В этом факте российской экономики завуалированы все угрозы экономической и социальной безопасности российского общества. Как свидетельствует история, в России было много разных реформ. Современные реформы в сфере образования, предусматривающие программы подготовки бакалавра и магистра, направлены на регресс интеллектуальных способностей выпускников вузов России. Само явление подготовки таких выпускников мотивирует сразу несколько вопросов. На некоторые из них ответить однозначно невозможно в силу того, что отсутствует правовой и социальный механизм трудоустройства выпускников вузов. Наконец, резонный вопрос – кто будет нести ответственность за реализацию таких образовательных программ?

В результате таких проектов российской экономике будет нанесен ощутимый финансовый ущерб. Здесь также кроются явные угрозы российскому обществу.

Таким образом, грядущая реформа в российском образовании в меньшей степени полезна, а в большей - явная угроза распада накопленного научно-образовательного потенциала российской высшей школы.

Конечно, ритмы развития современных наук резко ускоряются и мотивируют рост новых информационных технологий, что способствует формированию новых принципов мышления.

При этом никак нельзя допускать, чтобы политика в сфере профессионального образования России исходила от финансовых олигархов. Им безразличны духовные составляющие гражданина, в силу того, что деньги как эквивалент материальных ценностей ничего общего не имеют с духовными ценностями. К счастью, не все вузы России и Европы придерживаются интересов финансовых олигархов. Университеты Германии, например, отстаивают собственную индивидуальность.

Таким образом растет количество вузов, сопротивляющихся идеологии глобальной конкурентоспособности в силу того, что именно интеллигенция вузов всегда отстаивала духовные ценности, которые невозможно «заказать» никакими деньгами. Важная традиция!

Считаю, что именно таким традициям должна следовать российская образовательная система. Ибо человеческий морально-нравственный потенциал, который воспитывает и цементируется в вузах России, является и будет в дальнейшем являться критерием могущества российской государственной системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Алешенков М.С.* Комплексные угрозы российскому обществу XXI века: онтологические и методологические основы прогнозирования. –М.: ФГОУ ВПО МГАВМиБ им. К.И. Скрябина, 2003. - 168 с.

**Ю.В. Лозбенева, А.К. Шилов**
Россия, г. Таганрог, ТРТУ

## РАЗРАБОТКА ПРОФИЛЕЙ ЗАЩИТЫ В УЧЕБНОМ ПРОЦЕССЕ

Парадигма стандарта "Общие критерии" [1] требует формирования требований безопасности систем и продуктов информационных технологий (ИТ-продуктов) в виде профилей защиты (ПЗ) и заданий по безопасности (ЗБ).

Понятно, что изучение представления функциональных требований и требований доверия, а также приобретение навыков по разработке ПЗ и ЗБ различных ИТ-продуктов должно найти место в учебном процессе подготовки специалистов по защите информации.

«Общими критериями» [1] определены три основных этапа разработки профиля защиты, на которых устанавливаются: *среда безопасности*, *цели безопасно-*

*сти и требования безопасности*. Результаты выполнения этих этапов составляют основное содержание ПЗ. Курсивом здесь и далее выделены стандартные термины и понятия, относящиеся к «Общим критериям».

*Среда безопасности* устанавливается путем анализа:

- *физической среды* функционирования объекта оценки (ОО), в той ее части, которая определяет все аспекты эксплуатационной среды ОО, касающиеся его безопасности, включая мероприятия, относящиеся к физической защите и персоналу;

- *активов,* которые требуют защиты элементами ОО непосредственно, типа файлов и баз данных, или косвенно подчиненных требованиям безопасности, типа данных авторизации и реализации ИТ-продукта;

- *предназначения* объекта оценки, включая тип продукта и предполагаемую сферу его применения.

*Среда безопасности* включает законы, опыт, специальные навыки и знания, для которых решено, что они имеют отношение к безопасности, т.е. она определяет контекст предполагаемого применения ОО.

Установить *среду безопасности* также значит определить:

- *предположения,* которым удовлетворяла бы среда функционирования ОО для того, чтобы он считался безопасным;

- *угрозы* безопасности активов, относящиеся к ОО, идентифицированные и прогнозируемые на основе *анализа рисков* безопасности через понятие *агента угрозы* (нарушителя), предполагаемого *метода нападения* и *уязвимостей,* которые являются предпосылкой для нападения;

- *политику безопасности организации,* где функционирует оцениваемый ИТ-продукт с идентифицированными политиками и правилами, относящимися к ОО.

*Цели безопасности* устанавливаются на основе результатов анализа среды безопасности и направлены на противостояние установленным угрозам. Смысл определения *целей безопасности* заключается в отделении аспектов безопасности, связаных непосредственно с ОО, от тех, которые связаны с его средой. Такое разделение основано на совокупном учете проектных решений, политик безопасности, экономических факторов и решения о приемлемости рисков. *Цели безопасности для среды* ОО достигаются как в рамках информационных технологий, так и нетехническими или процедурными способами. *Требования безопасности ИТ* проистекают только из целей безопасности ОО и целей безопасности его среды, относящихся к ИТ.

В «Общих критериях» [1] представлены две различные категории *требований безопасности ИТ – функциональные требования* и *требования доверия*. *Функциональные требования* налагаются на функции ОО, предназначеные для поддержания безопасности ИТ, и определяют желательный безопасный режим функционирования ОО. Примерами функциональных требований являются требования к идентификации, аутентификации, аудиту безопасности и неотказуемости источника (невозможности отказа от факта отправления сообщения). Степень доверия для заданной совокупности *функциональных требований* может быть выражена через *требования доверия* и *шкалу оценочных уровней доверия (ОУД)*. *Требования доверия* налагаются на *действия разработчика*, *представленные свидетельства* и *действия оценщика*. Примерами *требований доверия* являются требования к строгости процесса разработки и требования по поиску потенциальных уязвимостей и анализу их влияния на безопасность. Понятие *доверия* к тому, что цели безопасности достигаются посредством выбранных *функций безопасности*, связано с уверенностью в *корректности реализации* и *эффективности* этих функций.

В стандарте 15408 [1] имеется строгая таксономия этих двух типов *требований – функциональных* и *доверия*. Таксономия включает в себя *классы, семейства, компоненты и элементы.* Основными конструктивными "кирпичиками" для синтеза систем защиты являются *компоненты,* которые содержат *функции безопасности* объекта оценки, а по сути – механизмы защиты. Конкретная настройка этих механизмов производится выполнением разрешенных операций в элементах: *итераций, назначения, выбора и уточнения.* Системность подхода поддерживается отражением в стандарте множества разнородных связей, которые в реальной системе защиты имеют место между ее отдельными механизмами. Так, между *компонентами* установлены следующие типы связей: по *ранжированию (иерархические*), по *управлению,* по *аудиту* и, так называемые, *зависимости*. Ключевым видом связей являются *зависимости,* которые в свою очередь, классифицируются на *прямые, косвенные* и *выбираемые.* Более половины *компонентов* в среднем имеют зависимости с пятью другими *компонентами*. Самих же *компонентов*, нормированных в стандарте, несколько сотен. И это отражает мировой опыт разработки, оценки и эксплуатации систем защиты ИТ-продуктов. Если в этом имеется необходимость, то при достаточном обосновании возможно введение и новых компонентов с соответствующими связями. Таким образом, на этапе проектирования формируется иерархическая структура системы защиты, составленная из сложных и часто длинных цепочек взаимосвязанных *компонентов*, а также материалы по *спецификациям безопасности*. Основные результаты представляются в виде конструкций: *профилей защиты* и *заданий по безопасности*. Каждая из них отличается степенью общности сформулированных требований по безопасности. В частности, *спецификации безопасности* описывают механизмы защиты конкретного ИТ-продукта (например, конкретной версии операционной системы) и являются отличительной частью *задания по безопасности.* В то время как *профиль защиты* – это независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

Методика составления требований по безопасности в виде ПЗ и ЗБ определена рядом международных стандартов, например 15446 [3]. При этом следует использовать наиболее полные и подробные каталоги таких требований с максимально возможным учетом условий функционирования и ограничений на разработку.

Из трех основных этапов разработки профиля защиты по установлению *среды безопасности, целей безопасности и требований безопасности* только третий этап в определенной степени формализован, поскольку стандарт [1] содержит язык формального описания требований по безопасности. Для успешного выполнения первых двух этапов необходимо иметь базу знаний *угроз, предположений, политик безопасности организации и целей безопасности.* В стандарте 15446 [3] приводится небольшое количество примеров возможных формулировок этих составляющих базы знаний со своими идентификаторами. Скорее всего, нецелесообразно, создавать такую базу, как говорится, на все случаи жизни. Но для конкретных типов ИТ-продуктов знание перечисленных выше сведений, связанных с определением *среды и целей безопасности* для специалистов по защите информации, необходимо. Значительно более полная информация о возможных *угрозах, предположениях, политиках безопасности организации и целях безопасности* содержится в базе знаний CC Profiling Knowledge Base™ (CC PKB) [4]. Эта база знаний отражает принятый в департаменте обороны США подход DoD, но содержит информацию только из открытых источников. Более подробная информация имеется на сайте http://niap.nist.gov.

Формирование профилей защиты представляет собой интеллектуальный процесс, требующий учета больших объемов данных и различных факторов и их взаимосвязей. В [2] дается такая оценка трудоемкости разработки ПЗ – несколько человеко-лет, в том числе и из-за большого объема документов (профиль защиты может содержать 70 и более страниц). В этой же работе ставится задача создания инструментальных средств автоматизации разработки профилей защиты и заданий по безопасности.

В настоящее время такие средства созданы – это программные средства поддержки разработки ПЗ – CC Toolbox [4 -7]. Основная цель разработки инструментальных средств – облегчить внедрение стандарта 15408 – совпадает с целями учебного процесса. В частности, инструментальные средства могут быть использованы при проведении лабораторно-практических занятий, в курсовом и дипломном проектировании. Интегрированный набор программных средств предназначен для помощи потребителям и разработчикам ИТ-продуктов (в роли которых могут выступать студенты) при формулировании профилей защиты и заданий по безопасности. Набор включает три основных компонента: CC Toolbox™ – программа, с которой пользователи работают в интерактивном режиме, CC Profiling Knowledge Base™ – база знаний, которая содержит информацию, необходимую для разработки ПЗ и ЗБ, включая информацию о всех видах связей компонентов, Touring the CC Toolbox™ – дополнительное средство для иллюстративного просмотра примеров, полезное пользователям как при первом знакомстве с CC Toolbox, так и при углубленной работе. Поскольку парадигмы создания ПЗ и ЗБ сходны, то CC Toolbox позволяет их совместную разработку и формирование их финальных отчетов. Набор программных средств позволяет пользователям маневрировать, определяя функциональные требования или требования доверия, выбирая оценочные уровни доверия, задачи защиты, угрозы, политики безопасности и другие компоненты, а также задавая тип отчета. Результатом такой работы являются варианты ПЗ и ЗБ. Получившиеся таким образом формальные результаты не могут считаться окончательными, они должны быть тщательно проанализированы и выверены, что может составлять предмет защиты курсовых и дипломных проектов.

Минимальная конфигурация аппаратных средств ЭВМ для работы с инструментальными средствами, включая базу знаний может быть примерно эквивалентна конфигурации, необходимой для эффективного управления базой данных Microsoft Access средних размеров. Например, конфигурация может быть такой: CPU Pentium II 133 МГц или быстрее, оперативная память 64 Мбайт, жесткий диск 4 Гбайта, монитор 17 дюймовый, чтобы были хорошо видны создаваемые формы.

Создание профиля защиты в среде CC Toolbox™ представляет собой следующий пошаговый процесс.

***Шаг 1.*** **Выбор базы знаний.** Запустить программу CC Toolbox. В окне Predefined Environment List можно выбрать путь DKV5-0-0. Это означает, что будут выбраны *угрозы, предположения и политики безопасности*, из упоминавшейся выше базы знаний CC Profiling Knowledge Base™. Применение это базы знаний носит рекомендательный характер. Она может быть полезной отправной точкой, особенно для начинающих специалистов по защите информации. Если необходимо, эту базу можно расширить своей информацией с помощью кнопки Добавить (Add) во вкладке Контекст (Context). Если выбрать None, то нужно сразу переходить на вкладку Контекст и все исходные данные по *среде безопасности* устанавливать самим. Соответственно, необходимо будет установить и взаимосвязи (Maps) между компонентами *среды безопасности* и *целями безопасности*. Для выполнения следующего шага на верхней панели надо выбрать Protection Profile.

***Шаг 2.*** **Идентификация *среды безопасности*.** На этом шаге определяется среда безопасности с помощью опросника (Promt), который также является частью СС РКВ. Это осуществляется в первой вкладке Опрос по Среде Безопасности (Environment Interview). Метод интервью работает на принципе взаимосвязи определенного вопроса с тем или иным пунктом среды. Три главных категории вопросов – это вопросы по *угрозам, предположениям и политикам безопасности*. Категории вопросов можно выбирать самостоятельно, в противном случае при ответе на вопрос помеченный пункт будет опускаться вниз по иерархии и далее на следующую категорию. Ответы на вопрос могут быть только Да или Нет. Положительный ответ определяет выбор связанных с этим вопросом пунктов *среды безопасности*. Выбор можно посмотреть на вкладке Контекст. Там же в разделе Objectives List будут показаны взаимосвязи определенных пунктов *среды безопасности* с *целями безопасности*.

***Шаг 3.*** **Спецификация *среды безопасности*.** На этом шаге производится формирование содержания *целей безопасности* переходом на вкладку Контекст (Context). Здесь имеются следующие возможности.

Создать (если это необходимо) или выбрать *политики, угрозы и предположения,* которые наиболее полно описывают *среду безопасности* ОО.

Создать (если это необходимо) и выбрать *цели безопасности*, которые связаны с этими *политиками*, *угрозами* и *предположениями*. Выбор *целей безопасности* производится путем «перетаскивания» нужной *цели* из списка Objectives List на панель *целей безопасности*.

Если необходимо добавить *политику, угрозу* или *предположение* в связь с какой-либо *целью*, то так же «перетаскиванием», их можно перенести в эту панель справа, с соответствующим именем Policies, Threats и Assumptions.

Выбранные параметры и взаимосвязи появятся в частях профиля защиты, таких как Среда Безопасности (Security Environment), Цели Безопасности (Security Objectives) и Обоснование (Rationale).

***Шаг 4.*** **Выбор оценочного уровня доверия (ОУД).** На этом шаге работая с вкладкой ОУД (EAL), можно задать ОУД для выбранных условий *среды безопасности*. На экране воспроизводится таблица 6.1 из третьей части стандарта 15408 «Обзор оценочных уровней доверия». Интерфейс позволяет определить ОУД, кликнув на одну из семи кнопок ОУД. Компоненты доверия, относящиеся к выбранному ОУД, будут помечены как включенные в интерфейс Component Interview и связанные с главными *целями безопасности* в интерфейсе Назначение (Allocation). Индикатор CCRA Status может стать желтым (написано CCRA Violation), когда выбраны уровни 5, 6 и 7, а также в случае, когда выделен индивидуальный компонент для ОУД выше 4 или когда помечен расширенный компонент для ОО. Это предупреждение означает, что остальные участники международного соглашения CCRA – Common Criteria Recognition Agreement могут не признать этот ПЗ, но при этом профиль защиты может оставаться корректным в рамках действующих стандартов.

Введение расширения уровня доверия производится во вкладке Назначение (Allocation) путем «перетаскивания» *компонентов доверия* в окна TOE и Non-TOE. В таблице во вкладке ОУД расширенные *компоненты* будут выделены другим цветом. Для TOE – голубой, для Non-TOE – желтый.

***Шаг 5.*** **Идентификация компонентов**. Необходимая для идентификации вкладка имеет имя Опрос по Компонентам (Component Interview). Аналогична Опросу по Среде Безопасности, только вопросы относятся к *функциональным требованиям* и *требованиям доверия* по систематике стандарта 15408. Показываются составляющие выбранного *компонента*, элементы, а также зависимости с други-

ми *компонентами* и взаимосвязи с *целями безопасности*. Этот интерфейс позволяет неопытному специалисту по защите информации ознакомиться с *компонентами*, при этом выбранные *компоненты* не включаются пока в ПЗ. Включение производится во вкладке Назначение (Allocation). Опытный специалист может сразу переходить к этой вкладке. Удобство еще и в том, что новичку легче освоить интерфейс. Во вкладке Назначение можно с помощью флага Filter сделать видимыми только выбранные в процессе интервью *компоненты.*

***Шаг 6.*** **Спецификация компонентов**. На этом шаге, используя вкладку Назначение (Allocation), можно принять решение об использовании для *целей безопасности* определенных конкретных *компонентов*. Для этого для каждого *компонента*, который необходимо использовать, надо определить *цели безопасности*, которые этот *компонент* поддерживает, и к какой области он относится (инструмент самого объекта оценки – TOE или среды ОО, т.е. Non-TOE).

***Шаг 7.*** **Обоснование компонентов**. На этом шаге, используя вкладку (Elaboration), можно увидеть все используемые *компоненты* для ОО и для среды ОО. Здесь можно детализировать эти *компоненты*, добавить свои пометки, написать, почему какие-то зависимости необязательны. Вся информация, которая будет здесь внесена, попадет в ПЗ и в так называемый Отчет Ошибок.

***Шаг 8.*** **Дополнение «сырой» версии отчета ПЗ**. Интерфейс Отчет (Report) позволяет произвести драфт-отчет и редактировать его редактором с ограниченными возможностями. Затем уже после выхода из CC Toolbox вручную отчет профиля защиты выверяется и завершается. К сожалению, CC Toolbox не предназначен для создания цельного и законченного ПЗ в принятом формате, а может лишь уменьшить утомительность процесса его составления. Отчет, выведенный из CC Toolbox, будет показывать только ту информацию, которая была введена с помощью вкладок Context, Allocation, Elaboration и EAL.

***Шаг 9.*** **Генерация отчета**. На этом шаге генерируется отчет с использованием кнопки Показать Отчет (View Report). При первой генерации необходимо ввести в диалоговое окно такие данные, как Название (Title), Авторы (Authors), Версия (Version) и т. д. Обязательные для заполнения поля помечаются звездочкой. Если впоследствии будет необходимо изменить введенные данные, то в главном меню надо выбрать кнопку Add Identification. Сгенерированный отчет имеет формат HTML. Слева от него будет выведено содержание отчета для облегчения навигации по ПЗ. Последующие нажатия кнопки View Report изменяют отчет, только если будут изменены какие-то лежащие в его основе данные. Если по каким-то причинам необходимо создать отчет заново, необходимо в главном меню выбрать Report/Report Update. Возможно редактировать определенные места отчета. Эти места обведены в прямоугольник и выделены зеленым цветом, и их можно изменять, дважды кликнув по ним. Введенные данные имеют голубой цвет.

***Шаг 10.*** **Сохранение отчета.** В главном меню следует выбрать Export Report, и отчет сохранится в формате HTML. После сохранения отчета и вывода его на экран, теряется возможность его модификации. Недостатки отчета можно просмотреть, нажав кнопку View Error Report. CC Toolbox может исправить некоторые ошибки и выдать о них предупреждения.

Изучение CC Toolbox может стать важным инструментом освоения процесса составления ПЗ или ЗБ для будущего специалиста по защите информации. Составление ПЗ/ЗБ вручную – нелегкий труд не одного специалиста, который вряд ли возможно полностью автоматизировать. Для того чтобы составить адекватный, четкий и удовлетворяющий всем требованиям профиль защиты, специалист должен обладать огромным опытом работы, который он приобретает в течение жизни.

Появление автоматизированных систем составления ПЗ типа CC Toolbox позволяет значительно облегчить эту работу. Конечно, сделанный с помощью такой программы профиль не будет являться истиной в последней инстанции, и все-таки CC Toolbox может стать огромным подспорьем как для опытных пользователей, так и для новичков, в том числе и студентов. Обучение работе с данным программным пакетом может значительно улучшить понимание и увеличить заинтересованность студентов в стандарте 15408, поскольку позволит напрямую поработать с определением *среды, целей* и *требований безопасности* для конкретных ОО. CC Toolbox удобен тем, что содержит варианты взаимосвязей между *средой безопасности, целями безопасности* и *требованиями безопасности*, а также зависимости между *компонентами.*

Все эти связи автоматически определяются с помощью встроенного механизма, называемого Mapping. Кроме того, вместе с комплектом CC Toolbox поставляется база данных CC Profiling Knowledge Base для *среды безопасности*, что также позволяет не углубляться в процесс создания своих *политик, угроз* и *предположений безопасности*, а принять уже готовые и выбрать из них наиболее подходящие. К тому же, имеется возможность добавить к уже имеющимся свои *политики, угрозы* и *предположения*, что расширяет инструментарий и позволяет варьировать на основе заданной базы знаний. Это также может пригодиться при расширении вариантов заданий для студентов.

Ниже приведены примеры лабораторно-практических работ, которые помогут приобрести навыки работы с CC Toolbox и освоить процесс составления ПЗ. Перед тем, как выполнять эти лабораторные работы, студенты должны ознакомиться со стандартом 15408. Вполне допустимо работать в бригаде по 2-3 человека.

***Лабораторная работа №1.*** **Изучение программного пакета CC Toolbox.** Целью работы является знакомство и приобретение навыков работы с CC Toolbox. Необходимо дать возможность самостоятельно изучить программу и поработать со связями между *средой безопасности, целями безопасности и* компонентами. Студенты должны сформировать через CC Toolbox один из известных утвержденных профилей защиты, например, «Профиль защиты межсетевых экранов трафикового уровня для сред низкого риска» [8]. Итогом проделанной работы должен являться Отчет (Report), который студенты должен уметь самостоятельно редактировать. Результатом данной лабораторной работы должен быть также устный отчет преподавателю, содержащий как основы работы с CC Toolbox, так и некоторые положения «Общих критериев», связанные с составлением конкретных конструкций.

***Лабораторная работа №2.*** **Оценочный уровень доверия**. Цель работы - изучение ОУД. Студенту задается определенный уровень доверия, и он должен повысить или понизить его. Особое внимание необходимо уделить включаемым или исключаемым *компонентам*.

***Лабораторная работа № 3.*** **Функциональные компоненты.** На основе классов функциональных требований, например FDP «Защита данных пользователя», составить пакет требований по вариантам – дискреционная и мандатная модель управления доступом.

Для студентов специальностей 075300 и 075400 изучать процесс разарботки профилей защиты с использованием CC Toolbox целесообразно в курсах "Теория информационной безопасности и методология защиты информации" (3 семестр) и "Комплексные системы защиты информации на предприятии" (9 семестр). Однако значительной трудностью применения программного пакета CC Toolbox в процессе обучения может стать то, что сама программа и все инструкции к ней написаны

на английском языке. Для студентов, изучающих английский язык первые четыре курса, это не должно являться проблемой, но студентам, изучающим другие иностранные языки, будет сложно, вплоть до полного непонимания. Поэтому в настоящее время весьма актуально появление российского аналога данной программы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М.: Изд-во стандартов, 2002. – 527 с.

2. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий. Серия «Безопасность информационных технологий» - М.: МГУЛ, 2001. –278с.

3. ISO/IEC 15446: 2000. Information technology. Security techniques. Guide for the production of protection profiles and security targets. – 156 p.

4. CC Profiling Knowledge Base™. User Guide. Profiling Assumptions, Threats, and Policies. Through Objectives to Requirements. Version 1.0 j, k. – NIAP, May, 2000. – 94 p.

CC Toolbox™. Installation Guide. Version 6.0f, 12 - NIAP, March 2001.

6. CC Toolbox™. Reference Manual. Version 6.0f – NIAP, 2000.

7. CC Toolbox™. User's Manual. Version 6.0f. – NIAP, 2000. (http://niap.nist.gov).

8. Профиль защиты межсетевых экранов трафикового уровня для сред низкого риска.Traffic-Filter Firewall. Protection Profile For Low-Risk Environments. Version 1.1//U.S. Department of Defense – April 1999. – 59 p. (http://www.radium.ncsc.mil/tpep).