1 Загальні питання інформаційної безпеки. Правове забезпечення захисту інформації. Міжнародне співробітництво в сфері захисту інформації

УДК 681.3.06: 519.248.681

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 15408 В УКРАИНЕ

Михаил Бондаренко, Леонид Скрыпник*, Иван Горбенко, Александр Потий
*Харьковский Национальный Университет Радиоэлектроники, *ДСТСЗИ СБ Украины*

Анотація: **Аналізується сучасний стан забезпечення безпеки інформаційних технологій (ІТ-безпеки) з точки зору прийняття низки міжнародних та національних стандартів зарубіжних країн. Розглядається базова технічна модель ІТ-безпеки, робляться та обгрунтовуються висновки щодо необхідності гармонізації вітчизняних нормативних документів з міжнародним стандартом ISO/IEC 15408.**

Summary: **Modern situation of IT-security support is analyzed from the point of view of adopting international and national standards series of foreign countries. The base technical model IT-security is considered, conclusions about necessity of harmonization national normative documents with international standard ISO/IEC 15408 are developed and substantiated.**

Ключевые слова: **ИТ-безопасность, ISO/IEC 15408, задача защиты, профиль защиты, проект безопасности.**

Введение

Начиная с 1999 года специалисты Харьковского Национального университета радиоэлектроники пытаются обратить внимание профессиональной общественности и государственных органов на новый международный стандарт ISO/IEC 15408 «Единые критерии оценки безопасности информационных технологий» (далее Единые критерии) и группу поддерживающих его нормативных документов [1–6]. Однако до сих пор, по нашему мнению, данным нормативным документам в Украине уделяется недостаточное внимание. Специализированные отечественные журналы, начиная с 1999 года, не содержат каких либо статей с обсуждением этого и других нормативных документов, за исключением работ, опубликованных специалистами Харьковского региона [7–10]. Нами, в меру наших возможностей, осуществляется постоянный мониторинг состояния вопросов стандартизации в области безопасности информационных технологий (ИТ). Активность организаций по стандартизации ведущих государств (государств большой семерки и ЕС), реально произошедшие изменения во взглядах специалистов на проблему информационной безопасности (ИБ) и явились поводом подготовить настоящую статью. Другой причиной подготовки статьи является осознание того, что Украина может упустить реальный шанс вовремя освоить новейшие технологии обеспечения ИБ.

Основная цель настоящей работы – обосновать необходимость принятия международного стандарта ISO/IEC 15408 в качестве Национального стандарта Украины.

В статье излагаются:

– результаты анализа состояния обеспечения безопасности информации на основе международных стандартов и нормативных документов зарубежных государств;

– оценка состояния создания отечественных и использования международных нормативных документов в Украине;

– обоснование необходимости гармонизации отечественной нормативной базы с международной;

– предложения по разрешению сложившихся противоречий.

По нашему мнению актуальность решения задачи гармонизации отечественной нормативной базы с международными стандартами, а также вопросов применения международных стандартов в отечественной практике очень велика. Отрицательное решение данных задач может не только затормозить развитие отечественных систем информационной безопасности, но и отбросить Украину с достигнутых на сегодняшний день позиций в данной области.

I Идеологический (теоретический) аспект. Новый взгляд на место услуг безопасности в обеспечении безопасности информационных технологий

Сегодня можно утверждать, что в мире произошло переосмысление подходов к решению проблемы обеспечения информационной безопасности. С момента принятия международного стандарта ISO/IEC 15408 начался новый этап развития теории и практики обеспечения информационной безопасности.

К настоящему времени идеологически изменился взгляд специалистов на место и роль услуг безопасности в решении задачи обеспечения информационной безопасности. До недавнего времени нормативной основой решения задач защиты информации являлись стандарты ISO 7498-2:1989 «Архитектура безопасности ВОС» [11] и ISO/IEC 10181:1996 «Основные положения безопасности открытых систем» [12]. Именно эти документы определяли взгляды специалистов на теоретические подходы к обеспечению защиты информации. Общую логику построения систем защиты информации на основе этих документов можно представить в следующем виде (рис. 1).

Рисунок 1 – Применяемая логика обеспечения безопасности информации

Международный стандарт ISO 7498-2 посвящен вопросам безопасности компьютерных сетей, построенных на основе модели взаимодействия открытых сетей (ВОС). Он рекомендует реализовать в компьютерных сетях пять базовых услуг безопасности. При этом услуги безопасности представляют собой абстрактные понятия, которые могут быть использованы для характеристики требований безопасности и выбираются для обеспечения защиты от идентифицированной угрозы. В свою очередь услуги безопасности реализуются и применяются путем использования специальных средств – механизмов безопасности.

Сфера действия стандарта ISO 7498-2 ограничивалась компьютерными сетями, построенными на основе семиуровневой модели ВОС. Однако предложенный подход к построению систем защиты информации был обобщен на все открытые системы обработки, передачи и хранения информации (базы данных, телекоммуникационные системы и т. п.) принятием в 1996 году международного стандарта ISO/IEC 10181. Можно говорить, что на данном этапе с практической точки зрения говорили о построении системы **защиты информации**, в то время как вопросы обеспечения **информационной безопасности** носили больше абстрактный характер.

С течением времени в информационном плане перестали делать какие-либо существенные различия между системами обработки, передачи и хранения информации. В связи с сильной интеграцией телекоммуникационных, сетевых и иных технологий, превалированием в проектировании телекоммуникационных и информационных систем идеологии единой информационной магистрали все большее практическое распространение получает термин информационная технология (ИТ) и его производные: системы информационных технологий (ИТ-системы), продукты информационных технологий (ИТ-продукты), и, наконец, безопасность информационных технологий (ИТ-безопасность). Под информационной технологией понимают целенаправленную организованную совокупность

информационных процессов, реализованных с использованием средств вычислительной техники, обеспечивающих высокую скорость обработки данных, быстрый поиск информации, распределение данных, доступ к источникам информации независимо от места их расположения [13, 14].

Одновременно с трансформацией взглядов на процессы обработки информации происходит и изменение взглядов на подходы к обеспечению информационной безопасности. Исключительно широкая сфера применения информационных технологий, беспрецедентное расширение функциональных возможностей ИТ-систем и многие дугие причины привели к тому, что существующая модель обеспечения ИБ «угроза безопасности → услуга безопасности → механизм безопасности» перестала удовлетворять как потребителя ИТ-систем, так и их разработчика.

Во многом именно изменившаяся обстановка вокруг информационных технологий побудила специалистов искать новую модель безопасности информационных технологий. Новый взгляд на эту проблему окончательно был закреплен в стандарте ISO/IEC 15408. Теперь чаще говорят о построении системы обеспечения безопасности информации. Логика построения такой системы представлена на рис. 2. Международный стандарт вводит новые понятия, такие как задача защиты или задача по обеспечению безопасности (security objective), профиль защиты (security profile) и проект безопасности (security target). Документ, по сути, определяет принципиально новую технологию проектирования систем ИТ-безопасности на основе разработки профиля защиты и проекта безопасности и вводит в практику новую модель ИТ-безопасности.

I.1 Главная цель и задачи безопасности ИТ-систем

Главная цель безопасности информационных технологий заключается в обеспечении возможности любой организации решать (выполнять) свои функциональные задачи (бизнес-задачи, задачи управления предприятием, технологическими процессами, подразделениями и т. д.) путем построения ИТ-систем, которые исключают или минимизируют ИТ-риски организации, ее партнеров и потребителей.

Отправной точкой в достижении цели ИТ-безопасности являются **задачи обеспечения безопасности** – целевая постановка на противодействие выявленным угрозам безопасности и удовлетворение требований политики безопасности. Специалисты по типу основных классов угроз выделяют **пять** основных целевых задач (вспомним пять базовых услуг безопасности) [15].

1. *Обеспечение доступности (системы, данных, ресурсов).* Обеспечение доступности предполагает, что обладающий соответствующими правами пользователь (субъект, процесс) может использовать ресурс в соответствии с правилами, установленными политикой безопасности, не ожидая дольше заданного промежутка времени. Таким образом, доступность направлена на поддержание системы в работоспособном состоянии, обеспечивающем своевременное и точное ее функционирование. Ресурсы при этом находятся в виде, необходимом пользователю, в месте, необходимом пользователю, и в то время, когда они ему необходимы. Эта задача направлена на предотвращение преднамеренных или непреднамеренных угроз неавторизованного удаления данных или необоснованного отказа в доступе к услуге, попыток использования системы и данных в неразрешенных целях.

2. *Обеспечение целостности системы и данных.* Целостность рассматривается в двух аспектах. Во-первых, это целостность данных, заключающаяся в том, что данные не могут быть модифицированы неавторизованным пользователем или процессом во время их хранения, передачи и обработки. Во-вторых, это целостность системы, заключающаяся в том, что ни один компонент системы не может быть удален, модифицирован или добавлен в обход или в нарушение политики безопасности.

3. *Обеспечение конфиденциальности данных и системной информации.* Конфиденциальность информации, это свойство информации, состоящее в том, что информация не может быть получена неавторизованным пользователем во время её хранения, обработки и передачи.

4. *Обеспечение наблюдаемости.* Наблюдаемость направлена на обеспечение возможности ИТ-системы фиксировать любую деятельность пользователей и процессов, использование пассивных объектов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и обеспечения ответственности пользователей за выполненные действия. Наблюдаемость поддерживается механизмами причастности, методами принуждения, локализацией неисправностей, обнаружения вторжений, восстановления действий и т. д.

5. *Обеспечение гарантий (гарантированность).* Гарантии – это совокупность требований, составляющих некоторую шкалу оценки, для определения степени уверенности в том, что:

– функциональные требования действительно сформулированы и корректно реализованы;

– принятые меры защиты, как технические, так и организационные, обеспечивают адекватную защиту ИТ-системы, информационных процессов и ресурсов;

Рисунок 2 – Логика построения систем ИБ

– обеспечена достаточная защита от преднамеренных ошибок пользователей или ошибок программного обеспечения;

– обеспечена достаточная стойкость от преднамеренного проникновения и использования обходных путей.

Обеспечение гарантий – общая задача, без решения которой решение остальных четырех не имеет смысла.

Пять основных задач тесно взаимосвязаны и взаимозависимы друг от друга. На рис. 3 проиллюстрирована эта взаимосвязь.

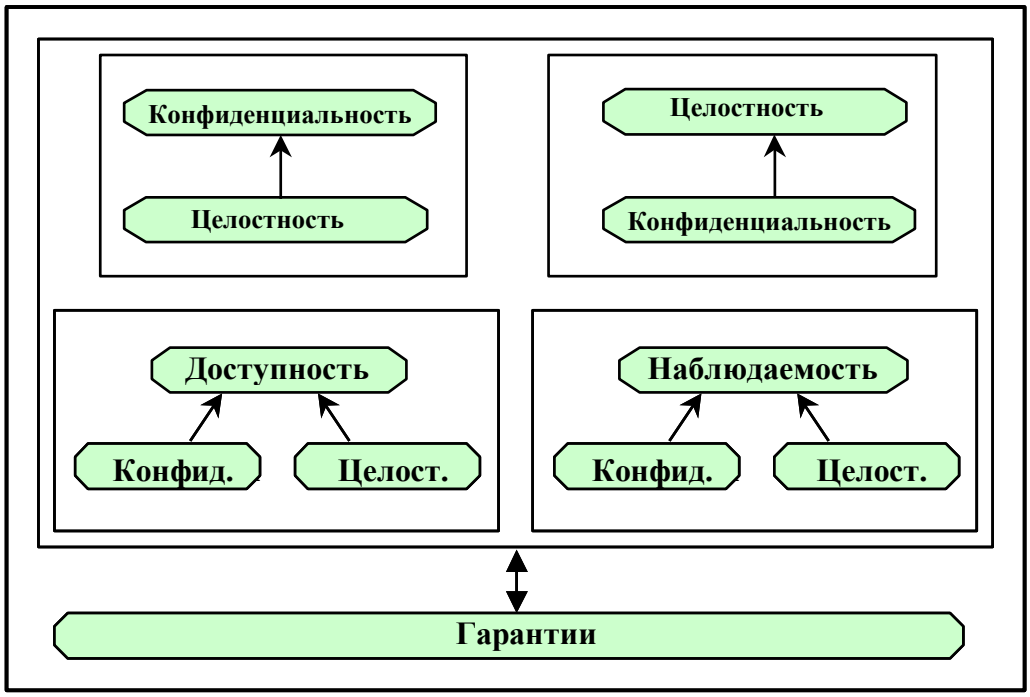

Рисунок 3 – Взаимозависимость задач безопасности

Зависимость конфиденциальности от целостности выражается в том, что если целостность системы будет нарушена, то тогда, скорее всего, и снизится эффективность механизмов конфиденциальности. И наоборот, нарушение конфиденциальности (например, раскрытие пароля администратора) приведет к возможности обхода механизмов целостности.

Суть зависимости доступности и наблюдаемости от конфиденциальности и целостности заключается, например, в том, что:

– если будет нарушена конфиденциальность определенной информации (например, парольной информации), то возникает реальная угроза обхода механизмов доступности и наблюдаемости;

– если будет нарушена целостность системы, то это приведет к компрометации механизмов доступности и наблюдаемости.

И, наконец, все задачи зависят от степени решения задачи обеспечения гарантий. При разработке и создании системы разработчики должны обеспечить определенный уровень гарантированности того, что для выполнения каждой из четырех задач определены функциональные требования, а система разработана и создана с требуемым уровнем качества. Гарантированность подтверждает тот факт, что ИТ-система безопасна и может обеспечить не только выполнение функциональных задач, но и отсутствие незадекларированных возможностей.

В дальнейшем каждая общая задача декомпозируется на составляющие в зависимости от перечня конкретных угроз. Такой подход к построению системы ИБ определяет новые требования и к содержанию основополагающего документа системы обеспечения ИБ – политики безопасности. Так теперь в документе недостаточно определить только классы угроз. Каждая угроза должна быть идентифицирована и конкретизирована, а именно: указывается, кто реализует конкретную угрозу (модель источника (агента) угроз), каким образом данная угроза реализуется (метод нападения (атака) и путь нападения – уязвимость

системы), какой ресурс является объектом ее воздействия и какой ущерб наносится в случае реализации угрозы. Все перечисленное является основой решения задачи оценки рисков.

В итоге формируется детализированный перечень угроз безопасности и соответствующих конкретизированных задач защиты, что на практике отображается в виде матрицы «угроза безопасности – задача защиты».

I.2 Базовая техническая модель ИТ-безопасности

Решение задач защиты возлагается на услуги безопасности. Перечень услуг безопасности [15], по сравнению с ISO 7498-2, значительно расширился. Теперь услуги, в зависимости от того, на решение каких задач они направлены, можно отнести к одному из трех классов (рис. 4):

1. *Опорные услуги безопасности* (4 услуги). К данному классу относятся услуги, которые являются общими и лежат в основе реализации большинства остальных услуг безопасности. Другими словами, они выступают в роли базиса для надстройки, в которую входят услуги двух других классов.

2. *Услуги предотвращения* (6 услуг). Это услуги безопасности, в основном ориентированные на предотвращение различного рода нарушений безопасности.

3. *Услуги обнаружения нарушений и восстановления безопасности* (4 услуги). Эти услуги направлены, прежде всего, на решение задач выявления нарушений безопасности (до или после их осуществления) и восстановления системы в безопасное состояние.

Системное объединение услуг позволило построить базовую техническую модель ИТ-безопасности, которая предложена в рекомендациях NIST [15] (рис. 4). Данная модель иллюстрирует использование основных услуг безопасности при обеспечении ИТ-безопасности и взаимодействие данных услуг.

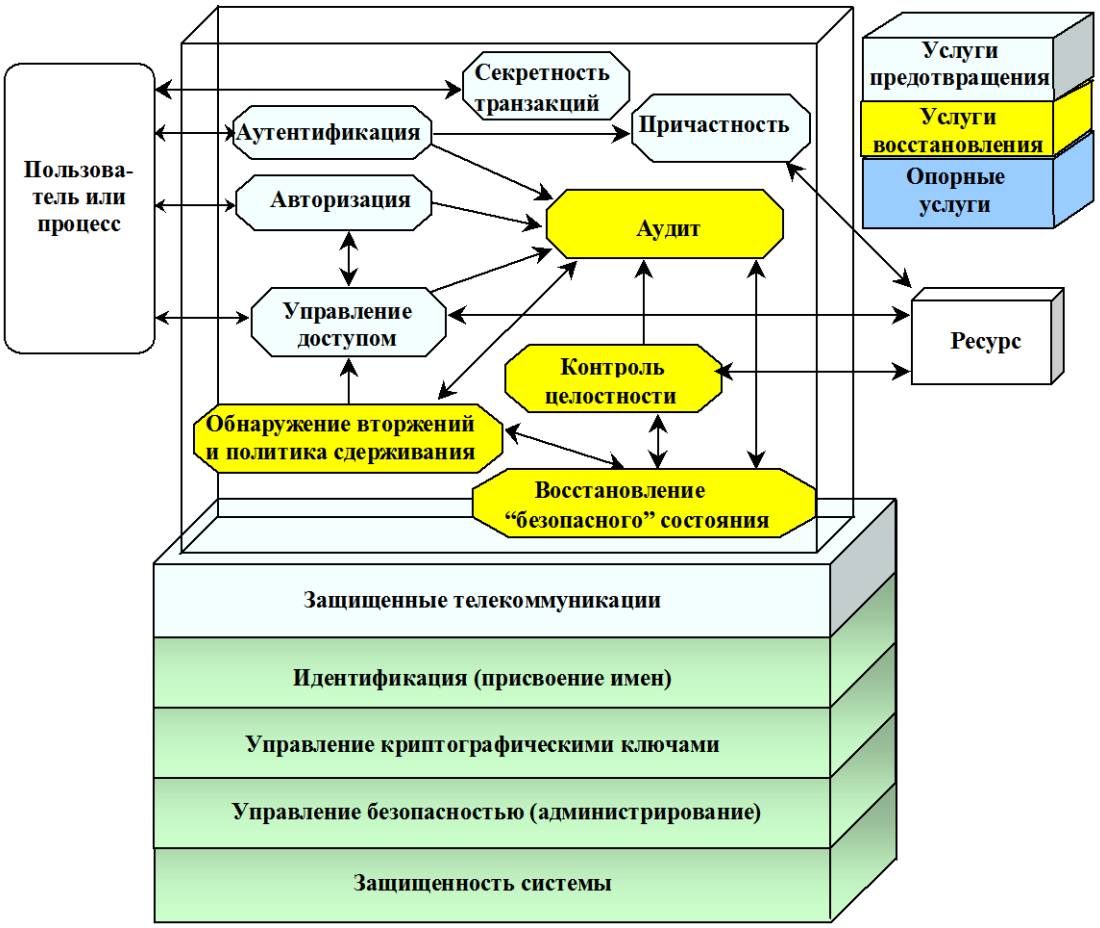

Рисунок 4 – Базовая техническая модель взаимодействия услуг безопасности

Опорные услуги безопасности выступают в роли базиса, по сути, связующей средой для построения всех остальных услуг безопасности. К данному классу относятся следующие услуги безопасности.

Идентификация (присвоение имен). Однозначная идентифицируемость объектов и субъектов информационных взаимоотношений является необходимым условием для реализации большинства услуг безопасности. Идентификация обеспечивает возможность присвоения уникального идентификатора пользователям, процессам, информационным и иным ресурсам.

Управление криптографическими ключами. Данная услуга обязательна в случае применения в услугах безопасности криптографических функций. Под управлением ключами понимают совокупность методов и процедур, осуществляющих безопасное установление и управление ключевыми взаимоотношениями между авторизованными объектами.

Управление безопасностью и администрирование. Под управлением безопасностью понимают распространение информации и управление информацией, необходимой для работы услуг и механизмов безопасности. Под администрированием понимают процессы настройки параметров инсталляции и эксплуатации программного и аппаратного обеспечения услуг безопасности, а также учет вносимых изменений в эксплуатируемое оборудование.

Защищенность системы представляет собой совокупность свойств системы, которые позволяют доверять технической реализации системы. Рассматривается не только качество реализованных средств защиты, но и процедуры их разработки, способы достижения и решения технических задач. Примерами средств защищенности системы являются защита остаточной информации (или защита от повторного использования), минимизация полномочий, разделение процессов, модульность и уровневость разработки, минимизация круга осведомленных лиц и т. д.

Услуги предотвращения нарушений безопасности**.** К данному классу можно отнести следующие услуги.

Защищенные телекоммуникации (*каналы связи*). В распределенных системах обеспечение надежной защиты в большой степени зависит от защищенности каналов связи. Услуга защиты каналов связи обеспечивает целостность, конфиденциальность и доступность информации при её передаче по каналам связи. Различные механизмы безопасности обеспечивают скрытие смыслового содержания передаваемых сообщений, защиту от уничтожения, подстановки, модификации, повторной передачи данных и других видов злоумышленных действий.

Аутентификация является наиболее важной услугой безопасности, особенно в открытых системах. Аутентификация представляет собой услугу проверки подлинности, которая позволяет достоверно убедиться в подлинности субъекта или сообщений.

Авторизация представляет собой услугу, направленную на предоставление (наделение) субъектам определенных полномочий относительно выполнения ими действий в данной ИТ-системе.

Управление доступом. Данная услуга определена как «предотвращение неавторизованного использования ресурсов, включая предотвращение использования ресурсов недопустимым способом» [11]. Услуга применяется к различным типам доступа к ресурсам, например использование коммуникационных ресурсов, чтение, запись или удаление информационных ресурсов, использование ресурсов вычислительных систем по обработке данных и т. д. Политика управления доступом является важнейшей составляющей политики безопасности ИТ-системы.

Причастность (*доказательство принадлежности*). В стандарте ISO 7498-2 причастность определяется как «предотвращение возможности отказа одним из реальных участников коммуникаций от факта его полного или частичного участия в передаче данных». Определены две формы причастности: *причастность к посылке сообщения* (*доказательство источника*) и *подтверждение* (*доказательство*) *получения сообщений.*

Причастность выполняет функции, как предотвращения, так и обнаружения нарушений безопасности. В класс услуг предотвращения она помещена потому, что механизмы причастности предотвращают возможность отказа от выполненных действий.

Приватность (секретность) транзакций. И в государственных, и в частных (корпоративных) ИТ-системах в последнее время усиливаются требования по обеспечению приватности личности, использующей услуги и ресурсы ИТ-системы. Под приватностью (privacy) понимают использование ИТ-системы без угрозы разглашения информации (данных) о личности пользователя. Услуга приватности транзакций обеспечивает защиту от потери приватности путем анализа действия, операций и т. п., выполняемых пользователем в ИТ-системе.

Услуги предупреждения и восстановления безопасности**.** Поскольку не существует достаточного множества предотвращающих мер безопасности, в ИТ-систему встраиваются услуги обнаружения нарушений безопасности, направленные на усиление услуг предотвращения. К данному классу услуг относятся следующие.

Аудит безопасности, направленный на обнаружение событий, оказывающих влияние на безопасность системы и обеспечение реагирования системы на выявленные вторжения, а также на обеспечение формирования необходимых данных для последующего восстановления ИТ-системы в безопасное состояние.

По сути, аудит безопасности выполняет функцию контроля безопасности системы, под которым понимают сбор, накопление информации о событиях, происходящих в информационной системе и анализ записей безопасности с целью проверки эффективности управления системой, обеспечения гарантий соответствия функционирования системы политике безопасности и выработке рекомендаций о необходимых изменениях в управлении, политике и процессах безопасности. Механизмы аудита служат для решения следующих задач:

– обеспечение подотчетности пользователей и администраторов, что является средством сдерживания;

– обеспечение возможности восстановления последовательности событий, что позволяет обнаружить слабости в защите информации, выявить виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе;

– предоставление информации для выявления и анализа проблем через подготовку соответствующих отчетов.

Особенностью аудита является его сильная зависимость от других услуг и механизмов безопасности. Так идентификация и аутентификация служат отправной точкой подотчетности пользователей. Для обеспечения конфиденциальности и целостности регистрационной информации применяют механизмы управления доступом.

Обнаружение происшествий и политика сдерживания. Услуга обнаружения происшествий направлена на обнаружение, как попыток нарушений безопасности, так и на регистрацию легитимной активности пользователей. Обнаружение может быть локальным и/или дистанционным и реализуется через тревожную сигнализацию о происшествиях (event reporting (alarm)), регистрацию событий (event logging) и восстановительные действия (recovery actions). Реализация механизмов обнаружения попыток нарушений безопасности – довольно сложная задача, требующая привлечения методов искусственного интеллекта. Здесь проблема заключается в определении того минимума информации, который бы позволил с заданной вероятностью выявить (или не пропустить) возможные события по вмешательству в работу компьютерной системы.

Контроль целостности программной, аппаратной и информационной частей ИТ-системы и ресурсов направлен на своевременное обнаружение нарушений целостности.

Восстановление безопасности выполняет функцию реакции системы на нарушение безопасности. Услуга реализуется через выполнение таких действий как немедленное разъединение или прекращение работы, отказ субъекту в доступе, временное лишение субъекта прав, занесение субъекта в "черный список" и т. п.

На основе базовой модели можно построить модели обеспечения каждой из выше рассмотренных задач обеспечения безопасности [15]. Для каждой задачи будут важны те или иные услуги безопасности. Ниже, на рис. 5–9 представлены модели решения каждой из основных задач безопасности. Однако следует учитывать, что адекватную защиту ИТ-систем можно обеспечить только путем комплексного решения всех задач.

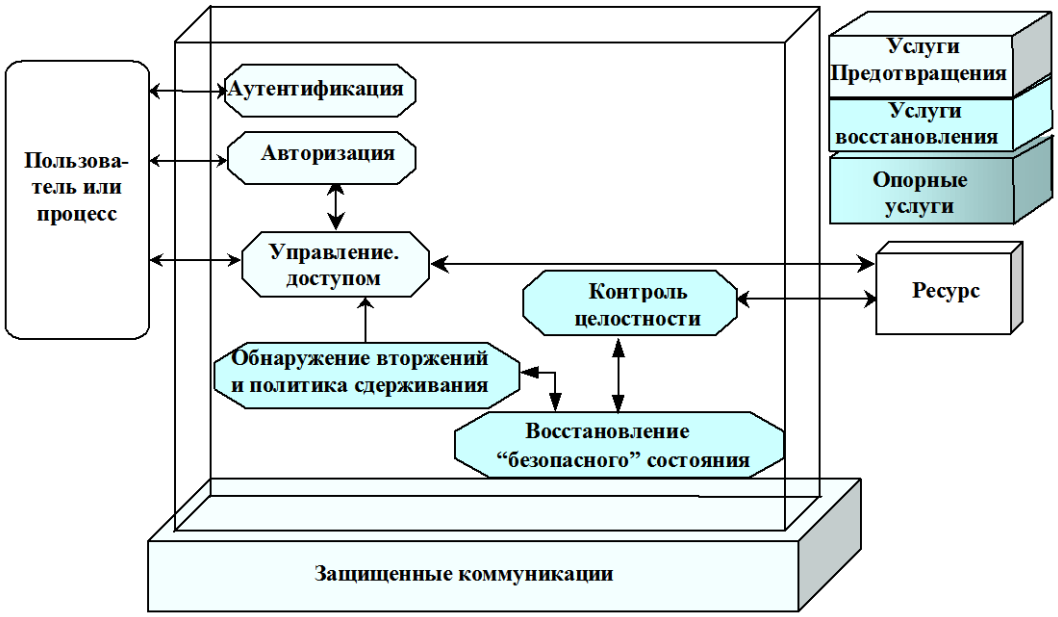

Рисунок 5 – Основные услуги обеспечения доступности

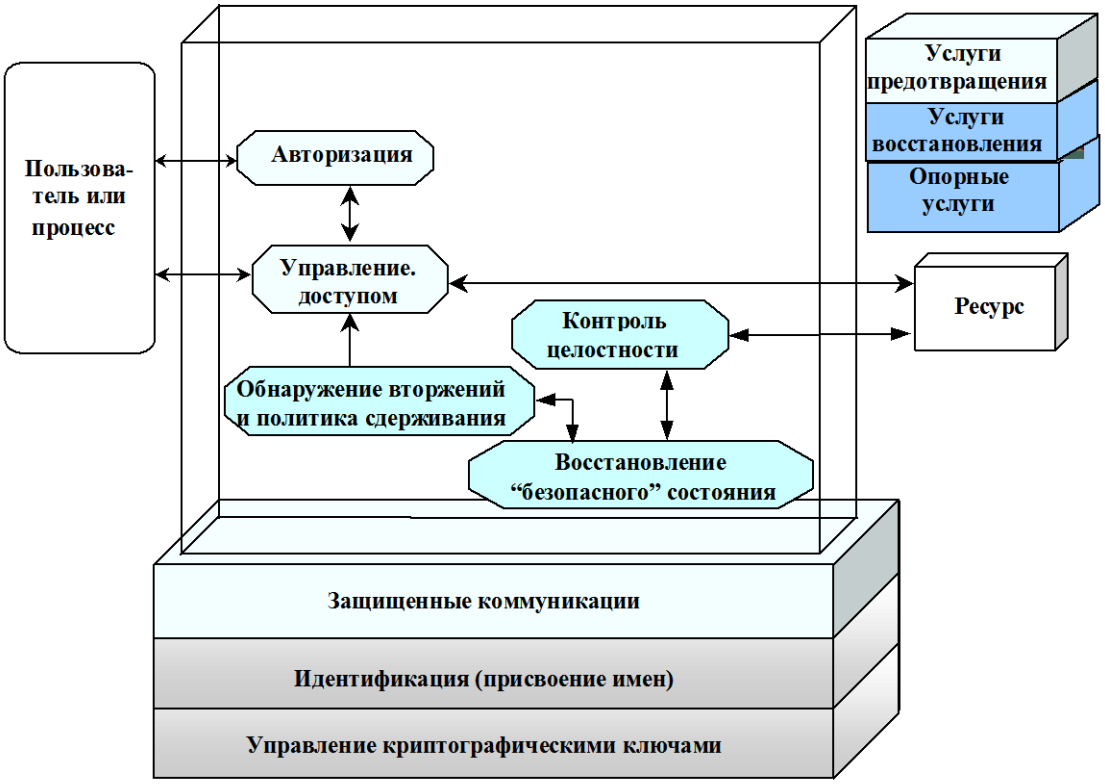

Рисунок 6 – Основные услуги обеспечения целостности

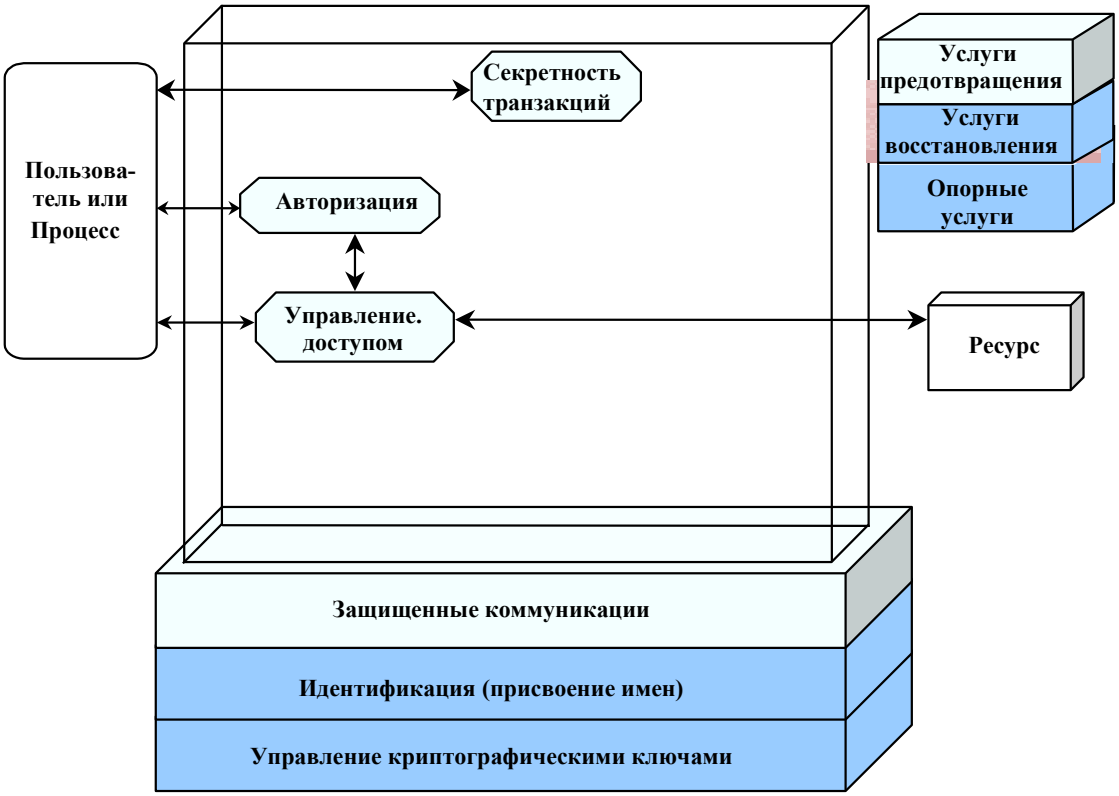

Рисунок 7 – Основные услуги обеспечения конфиденциальности

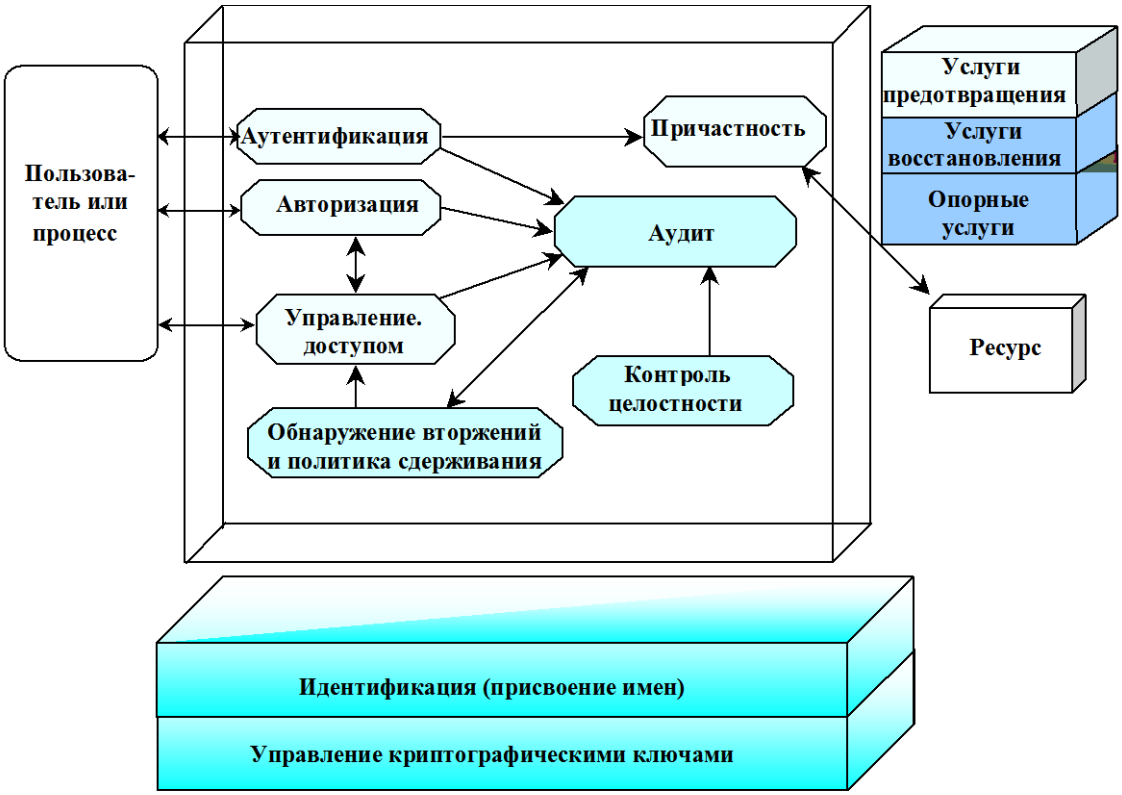

Рисунок 8 – Основные услуги обеспечения наблюдаемости

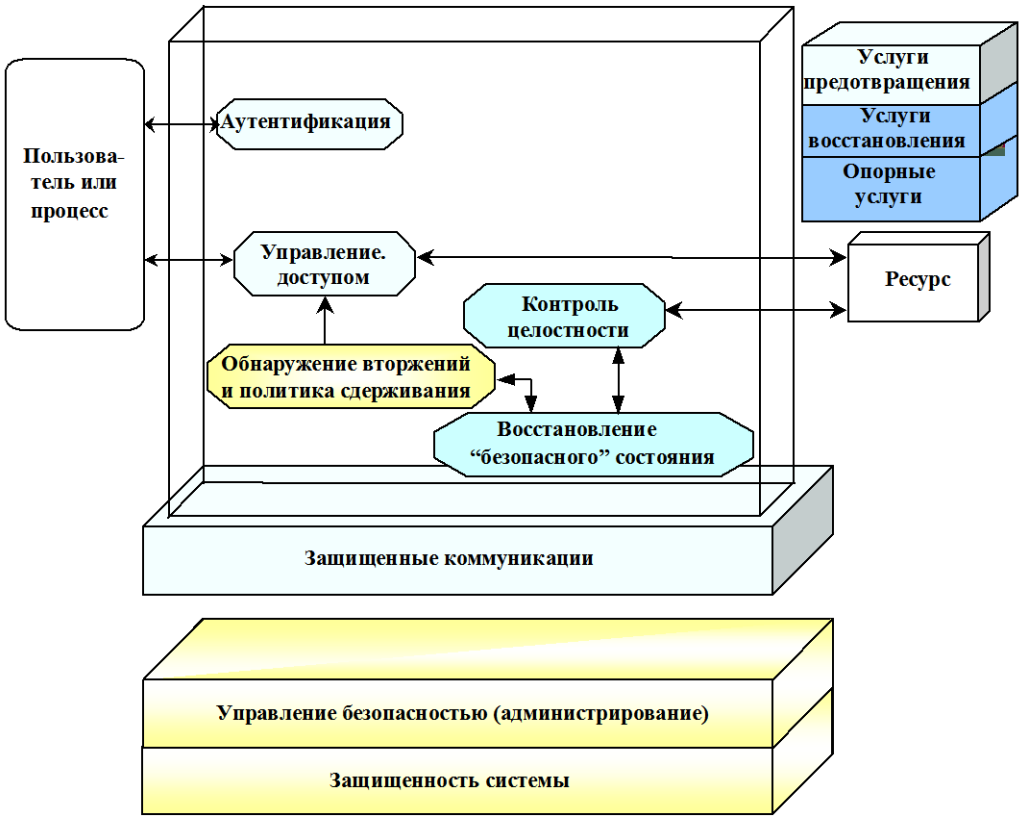

Рисунок 9 – Основные услуги обеспечения гарантированности

Таким образом, существующие услуги безопасности, введенные в стандартах ISO 7498-2 и ISO/IEC10181, были дополнены новыми услугами. Причем некоторые механизмы безопасности трансформировались в услуги (например, аудит), а некоторые услуги трансформировались в задачи защиты (например, конфиденциальность и целостность).

Дальнейшая логика построения системы информационной безопасности обусловлена концепцией и моделью информационной безопасности, введенной в стандарте ISO/IEC 15408. Результаты анализа риска реализации угроз безопасности позволяют сформулировать требования ИТ-безопасности, которые включают функциональные требования безопасности и требования адекватности (гарантии). Функциональные требования безопасности, предъявленные к услугам безопасности, определяют конкретный набор функций безопасности, которые необходимо реализовать для решения каждой из задач по обеспечению безопасности. В свою очередь спецификация функций безопасности представляет собой выбор механизмов безопасности, реализующих функцию. Чтобы механизмы безопасности и средства защиты, реализующие функции безопасности, можно было признать эффективными или адекватными выявленным угрозам, требуется высокая степень уверенности в правильности их выбора и надежности функционирования. Такая уверенность достигается путем предъявления и реализации требований адекватности. Заметим, что стандартизации подлежат только функциональные требования и требования адекватности. В некоторой мере стандартизированы перечни угроз безопасности и соответствующие задачи защиты. Функции и механизмы безопасности на сегодня не стандартизируются, поскольку их реализация в существенной мере зависит от специфики объекта, подлежащего защите, и среды его эксплуатации.

Вывод. На сегодняшний день можно с уверенностью утверждать, что в мире изменилась сама концепция (система взглядов) обеспечения информационной безопасности. Новая концепция учитывает теоретические, технические и социологические изменения, произошедшие в области информационных технологий. Произошел отказ от линейной модели «угроза безопасности → услуга безопасности → механизм безопасности» к расширенной модели: от цели ИТ-безопасности и угроз безопасности к задачам по обеспечению безопасности и услугам безопасности, через формулировку на основе анализа угроз безопасности требований ИТ-безопасности, предъявляемых каждой услугой безопасности к функциям и механизмам безопасности. В практику вводится новая техническая модель безопасности информационных технологий. В целом осуществлен принципиальный переход от ориентации на построение системы защиты информации на объекте к построению системы обеспечения безопасности информации объекта.

II Технологический (практический) аспект. Новая технология проектирования систем обеспечения ИТ-безопасности

Любая теория только тогда становится по настоящему ценной, когда она находит реальное воплощение в практике. Анализ внедрения в практику положений новых международных стандартов и, в частности ISO/IEC 15408, позволяют авторам с уверенностью утверждать, что новая идеология построения систем безопасности информации уже реально воплотилась в новую технологию проектирования систем обеспечения ИТ-безопасности. На рис. 10 представлена схема, которая позволяет нам убедиться в верности высказанного убеждения. Мы выделили три линии или позиции убеждения.

Во-первых. Новая технология проектирования основана на разработке профиля защиты и проекта безопасности, и международный стандарт четко определяет последовательность и содержание каждого этапа проектирования системы ИТ-безопасности.

Во-вторых. Каждый этап уже сейчас имеет нормативную поддержку, в виде принятых или разрабатываемых международных стандартов, а также нормативных документов национальных органов по стандартизации государств, поддерживающих Единые критерии. То есть, сформирована нормативно-правовая база для обеспечения ИБ на законодательном и административном уровнях.

В-третьих. Каждый этап на сегодняшний день имеет достаточно проработанную инструментальную поддержку, что обеспечивает эффективное решение задач ИБ на программно-техническом уровне.

Рассмотрим новую технологию проектирования систем обеспечения ИТ-безопасности со всех трех позиций.

На практике требования ИТ-безопасности конкретизируются в функциях безопасности, а затем реализуются через множество механизмов безопасности в конкретный программно-технический объект. В терминах единых критериев таковым является *объект оценки* (TOE-Target of Evaluation) – ИТ-продукт или ИТ-система, а также связанная с ними эксплуатационная, техническая, пользовательская и иная документация, являющиеся объектом проверки и оценки. Основными документами, характеризующими TOE с точки зрения обеспечения ИТ-безопасности являются профиль защиты и проект безопасности. Разработка

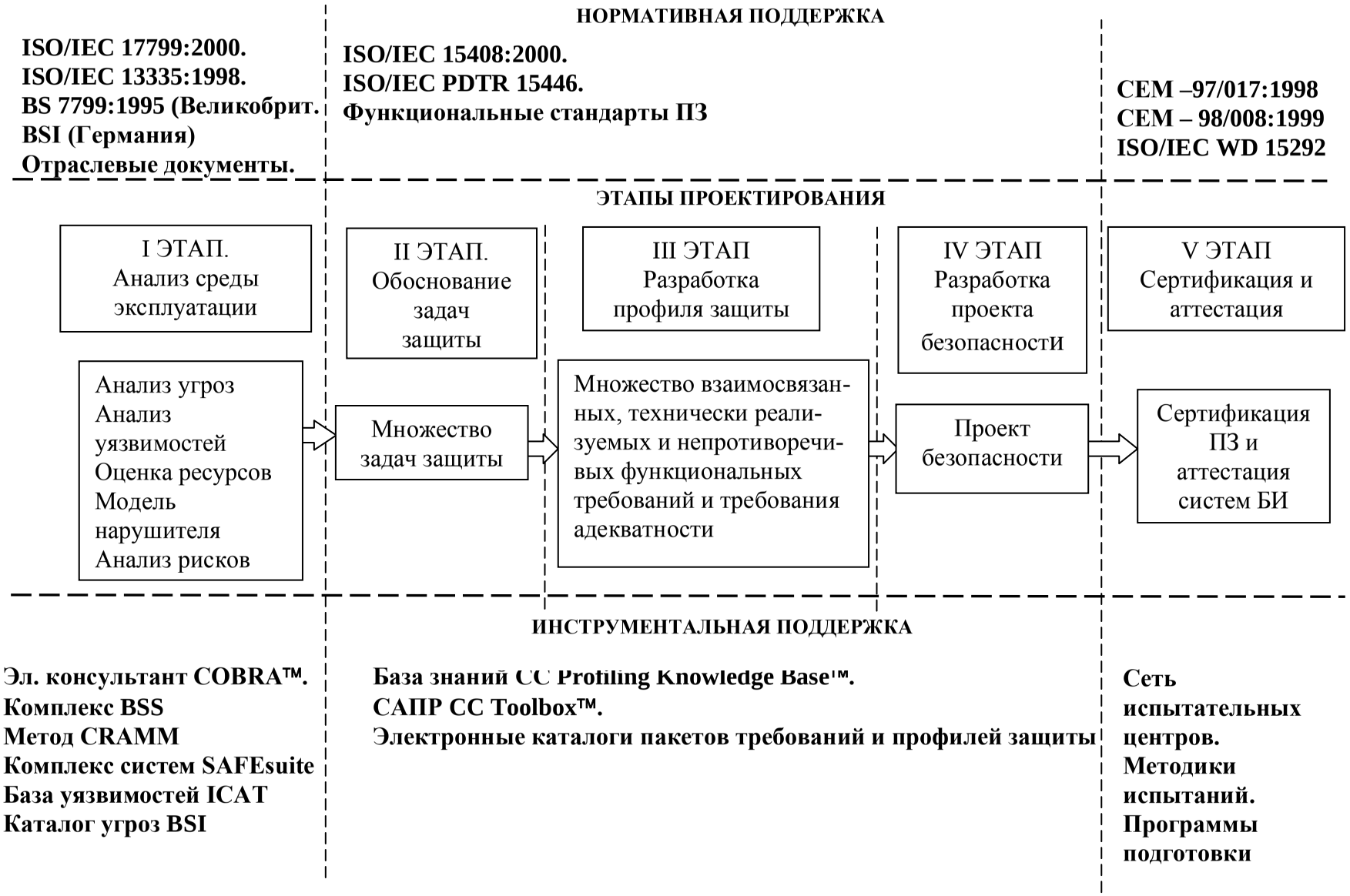

Рисунок 10 – Новая технология проектирования систем обеспечения ИТ-безопасности

профиля защиты и проекта безопасности являются основой технологии проектирования системы обеспечения ИТ-безопасности.

II.1 Этапы проектирования современных систем ИТ-безопасности

Проектирование системы обеспечения ИТ-безопасности осуществляется в пять этапов (рис. 10).

I этап. Анализ безопасности среды эксплуатации

На данном этапе осуществляется:
- определение сферы (границ) системы ИБ и конкретизация целей ее создания;
- определение степени опасности (агрессивности) среды эксплуатации для функционирования ТОЕ путем выявления угроз и оценки рисков;
- формирование исходных предпосылок для определения задач по обеспечению ИТ-безопасности.

Среда эксплуатации представляет собой совокупность физических, информационных, технических объектов и систем, внешних по отношению к ТОЕ, а также организационных мер, правовых норм, условий эксплуатации и технологических особенностей применения ТОЕ, оказывающих физическое, информационное, энергетическое и другое воздействие на функционирование ТОЕ.

На данном этапе решаются следующие задачи:
- анализ среды эксплуатации, с точки зрения обеспечения физической безопасности;
- оценка ресурсов, подлежащих защите;
- построение модели нарушителя, анализ методов нападений и уязвимостей системы;
- формирование полного перечня угроз безопасности;
- оценка рисков и выбор стратегии управление рисками.

По сути, на данном этапе вырабатываются концепция обеспечения информационной безопасности и политика безопасности.

Стандарт ISO/IEC 15408 детально не регламентирует последовательность решения и содержание выше перечисленных задач. Однако данные вопросы являются объектами стандартизации международных стандартов ISO/IEC 13335:1997 «Руководство по управлению ИТ-безопасностью» [16], ISO/IEC 17799:2000 «Практические рекомендации по управлению ИТ-безопасностью» [17]. Также эти вопросы стандартизуются Национальным стандартом Великобритании BS 7799:1995 «Управление безопасностью» [18], немецким стандартом BSI «Руководство по защите информационных технологий для базового уровня» [19] и иными документами.

Требования этих стандартов учтены при разработке нескольких инструментальных средств, направленных на решение задач первого этапа. К наиболее мощным и широко поддерживаемым средствам можно отнести:

- электронный консультант COBRA™, который содержит основные базы знаний для оценки рисков в соответствии с требованиями стандарта ISO/IEC 17799 (Великобритания);
- инструмент для проведения базового анализа рисков BSS (Baseline Security Survey, Великобритания);
- метод CRAMM – метод Центрального агентства по компьютерам и телекоммуникациям Великобритании для анализа рисков; метод опирается на использование методов структурного анализа и проектирования;
- комплекс систем SAFEsuite, реализующий методику ADDME (Assess, Design, Deploy, Manage and support Education); комплекс обеспечивает поддержку стандарта BS 7799 и предлагается компанией ISS.

Кроме того, широко доступны каталог угроз безопасности Германского комитета по стандартизации (поддержка стандарта BSI) и база уязвимостей ICAT Национального института по стандартизации и технологиям США.

II этап. Определение и формулировка задач по обеспечению безопасности

На данном этапе на основе результатов анализа среды эксплуатации осуществляется формулировка множества задач защиты. Задачи защиты должны быть согласованы со множеством других функциональных задач объекта оценки и не противоречить основному назначению ТОЕ. Они определяются как для объекта оценки, так и для среды его эксплуатации и адресованы исключительно для реализации требований по обеспечению ИТ-безопасности.

III этап. Выбор и разработка требований ИТ-безопасности

Сформулированные задачи защиты являются базой для непосредственной разработки профиля защиты, которая осуществляется в два этапа:

– поиск и выбор профиля прототипа;
– уточнения и синтез требований ИТ-безопасности.

Профиль защиты (ПЗ) – это реализационно-независимая совокупность функциональных требований и требований адекватности, направленных на удовлетворение потребностей потребителя (пользователя и владельца) защищаемых ресурсов в обеспечении безопасности информации. Профиль защиты является нормативным документом, который регламентирует все аспекты ИТ-безопасности в виде совокупности требований ИТ-безопасности, предъявляемых к функциям безопасности и, следовательно, к механизмам безопасности и средствам защиты.

Международный стандарт предусматривает создание специальной электронной картотеки пакетов требований безопасности, профилей защиты и проектов безопасности. *Пакетом требований* называется промежуточная комбинация требований безопасности, которая описывает множество функциональных требований и требований адекватности, обеспечивающих решение одной или выделенного подмножества задач защиты. Данная картотека уже доступна разработчикам, что позволяет минимизировать затраты на разработку новых профилей защиты, учесть опыт предыдущих разработок, обеспечить реальную взаимосвязь и совместимость разрабатываемых продуктов, а также повысить взаимопонимание разработчиков систем ИТ-безопасности различных государств.

Требования ИТ-безопасности являются уточнением, конкретизацией и практическим отображением задач защиты и включают в себя три компоненты:
– функциональные требования безопасности;
– требования адекватности;
– требования безопасности к среде эксплуатации.

В ходе разработки профиля защиты осуществляется выбор требований безопасности, специфичных для конкретной среды. Выбор осуществляется на основе оценки эффективности реализации данных требований для решения задачи противодействия угрозам безопасности. Функциональные требования определяют свойства безопасности и характеризуют функции безопасности ТОЕ, которые являются типичными для поддержки ИТ-безопасности. Единые критерии отличаются особенно тщательной проработкой функциональных требований. На наш взгляд функциональные требования позволяют осуществить описание функции безопасности в виде операторной модели (рис. 11).

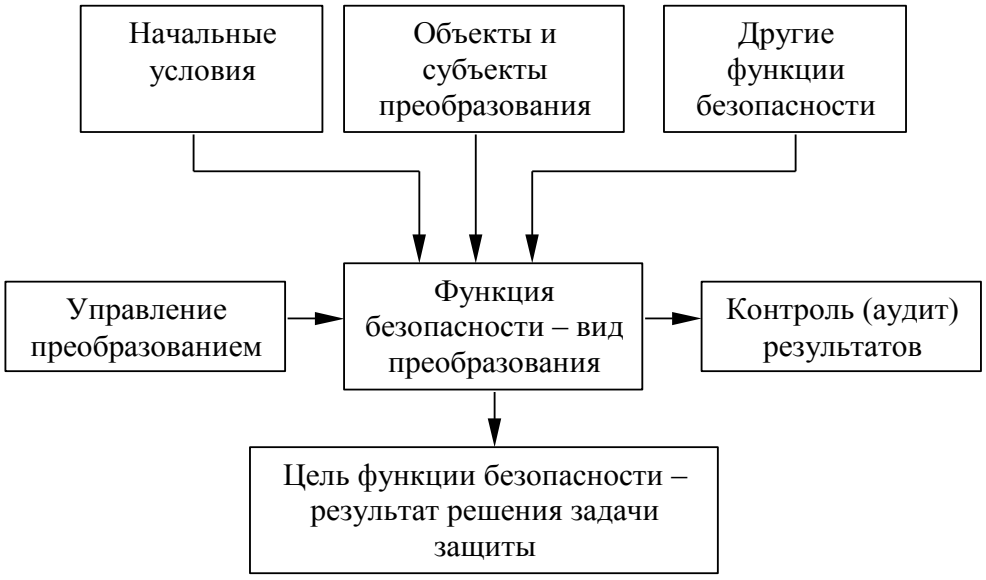

Рисунок 11 – Операторная модель функции безопасности

Здесь функция безопасности выступает в роли оператора – целенаправленного воздействия на объект (действий над объектом) с целью реализации функциональных требований (набора функциональных требований), направленного на решение задачи защиты и, в конечном итоге, достижения главной цели безопасности.

Функция безопасности (оператор безопасности) определяется (описывается) следующим образом:
- вид осуществляемого преобразования (простого или сложного), т. е. какую операцию осуществляет;
- объекты и субъекты, подлежащие преобразованию или участвующие в преобразовании;

- условия выполнения преобразования: начальные условия, управление преобразованием, аудит (контроль) над ходом и результатом преобразования;
- взаимосвязи с другими операторами.

Демонстрация того, что выполнение функциональных требований ведет к обеспечению требуемого уровня безопасности, осуществляется путем включения в профиль защиты требований адекватности. Адекватность включает в себя два аспекта:

– эффективность функции безопасности;
– корректность реализации функции безопасности.

При оценке эффективности функций безопасности необходимо определить степень соответствия между задачами защиты и предлагаемым набором функций безопасности, их функциональной полнотой, согласованностью, простотой использования и степенью предотвращения угроз безопасности. Кроме того, можно выдвигать и дополнительные требования, например, такое как гибкость, рассмотренное в [8].

Корректность выражается в оценке правильности и надежности реализации функций безопасности.

Для конкретного множества функциональных требований в зависимости от среды эксплуатации и требований безопасности уровень обеспечиваемой адекватности может варьироваться, что выражается через уровни строгости требований адекватности. Шкала уровней также вводится Едиными критериями.

При разработке профиля защиты учитываются связи, как между различными функциональными требованиями, так и между функциональными требованиями и требованиями адекватности.

IV этап. Разработка спецификаций функций безопасности и итоговой спецификации обеспечения безопасности TOE

Данный этап является по сути разработкой проекта безопасности.

Проект безопасности представляет собой множество требований ИТ-безопасности и спецификаций функций безопасности. Проект безопасности используется в качестве основы для разработки и оценки (аттестации) TOE на соответствие требованиям ИБ. Итоговая спецификация включает в себя описание заявленных функций безопасности, которые удовлетворяют функциональным требованиям, и определение показателей адекватности, характеризующих степень удовлетворения требований адекватности.

Нормативной поддержкой второго, третьего и четвертого этапа являются международный стандарт ISO/IEC 15408 [1–3]. Кроме того, уже разослан на обсуждение проект международного стандарта ISO/IEC 15446 “Руководство по разработке профилей защиты и проектов безопасности” [4].

В настоящее время уже представлены проекты многих профилей защиты, таких как:

– профиль защиты CS2 – соответствует одноименному ПЗ американских Федеральных критериев безопасности и ориентирован на коммерческие системы общего назначения с жесткими требованиями по обеспечению информационной безопасности;
– профиль защиты RBAC – ПЗ управления доступом на основе ролей (функциональных обязанностей персонала в пределах одной организации);
– два правительственных профиля защиты межсетевых экранов Firewall PP project – ПЗ межсетевого экрана прикладного уровня и ПЗ межсетевого экрана фильтра трафика для операционной среды с низкими рисками.

На стадии разработки находятся ПЗ телекоммуникационных коммутаторов, обнаружения проникновения, офисных АТС, системы управления доступа на основе класса «С2» «Оранжевой книги» и системы обеспечения безопасности с использованием меток безопасности на основе класса В1. Готовятся к выполнению проекты по разработке ПЗ медицинских и финансовых информационных систем, а также ПЗ для системы распределенной системы управления воздушным движением США [20].

Как видно уже осуществляется не только разработка новых профилей, но и активная адаптация прежних систем, разработанных на основе требований более ранних нормативных документов к требованиям новых стандартов. Поддержка документов осуществляется в рамках международной программы NIAP – The National Information Assurance Partnership, координаторами которой являются NIST и Агентство национальной безопасности США.

Глубина и продуманность нового документа уже сегодня позволила создать автоматизированные средства проектирования профиля защиты и проекта безопасности. В рамках программы NIAP разработана база знаний CC Profiling Knowledge Base™ и САПР профиля защиты CC Toolbox™, которые в совокупности представляют собой мощную среду разработки и являются АРМом разработчика профилей защиты и проектов безопасности.

Требования безопасности демонстрируют как наличие желаемых характеристик и свойств безопасности, так и отсутствие нежелательных характеристик. Желаемые характеристики можно продемонстрировать путем использования и тестирования конкретного продукта, в то время как определение нежелательных

характеристик затруднительно. Проверка, моделирование, анализ конструкции и реализации профиля защиты и проекта безопасности существенно снижает риск присутствия таких нежелательных характеристик. Поэтому итогом проектирования является **последний этап.**

V этап. Сертификация или аттестация ПЗ и ПБ

На данном этапе осуществляется оценка полноты, корректности, непротиворечивости (согласованности) и реализуемости ПЗ и ПБ. Основой нормативной поддержки этого этапа является проект документа «Общая методология оценки безопасности информационных технологий» [5, 6] (CEM-97/017 и CEM - 99/008).

В основу общей методологии заложены принципы соответствия, беспристрастности, объективности, повторимости и воспроизводимости, единства терминологии [5]. *Общая модель методологии испытаний* – это определение ролей и сфер ответственности всех участников испытаний. Она определяет требования, которым должны удовлетворять методики испытаний, чтобы результаты получили взаимное признание.

Серию документов Единых критериев логически завершает «Соглашение о взаимном признании сертификатов в области безопасности информационных технологий», заключенное между правительственными организациями США и ведущими западноевропейскими державами. Если Единые критерии и Общая методология создали единую методологическую базу для проектирования систем ИТ-безопасности и признания сертификатов, то соглашение закрепляет эту базу юридически.

II.2 Где находится Украина

Попытаемся оценить состояние решения проблемы обеспечения информационной безопасности в нашем государстве. Авторы не берутся выразить взгляды всей профессиональной общественности, однако считают, что выразителем этих взглядов является отечественная нормативная база. Показательным, в данном случае, является анализ таких документов, как НД ТЗИ 1.1 – 002 –99 «Основные положения по защите информации в компьютерных системах от несанкционированного доступа», НД ТЗИ 3.7. – 001 – 99 «Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе», НД ТЗИ 1.1 – 003 –99 «Терминология в области защиты информации в компьютерных системах от несанкционированного доступа» и других документов [21 – 28].

В целом в данных документах отражены произошедшие изменения. Так в НД ТЗИ 1.1 – 002 – 99 одним из принципов обеспечения защиты информации является определение услуги безопасности, а задание функций и механизмов защиты является принципом реализации программно-технических средств. Однако, с одной стороны, перечень услуг безопасности включает в себя только услуги конфиденциальности, целостности, доступности и наблюдаемости. С другой стороны, сфера действия всех документов ограничивается компьютерными или автоматизированными системами, а идеология построения системы защиты имеет перекос в сторону обеспечения технической защиты информации. Хотя нужно отметить, что в документе говорится об эквивалентности терминов «компьютерная система» и «автоматизированная система» термину «объект оценки», вводимому Едиными критериями (под объектом оценки в ISO/IEC 15408 понимают ИТ-продукт или ИТ-систему). Однако в нем, а также в других отечественных нормативных документах, такие понятия, как информационная технология, задача защиты и ИТ-безопасность отсутствуют.

Это позволяет говорить о том, что хотя общее направление решения задач защиты информации, если можно так выразиться, «гармонизировано» с мировыми тенденциями, мы пока находимся под влиянием старой модели защиты информации. Украинские нормативные документы еще не свободны от устаревших взглядов на защиту информации, которые превалировали в СССР (жесткое деление на техническую и криптографическую защиту информации и ограниченность сферы применения положений защиты информации). Сейчас мы находимся на полпути, занимаем не совсем четкую позицию в вопросе обеспечения ИТ-безопасности и на законодательном уровне Украина, на наш взгляд, не готова перейти на новую идеологическую концепцию обеспечения информационной безопасности.

Анализ ситуации, сложившейся в данный момент в Украине, позволил авторам сделать следующие выводы.

Во многих организациях руководители и специалисты недостаточно используют международные стандарты при проектировании надежных систем безопасности. Причиной этого является незнание большинством руководителей и специалистов, отвечающих за организацию работ по обеспечению режима безопасности, требований международных стандартов. Порой специалисты вообще не знают, что такой стандарт существует. Основные усилия концентрируются на применении отдельных, не связанных между собой технических и криптографических средств. Несколько улучшает ситуацию принятие ряда нормативных документов ДСТСЗИ.

Отечественными специалистами–разработчиками освоена ничтожно малая доля международных стандартов в области обеспечения безопасности. Рассмотренные выше методологические стандарты

практически не известны и не используются многими специалистами при системном проектировании. Об этом говорит не только отсутствие соответствующих инструментальных средств проектирования на отечественном рынке, но и малое количество публикаций об этих стандартах в отечественной специальной прессе. Авторы смогли найти одну публикацию по стандарту ISO/IEC 13335 (Институт кибернетики), публикацию с упоминанием BS 7799 и несколько работ Харьковских специалистов.

Это говорит о том, что национальный разработчик не готов или не может использовать методологические наработки мирового сообщества в данном вопросе, руководители предприятий (потребители), по незнанию, не предъявляют повышенных требований к качеству решения проблемы информационной безопасности на вверенных им объектах, а контролирующие органы не готовы перейти на новую нормативную базу сертификации в данной области. Дальнейшая недооценка этих документов приведет, с одной стороны, к отставанию национальных систем от уровня разработок западных специалистов, а с другой, существенно усложнит выход Украины на западные рынки и интеграцию в ЕС, что является на сегодня одной из основных государственных задач.

Украина первая среди стран СНГ осознала перспективность разработок в данном направлении обеспечения ИТ-безопасности. Это выразилось в принятии в 1999 году нормативного документа НД ТЗИ 2.5-004-99 «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа», который базируется на анализе Федеральных критериев США и критериев оценки безопасности Канады. Данный документ сыграл значительную положительную роль, выражающуюся в том, что отечественные специалисты изучили новые подходы к оценке ИТ-систем и осваивают новые технологии разработки комплексных систем защиты информации. Однако, на наш взгляд, дальнейшее использование этого документа в том виде, в котором он существует сейчас, будет являться тормозом развития, как национальной нормативной базы, так и технологий разработки современных отечественных систем обеспечения ИБ. Основной причиной такого состояния является то, что национальный нормативный документ не гармонизирован с международным стандартом. Это значит, что отечественный разработчик, разрабатывающий системы по требованиям национального документа, не сможет обеспечить совместимости своих систем с зарубежными, а в перспективе не сможет достойно представить свою продукцию на рынках Западной Европы, Северной Америки и других регионов мира. С другой стороны необходимо признать, что отечественный нормативный документ не может сравниться по глубине системной проработки вопросов с ISO/IEC 15408 и группой поддерживающих документов.

Таким образом, на наш взгляд, назрела необходимость **организовать работы по пересмотру отечественных документов с целью их гармонизации с международным стандартом ISO/IEC 15408.** Этим шагом Украина должна подтвердить свое первенство в этих вопросах среди стран СНГ. Лучшее решение – это принятие международного стандарта в качестве национального стандарта.

II.3 Почему необходимо поддержать и принять такое решение

1. Украина, да и любая другая держава в отдельности, не способна поддерживать в полном объеме на достаточно высоком уровне всю нормативную базу в области ИТ-безопасности и соответствующую инструментальную поддержку новой технологии проектирования ИТ-систем и ИТ-продуктов. Уже сейчас наблюдается разделение труда в области разработки приложений, поддерживающих различные этапы технологического цикла разработки систем безопасности. Ведение же баз данных по угрозам безопасности и уязвимостей ИТ-систем вообще невозможно осуществить в одиночку.

Гармонизация с международными стандартами позволит разработчикам отечественных систем в полной мере воспользоваться уже существующими наработками в данной области. Имеется ввиду использование электронных каталогов профилей защиты и проектов безопасности. Кроме того, разработанные и сертифицированные в соответствии с Едиными критериями отечественные системы могут поставляться на рынки ЕС и иметь определенные конкурентные преимущества. Отсутствие такой сертификации практически закрывает нам эти рынки. Принятие гармонизированного с Едиными критериями национального стандарта даст новый толчок в развитии отечественных систем безопасности ИТ-технологий. Разработчики получат новый мощный инструмент проектирования и создания ИТ-систем, отвечающих современным требованиям ИТ-безопасности.

2. Гармонизация способствует интеграции информационных систем Украины с национальными системами других государств. Задача гармонизации – это государственная задача. Так в Указе Президента Украины № 797/2001 от 5. 09. 2001 указывается, что «с целью обеспечения реализации стратегического направления внешнеэкономической политики по отношению интеграции Украины в мировую экономику, комплексного реформирования внешнеторгового режима и обеспечения дальнейшей гармонизации законодательства Украины с нормами и принципами Всемирной организации торговли необходимо осуществлять работы по гармонизации национальных стандартов с требованиями международной и

Европейской систем стандартизации и сертификации и обеспечить ежегодную разработку и принятие не менее 500 гармонизированных стандартов». Имеются аналогичные решения Кабинета Министров и Совета по национальной безопасности и обороне. На наш взгляд в области безопасности информационных технологий мы должны показать пример решения этой задачи.

3. К этому решению нас подталкивают и решения наших ближайших соседей. Так в Российской Федерации уже ведутся работы по принятию стандарта ISO/IEC 15408 методом обложки, а на данный момент разработан проект руководящего документа Гостехкомиссии РФ «Руководство по проектированию и эксплуатации автоматизированных систем, отвечающих требованиям информационной безопасности» и ряд других документов, которые идеологически близки к международным стандартам. В Республике Беларусь также ведутся работы по разработке нормативной базы, информационной и научно-технической основой которой является стандарт ISO/IEC 15408 [20, 29].

III Что сделано и что нужно сделать

1. Несомненно, принятием ряда нормативных документов в Украине сделан первый и важный шаг по изменению старой идеологии, старых взглядов на обеспечение безопасности информации. Новые отечественные документы в некоторой степени отражают произошедшие изменения в области ИТ-безопасности и ориентируют разработчиков и заказчиков на принципиально новые технологии проектирования систем ИБ.

2. В Харьковском Национальном университете радиоэлектроники в учебные программы по дисциплинам “Стандартизация и сретификация в области безопасности информации” и “Проектирование систем и средств защиты информации” для специалистов и магистров введены разделы и темы по изучению новых международных стандартов и освоению современных методик и интсрументальных средств проектирования систем БИ. Осваивается работа с АРМом разработчика профилей защиты и проекта безопасности и инструментальные средства по анализу рисков. Таким образом, уже начата подготовка нового поколения специалистов, знакомых с требованиями международных стандартов.

3. В отечественную практику реально внедряются разработки, опирающиеся не только на национальную нормативную базу, но и на требования международных стандартов. Специалистами ХНУРЕ и Института информационных технологий, разработан ряд ведомственных нормативных документов и документов предприятий (концепция обеспечения безопасности и политика безопасности) с учетом требований международных стандартов. Очевидно, такие работы ведутся и другими разработчиками, однако они не имеют широкого распространения.

4. В рамках специальной программы специалистами ХНУРЕ осуществляется активная популяризация новых документов и взглядов в области обеспечения ИТ-безопасности на страницах не только научных журналов [7–10], но и научно-популярных и информационных изданий.

Однако этого не достаточно. По нашему мнению для того, чтобы существенно продвинутся вперед, необходимо предпринять ряд конкретных шагов по реальной гармонизации отечественной нормативной базы с международной. И здесь возможны два направления решения этой задач:

– принятие международного стандарта ISO/IEC 15408 в качестве национального государственного стандарта Украины на основе Закона Украины «О стандартизации» и других нормативно-правовых актов и международных соглашений;

– использование общих критериев в качестве методической, информационной и научной базы для разработки национальных стандартов в области безопасности информационных технологий и нормативных документов систем ТЗИ и КЗИ.

В первом случае имеются некоторые трудности, и их решение потребует определенного времени, поэтому параллельно с решением первой задачи в рамках нормативной работы Департамента специальных телекоммуникационных систем и защиты информации необходимо уже сейчас приняться за поэтапную разработку комплекса нормативных документов на основе международных стандартов. Новые нормативные документы с сегодняшнего дня, по нашему мнению, должны с самого начала разрабатываться на основе и с учетом требований ISO/IEC 15408. Эти документы могут быть разбиты на две группы:

– документы общего назначения, включающие: терминологию в области ИБ, общую модель оценки, каталог функциональных и гарантийных требований, руководство по проектированию ПЗ и ПБ, общую методологию оценки безопасности, документы по порядку аттестации и сертификации систем ИБ;

– документы прикладного характера, содержащие профили защиты различных объектов: СВТ, ЛВС, АСУ, СУБД, ОС и др., а также типовые программы и методики сертификационных испытаний типовых объектов информатизации.

Здесь как никогда разработчикам нормативных документов необходима поддержка всех отечественных специалистов. Мы должны консолидировать свои усилия для создания современной нормативной базы.

Среди других первоочередных задач можно выделить:

– активное внедрение в процесс подготовки новых профессиональных и научных кадров последних достижений стандартизации в данной области, для чего скорректировать соответствующие учебные планы и программы;

– практическое освоение новой технологии проектирования систем ИБ и поддерживающих ее инструментальных средств, при этом максимально использовать как открытые (свободного доступа), так и платные мировые ресурсы для оптимизации своей деятельности и экономии собственных ресурсов. На уровне правительственных, учебных, научных и общественных организация участвовать в международных программах и проектах, поддерживающих новые международные стандарты. В ближайшей перспективе принять участие в принятии межгосударственных стандартов (стандартов СНГ) в данной области совместно с Российской Федерацией, республикой Беларусь и другими странами СНГ;

– проводить активную популяризацию идей и требований международных стандартов среди потребителей ИТ-систем.

В ХНУРЕ уже имеется определенный опыт в решении этих задач и специалисты университета готовы поддержать проведение различных работ в данном направлении.

Выводы

1. Международные стандарты ISO/IEC 15408 и ISO/IEC 15446 закрепили новый подход к проектированию и разработке безопасных информационных технологий на основе разработки профиля защиты и проекта безопасности, которые включают в себя совокупность взаимосвязанных функциональных требований безопасности и требований адекватности. В сущности, стандарты определяют новый метаязык, позволяющий формализовать задачи проектирования систем ИТ-безопасности. Концепция обеспечения безопасности базируется на типовой схеме жизненного цикла сложных систем, последовательной детализации требований и спецификаций компонентов, к которым относятся среда эксплуатации, ТОЕ, задачи по обеспечению безопасности, требования ИТ-безопасности, спецификации функций безопасности, задачи инструментальных средств безопасности. Стандарты представляют парадигму построения и реализации структурированных и детализированных функциональных требований к компонентам защиты ИТ, а также раскрывают цели, определяют методы и уровни адекватности функций безопасности. В целом стандарты представляют собой детальное комплексное руководство, охватывающее требования к функциям и методам гарантирования качества основных современных методов и средств обеспечения безопасности ИТ. В совокупности с Общей методологией оценки ИТ-безопасности эти нормативные документы создали единую методологическую базу для создания, разработки и сертификации продуктов и систем информационных технологий с точки зрения обеспечения безопасности информации.

2. Принятие Единых критериев заложило основы реализации нового направления стандартизации – функциональной стандартизации в области ИТ-безопасности. При функциональной стандартизации объектом стандартизации являются каталоги функциональных требований и требований адекватности, общие требования к формированию на их основе профилей защиты и проектов безопасности и непосредственно профили защиты и проекты безопасности конкретных ИТ-продуктов и ИТ-систем. Уже сегодня разработано несколько профилей защиты различных ИТ-систем.

3. Новый международный стандарт и поддерживающие его документы активно поддерживаются ведущими в области информационных технологий государствами и международным сообществом в целом. Это выражается в заключении между государствами большой семерки соглашения о взаимном признании сертификатов в области ИТ-безопасности, полученных в системе сертификации, опирающейся на Единые критерии. Это позволяет:

– обеспечить высокий уровень стандартов, регламентирующих проведение сертификационных испытаний и как следствие повысить уверенность в безопасности ИТ-продуктов и ИТ-систем;

– обеспечить доступ на рынки других стран сертифицированных продуктов;

– исключить дублирование при проведении испытаний ИТ-продуктов и сертификации ПЗ;

– повысить эффективность и снизить стоимость процессов испытаний и сертификации продукции и услуг в области ИТ-безопасности.

В США, Великобритании, Канаде и Германии, в рамках международной программы NIAP реализуются проекты по разработке инструментальных средств, поддерживающих все этапы технологии проектирования ИТ-систем с учетом требований Единых критериев. Такое объединение усилий ведущих государств по разработке единой нормативно-правовой, организационно-методической и материально-технической базы обеспечения ИТ-безопасности говорит как о важности этой проблемы в целом, так и о значимости нового международного стандарта в частности. Сегодня весь мир переживает последствия террористического акта, произошедшего в США 11 сентября 2001 года. Одним из выводов экспертов Совета Национальной

безопасности США, сделанных в ходе анализа причин и последствий этого трагического события, является то, что в настоящее время имеется реальная возможность осуществления компьютерных атак с целью выведения систем управления объектами стратегического значения, информационных систем национального и межгосударственного значения. Успех в предотвращении такого рода атак может быть достигнут только путем интеграции усилий всех государств – участников информационных отношений. И, на наш взгляд, новый стандарт является одним из ключевых звеньев создания общей межнациональной системы обеспечения ИТ-безопасности.

Применение новых международных стандартов будет способствовать повышению уровня отечественных разработок, признанию сертификатов безопасности различных государств и послужит основой для вхождения Украины в международную систему стандартизации и сертификации в области безопасности информационных технологий.

Литература: 1. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model. 2. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements. 3. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements. 4. ISO/IEC WD 15292 – Information Technology – Security techniques – Protection Profile registration procedures – 1999. 5. CEM-97/017 – Common Evaluation Methodology for Information Technology security. – Part 1: Introduction and general model. – Ver. 0.6 – 1997. 6. CEM-99/008 – Common Evaluation Methodology for Information Technology security. – Part 2: Evaluation Methodology. – Ver. 0.6 – 1999. 7. Горбенко И. Д., Потий А. В, Терещенко П. И. Критерии и методология оценки безопасности информационных технологий // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2000. – Вып. 114. – С. 25–38. 8. Скрыпник Л. В, Потий А. В. Гибкость и специализация профиля защиты автоматизированной системы // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2001. – Вып. 119. – С. 17–21. 9. Горбенко И. Д., Потий А. В., Терещенко П. И. Рекомендации международных стандартов по оценке безопасности информационных технологий // Материалы третьей международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах». – Киев 2000. – С. 150–160. 10. Бондаренко М. Ф., Черных С. П., Горбенко И. Д., Замула А. А., Ткач А. А. Методологические основы концепции и политики безопасности информационных технологий // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – 2001. – Вып. 119. – С. 5–17. 11. ISO 7498-2:1989 – Information technology – Open Systems Interconnection – Basic reference model – Part 2: Security architecture. 12. ISO/IEC 10181-(1-7):1996 – Information technology – Open Systems Interconnection – Security frameworks for open systems. 13. Закон Украины «О Национальной программе информатизации» № 74/98-ВР – Ведомости Верховного совета – 1998 – № 27–28. 14. Щербо В. К. Стандарты вычислительных сетей. Взаимосвязи сетей. Справочник. – М.: Кудиц-образ, 2000. – 198 с. 15. Gary Stoneburner. Underlying Technical Models for Information Technology Security – NIST Special Publications – 2001. 16. ISO/IEC 13335-(1-3): 1998 – Information technology –Guidelines of IT Security. 17. ISO/IEC 17799:2001 – Information technology. – Information Security Management – Code of Practice for Information Security Management. 18. BS 7799: 1995 – Code of Practice for Information Security Management. 19. Bundesmat fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual. – 1998. 20. Анищенко В. В. Оценка информационной безопасности // PC Magazine/RE – № 2. – 2000. – С. 7–11. 21. НД ТЗИ 1.1 – 002 – 99. Основные положения по защите информации в компьютерных системах от несанкционированного доступа. 22. НД ТЗИ 1.1 – 003 –99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. 23. НД ТЗИ 2.5 – 004 – 99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа. 24. НД ТЗИ 3.7. – 001 – 99. Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе. 25. НД ТЗИ 2.5. – 005 – 99. Классификация автоматизированных систем и стандартные профили защищенности обрабатываемой информации от несанкционированного доступа. 26. Концепция технической защиты информации в Украине. Постановление Кабинета министров Украины от 08. 10. 97 № 1126. 27. Положение о технической защите информации в Украине. Указ Президента Украины от 27. 09. 99 № 1229. 28. Положение о порядке осуществления криптографической защиты информации в Украине. Указ Президента Украины от 22. 05. 1998 № 505/98. 29. Анищенко В. В., Фисенко В. К. Проблемы и перспективы стандартизации в области безопасности информационных технологий в Республике Беларусь // Материалы Международной НТК "Информационная безопасность" – Минск, 2000.