продукты).
- ***Класс AOT*** (тестирование автоматизированной системы):
  1. *AOT_FUN* (функциональное тестирование автоматизированной системы);
  2. *AOT_COV* (покрытие тестами автоматизированной системы);
  3. *AOT_DPT* (глубина тестирования автоматизированной системы);
  4. *AOT_IND* (независимое тестирование);
  5. *AOT_REG* (регрессионное тестирование).
- ***Класс AOV*** (анализ уязвимостей автоматизированной системы):
  1. *AOV_MSU* (неправильное применение автоматизированной системы);
  2. *AOV_SOF* (стойкость функций безопасности действующего СОО);
  3. *AOV_VLA* (анализ уязвимостей).
- ***Класс AOL*** (поддержка жизненного цикла автоматизированной системы):
  1. *AOL_DVS* (идентификация мер безопасности автоматизированной системы).
- ***Класс ASI*** (установка и поставка системной функциональности безопасности):
  1. *ASI_AWA* (отработка навыков);
  2. *ASI_CMM* (уведомление);
  3. *ASI_SIC* (проверка производственной совместимости).
- ***Класс ASO*** (записи в автоматизированной системе):
  1. *ASO_RCD* (записи функционирования организационных регуляторов);
  2. *ASO_VER* (верификация организационных регуляторов);
  3. *ASO_MON* (мониторинг организационных регуляторов).

Между девятью новыми классами требований доверия к безопасности, определенными в 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 проектом 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, начатой стандартом ISO/IEC 15408-3, классы ASP и ASS стоят особняком, хотя требования класса ASS можно отнести к этапу разработки/интеграции. В 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 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, 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.

Длительное время концептуальным базисом оценочных стандартов информационной безопасности, используемых в формальных целях, служили положения «Оранжевой книги» [8] и их интерпретация для сетевых конфигураций [9]. В РФ многие важные, в значительной степени оригинальные положения, взятые из «Оранжевой книги», были сформулированы в руководящих документах Гостехкомиссии России и ФСТЭК.

Таким образом, к достоинствам действовавшей системы оценки и составлявших ее основу нормативных документов следует отнести стабильность, обозримость, реализуемость, простоту интерпретации результатов. Недостаток - неясность соотношения между формальной (зафиксированной) и реальной (непрерывно меняющейся) безопасностью сложных современных ИС. При этом необходимо иметь в виду главный постулат ИБ: безопасность – это не продукт, а процесс.

Если оставить в стороне формальный аспект, то оценку (добровольную, содержательную)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 ISO/IEC 27001.

Современной базой содержательной (а также в значительной степени формальной) оценки безопасности информационных технологий служат международный стандарт ISO/IEC 15408 и ассоциированная с ним методология (ISO/IEC 18045). Здесь мы выделим такие достоинства концептуальных основ стандарта ISO/IEC 15408, как гибкость и масштабируемость, учет современного уровня информационных технологий, широкий спектр и высокий уровень детализации, параметричность требований безопасности. Стандарт ISO/IEC 15408 с расширением ISO/IEC PDTR 19791 можно представить как весьма обширную, тщательно проработанную библиотеку функциональных требований и требований доверия к безопасности, что по аналогии со структурным программированием позволяет анализировать и строить АС с любыми заданными требованиями к ИБ.

**Источники:**


1. NSS Labs' Vulnerability Threat Report. [Информационный ресурс]: http://www.tsarev.biz/informacionnaya-bezopasnost/nss-labs-vulnerability-threat-report-po-bezopasnosti-scada/.
2. А. Лукацкий. Безопасность критических инфраструктур: международный опыт. [Информационный ресурс]: http://www.slideshare.net/lukatsky/ss-26553193.
3. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model - ISO/IEC 15408-1:2008.
4. Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements - ISO/IEC 15408-2:2008.
5. Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements - ISO/IEC 15408-3:2008.
6. Information technology - Security techniques - Methodology for IT Security Evaluation - ISO/IEC 18045:2008.
7. Information technology - Security techniques - Security assessment of operational systems - ISO/IEC PDTR 19791: 2004.
8. Department of Defense Trusted Computer System Evaliation Criteria - DoD 5200.28-STD, December 26, 1985.
9. National Computer Security Center. Trusted Network Interpretation - NCSC-TG-005, 1987.


НЕОБХОДИМО ИМЕТЬ В ВИДУ ГЛАВНЫЙ ПОСТУЛАТ ИБ: БЕЗОПАСНОСТЬ – ЭТО НЕ ПРОДУКТ, А ПРОЦЕСС.