ИДЕОЛОГИЧЕСКАЯ И ТЕХНОЛОГИЧЕСКАЯ ОСНОВЫ ПОДГОТОВКИ СПЕЦИАЛИСТА В ОБЛАСТИ БЕЗОПАСНОСТИ БАНКОВСКИХ СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

***О.В. Васюренко**, д.э.н.; **И.Д. Горбенко**, д.т.н., проф.,*
Харьковский филиал Украинской академии банковского дела;
***А.В. Потий**, к.т.н.*
Харьковский национальный университет радиоэлектроники

Обеспечение безопасности банковской деятельности – комплексная задача, которая решается на законодательном, административном, процедурном и программно-техническом уровнях. При подготовке специалистов по безопасности банковских технологий необходимо четко определить область и предмет изучения. Сегодня можно с уверенностью говорить, что одним из принципов построения современных банковских технологий является широкое использование телекоммуникационных систем и информационных технологий (ИТ). Таким образом, областью подготовки специалиста будет являться безопасность информационных технологий (ИТ-безопасность), а предметом, в самом общем смысле, – надежные системы и продукты информационных технологий (ИТ-системы и ИТ-продукты), процессы их разработки, создания, внедрения, эксплуатации (администрирования), сертификации и аттестации, уничтожения.

В данной статье излагается концепция обеспечения безопасности информационных технологий. Данная концепция отражает идеологию построения систем информационной безопасности в рамках которой, по нашему мнению, должна осуществляться подготовка специалиста в области ИТ-безопасности.

Подготовка специалиста должна иметь также и практическую направленность, быть ориентированной на получение навыков по решению практических задач обеспечения ИТ-безопасности на объекте. По типу практической деятельности можно выделить три группы специалистов:

- организатор процесса обеспечения ИБ банка или банковской системы (руководящее звено);
- специалисты по администрированию систем ИТ-безопасности (звено эксплуатации ИТ-систем);
- разработчики систем информационной безопасности.

Специалисты этих групп выполняют различные функциональные обязанности, решают различные классы практических задач и должны обладать различными умениями. Однако с практической точки зрения в основу их деятельности закладывается, в той или иной мере, общий технический объект – система ИТ-безопасности. Специалисты всех трех групп должны знать общую технологию проектирования современных систем ИТ-безопасности и сущность проблем, возникающих на всех этапах жизненного цикла систем подобного рода. В связи с этим в статье рассматривается новая технология проектирования систем обеспечения ИТ-безопасности, закрепленная в международном стандарте ISO/IEC 15408 “Критерии оценки безопасности информационных технологий” (далее Единые критерии) и группе поддерживающих его нормативных документов [1-3].

Понимание профессорско-преподавательским составом идеологического и технологического аспектов обеспечения ИТ-безопас-ности, рассматриваемых в данной статье, должно выступить единой системной основой, объединяющим фактором при разработке учебных планов и программ подготовки специалистов различного профиля в области безопасности банковских технологий.

Главная цель безопасности банковских информационных технологий заключается в обеспечении возможности любой банковской организации решать (выполнять) свои функциональные задачи (финансовые операции, обслуживание населения, задачи управления банком и технологическими процессами, подразделениями и т.д.) путем построения ИТ-систем, которые исключают или минимизируют ИТ-риски банка, его партнеров и клиентов.

Отправной точкой в достижении цели ИТ-безопасности являются задачи по обеспечению 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).

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 они 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 её компонент не может быть удален, модифицирован или добавлен в обход или 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;
- 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.

Зависимость конфиденциальности от целостности выражается в том, что если целостность системы будет нарушена, 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”.

Решение задач защиты возлагается на услуги безопасности. Перечень услуг безопасности, по сравнению с ISO 7498-2 и ISO/IEC 10181, значительно расширился. Теперь услуги, в зависимости от того, на решение каких задач они направлены, можно отнести к одному из трех классов:

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* (5 услуг) – это услуги безопасности, в основном ориентированные на предотвращение различного рода нарушений безопасности.
3. *Услуги обнаружения нарушений и восстановления безопасности* (4 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 (рисунок). Данная модель иллюстрирует использование основных услуг безопасности при обеспечении ИТ-безопасности и взаимодействие данных услуг.

Опорные услуги безопасности, как уже было сказано, выступают в роли базиса, связующей среды 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.

Рис. Базовая техническая модель взаимодействия услуг безопасности

Управление криптографическими ключами. Данная услуга обязательна в случае применения криптографических функций в каких-либо услугах безопасности. 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 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 и 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". 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 основой 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.

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, позволяет авторам с уверенностью утверждать, что новая идеология построения систем безопасности информации уже реально воплотилась в новую технологию проектирования систем обеспечения ИТ-безопасности. Мы выделяем 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 профиля защиты и проекта безопасности являются основой технологии проектирования системы обеспечения ИТ-безопасности.

На основе результатов анализа среды эксплуатации осуществляется формулировка множества задач защиты. Задачи защиты должны быть согласованы с множеством других функциональных задач объекта оценки и не противоречить основному назначению TOE. Они определяются как для объекта оценки, так и для среды его эксплуатации и адресованы исключительно для реализации требований по обеспечению 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 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 компонента:

- функциональные требования безопасности;
- требования адекватности;
- требования безопасности к среде эксплуатации.

В ходе разработки профиля защиты осуществляется выбор требований безопасности, специфичных для конкретной среды, на основе оценки их эффективности 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. Функциональные требования позволяют осуществить описание функции безопасности в виде операторной модели.

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 такие как гибкость.

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.

Учитывая вышеизложенное, можно сделать следующие выводы.

Во-первых, 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 требования 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 требование 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.

Во-вторых, новый международный стандарт и поддерживающие его документы активно поддерживается 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 г. 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.

В-третьих, в программы подготовки всех специалистов по обеспечению ИТ-безопасности необходимо вводить изучение требований не только требований отечественных нормативных документов, но и требований международных

стандартов. Актуальность введения дисциплин, излагающих вопросы стандартизации и сертификации систем и средств безопасности информации, проектирования систем ИТ-безопасности в банковских системах усиливается еще и тем, что национальная банковская система Украины должна быть интегрирована с европейской системой, а информационные системы отечественных банков должны быть совместимыми с соответствующими системами зарубежных банков. При этом необходимо обеспечить надежную защиту информации. Решение этого противоречия может быть достигнуто путем использования международных стандартов и гармонизированных с ними национальных стандартов.

Список литературы

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.

Васюренко, О.В. Идеологическая и технологическая основы подготовки специалиста в области безопасности банковских систем инфрмационных технологий [Текст] / О.В. Васюренко, И.Д. Горбенко, А.В. Потий // Проблеми і перспективи розвитку банківської системи України: зб. наук. праць. - Суми: УАБС НБУ, 2002. - Т. 5. - С. 67-78.