УДК 681.3.06: 519.248.681

И.Д. ГОРБЕНКО, д-р. техн. наук, А.В. ПОТИЙ, канд. техн. наук, П.И. Терещенко

КРИТЕРИИ И МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Введение

Обоснованию критериев и созданию методологии оценки информационной безопасности уделено значительное внимание. В настоящее время можно выделить следующие документы, которые внесли серьезный теоретический и практический вклад в решение задач обеспечения информационной безопасности.

1. Критерии оценки защищенности компьютерных систем [1], которые известны как «Оранжевая книга».
2. Европейские критерии оценки безопасности информационных технологий [2]. Данные критерии разработаны с учетом выявленных недостатков и ограничений по применению «Оранжевой книги» и являются гармонизированными по отношению к первым.
3. Канадские критерии оценки безопасности надежных компьютерных систем [3].
4. Федеральные критерии США [4], разработанные по заказу правительства США и направленные на устранение ограничений, неудобств практического применения и недостатков «Оранжевой книги»
5. Международный стандарт ISO/IEC 15408 – «Критерии оценки безопасности информационных технологий» [5-7], или Единые критерии
6. Рабочий проект стандарт CEM-97/017 – «Общая методология оценки безопасности информационных технологий» [8].

Перечисленные нормативные документы, и особенно последние два, вносят существенный вклад в формирование единой международной научно-методологической базы решения проблемы обеспечения информационной безопасности в продуктах и различных информационных технологиях. Анализ этих документов подтверждает тот факт, что для решения задач обеспечения информационной безопасности, наряду с формальными методами моделирования процессов и оценки эффективности функционирования систем необходимо широко использовать методы декомпозиции и структуризации компонентов систем и процессов, неформальные методы оценки эффективности функционирования и принятия решений. Это означает, что аппарат системного анализа необходимо использовать на всех этапах жизненного цикла систем защиты информации.

Целью настоящей статьи есть рассмотрение и обсуждение основных положений Канадских критерии оценки безопасности, Единых критериев и Общей методологии оценки безопасности информационных технологий.

Первая часть статьи посвящена рассмотрению основных положений Канадских критериев, вторая часть – рассмотрению основных положений Федеральных критериев. Третья часть – рассмотрению основных положений стандарта ISO/IEC 15408-1 – Критерии оценки безопасности информационных технологий – Часть 1. Общая модель [5]. В четвертой части обсуждается версия документа CEM–97/017 - 1 – Общая методология оценки безопасности информационных технологий – Часть 1. Введение и общая модель [8].

В пятой части делается попытка оценить эти документы с позиций требований системного подхода к решению проблем и определению дальнейших перспектив развития методов и средств обеспечения информационной безопасности.

1. Канадские критерии оценки безопасности надежных компьютерных систем

В Канадских критериях, как одно из основных, введено такое понятие как гарантия. Она представляет собой степень доверия, с которой в системе реализована политика безопасности. Политика безопасности [3] представляет собой набор правил, регулирующих использование информации, включая ее обработку, хранение, распределение и представление в продукте или системе. Гарантии должны обеспечиваться на всех этапах жизненного цикла информационных продуктов. Каждый оцениваемый продукт должен иметь определенный требуемый уровень гарантий. Уровни гарантий организованы в ие-

рархическую систему и отражают доверие к тому, что политика безопасности продукта или системы реализована корректно.

В канадских критериях требования к гарантиям отделены от требований к функциональности. В них принято жесткое ограничение, что политика безопасности не зависит от функциональных возможностей. Под функциональностью в Канадских критериях понимается группирование услуг безопасности в соответствии с различными задачами безопасности, на решение которых и направлены эти услуги. Для этого используется понятие класса. Внутри каждого класса услуги ранжируются в соответствии с реальной стойкостью, функциональными возможностями и избирательностью действий. При этом реализация каждой из услуг обеспечивает защиту от угроз определенного класса.

При разработке Канадских критериев в основу были положены следующие принципы:

- существенная независимость от политики безопасности;
- обязательное измеримое отличие между уровнями услуг;
- безусловность наличия полезности для заказчика и гибкость документа.

Первый принцип требует, чтобы все аспекты проблем безопасности не были привязаны к какой-либо одной политике безопасности. Второй – возможности измерения разности услуг в части стойкости, функциональных возможностей и избирательности действия. Третий принцип требует, чтобы каждая услуга противостояла конкретным существующим или потенциальным угрозам, которые могут возникнуть при эксплуатации компьютерных систем.

Канадские критерии разрабатывались для технологий, в которых основными являются такие услуги как конфиденциальность, целостность, доступность и наблюдаемость.

Конфиденциальность есть свойство, которое гарантирует, что информация не может быть доступна или раскрыта, для неавторизованных (неуполномоченных на то) лиц, объектов или процессов. По существу, угрозами нарушения конфиденциальности являются такие угрозы, которые могут привести или приводят к несанкционированному ознакомлению с защищаемой информацией.

Целостность представляет свойство, которое обеспечивает условия ведения информационных отношений между субъектами и объектами, при которых информация сохраняется для использования и выполняет основные функции по назначению. Угрозы, относящиеся к несанкционированной модификации информации, являются угрозами нарушения целостности. В результате успешной реализации угрозы нарушения целостности объектам и субъектам наносится или может быть нанесен недопустимый ущерб.

Доступность представляет собой услугу по своевременному и качественному доступу к информации и ресурсам информационных технологий систем санкционированных объектов и субъектов. Как одна из услуг обеспечения безопасности она потенциально подвержена атакам, направленным на то, чтобы сделать ресурсы или информацию, а также услуги информационной системы неудовлетворительными или с пониженным качеством. Такие атаки наносят или могут наносить недопустимый ущерб.

Наблюдаемость (управление доступом) заключается в обеспечении возможности доступа к информации и/или ресурсам (системе) только объектам и субъектам, обладающим соответствующими полномочиями, или отслеживании их действий внутри системы. К угрозам нарушения наблюдаемости относятся угрозы, которые приводят к ухудшению управления и контроля доступом, манипулированию системой, ресурсами или информацией. Для управления доступом используется термин тЭг, который обозначает произвольную информацию, которая используется для управления доступом и связана с пользователями, процессами или объектами. Рассмотрим основные критерии более подробно.

В Канадских критериях каждая из услуг - конфиденциальность, целостность, доступность и наблюдаемость разбивается на уровни. Каждый уровень услуги представляет собой определенный перечень требований к избирательности или качеству защиты от специфического набора угроз. При этом с ростом уровня услуги должна предоставляться более надежная защита от соответствующих угроз. Уровни начинаются с нуля (0) и возрастают до «*n*», причем *n* уникально для каждой услуги.

Канадские критерии позволяют поставщику и заказчику точно определить набор услуг, которые требуются в системе (продукте). Для этого предусмотрена возможность создания функциональных профилей безопасности. Профиль представляет собой объединение (набор) услуг, как правило, совместно с описанием Политики безопасности. Профилю присваивается имя и численный идентификатор. Разработка и использование Канадских критериев было существенным шагом в решении проблем информационной безопасности, однако они имели ряд ограничений, особенно с появлением новых корпоративных и глобальных систем и сетей.

2. Федеральные критерии

Дальнейшее развитие американских, европейских и канадских критериев было заложено в Федеральных критериях [4]. Их особенностью является достаточная общность, совместимость с ранее использованными стандартами, соответствие требованиям. Критерии могут быть использованы для оценки различных информационных технологий (ИТ) - от баз данных до операционных систем. Применение критериев дает конкретные и точные рейтинги. Критерии разрабатывались агентством национальной безопасности США, они могут применяться как к коммерческим так и к военным ИТ. При разработке федеральных критериев за основу были приняты Канадские критерии.

В федеральных критериях, в отличие от канадских критериев, в которых избирательность услуг является «атомарной», компоненты управления доступом представляют собой определенную комбинацию услуг, а именно:

- доверительная конфиденциальность;
- административная конфиденциальность;
- доверительная целостность;
- административная целостность;
- повторное использование объекта.

В эту группу входит также услуга типа «откат», т.е. способность эффективно отменять определенные действия или группу действий.

Основной проблемой, которая возникла при введении Федеральных критериев, является совместимость функциональных услуг. В целом совместимость Канадских и Федеральных критериев составляет порядка 75%. Основным недостатком Федеральных критериев является их объемность. Как подчеркивают пользователи, федеральные критерии оказались очень объемными, а также сложными в применении. Кроме того, Федеральные критерии не предоставляют фиксированного набора уровней гарантий, на соответствие которым могут оцениваться продукты. Вместо набора уровней в Федеральных критериях введены наборы компонентов гарантий оценки и гарантий разработки. Компоненты объединяются и с учетом возможностей анализа взаимных зависимостей, вместе образуют уровни доверия. Более того, этот подход распространяется и на гарантии. Причем гарантии разделены на компоненты гарантий разработки (они касаются исключительно разработчика или поставщика), и компоненты гарантий оценки (например, сертификации). Это достаточно сильное решение и оно взято за основу в Единых критериях.

Для совместимости с Оранжевой книгой в Федеральных критериях введено понятие профиля защиты. Профиль защиты характеризуется тремя наборами компонентов: функциональный, гарантий разработки и гарантий оценки. Профиль защиты только тогда принимается, когда результаты анализа Политики безопасности и профиля защиты непротиворечивы. Освидетельствование состоит из этапов анализа и регистрации. Для создания профиля защиты необходим большой круг квалифицированных специалистов, соответствующие методики и значительные временные затраты на проведение анализа. Решить указанные задачи можно только при фиксации соответствующего набора ограничений, иначе анализ зависимостей может стать совершенно субъективным.

После появления в Федеральных критериях концепции профиля защиты было высказано много сомнений. Высказывались даже мнения, что она будет причиной «поражения» Федеральных критериев. Однако, как мы увидим ниже, эта концепция нашла свое развитие в Единых критериях оценки информационной безопасности.

3. Единые критерии оценки безопасности информационных технологий, ISO/IEC 15408

Стандарт ISO/IEC 15408 прошел достаточно долгий эволюционный путь развития. При его разработке учитывались положения таких документов как «Критерии оценки надежных компьютерных систем» (TCSEC) [1] (США, 1985), «Критерии оценки безопасности информационных технологий» (ITSEC) [2] (Европейская комиссия, 1991), «Канадские критерии оценки безопасности надежных компьютерных продуктов» (CTCPCEC) [3] (Канада, 1993), «Федеральные критерии безопасности информационных технологий» (FC) [4] (США, 1993). Также учитывались положения международных стандартов в области защиты информации, например ISO-7498-2, и ряда других документов [9]. Единые критерии (ЕК) информационной безопасности хорошо согласованы с существующими стандартами,

развивают и совершенствуют их путем внедрения новых компонент обеспечения безопасности для перекрытия большего числа угроз, в том числе в новых информационных технологиях.

В разработке стандарта принимали участие специалисты различных организаций, а именно Communications Security Establishment (Канада), Bundesamt fur Sicherheit in der Informationstechnik (BSI, Германия), German Information Security Agency (GISA), Service Central de la Securite des Systemes d'Information (SCSSI, Франция), Centre de Certification de la Securite des Technologies de l'Information (Франция), Netherlands National Communications Security Agency (Нидерланды), Communicstions-Electronics Security Group (Великобритания), National Security Agency, National Institute of Standards and Technology (США).

По мнению специалистов [10] ISO/IEC 15408 или как исторически сложилось называть этот документ Единые критерии, вобрал в себя все лучшее на сегодняшний день в области решения проблемы защиты информации и по всем показателям (актуальность, гибкость, реализуемость, универсальность, гарантированность) существенно превосходит все выше перечисленные документы. На данный момент этот документ представляет собой великолепный образец применения методов системного подхода к решению проблемы защиты информации и полностью соответствует принципу комплексной стандартизации в области обеспечения безопасности информации. Положительной чертой стандарта является то, что он разработан с учетом и использованием новейших достижений в области безопасности информационных технологий 90-х годов. В нем в полной мере учтены результаты анализа и применения всех существующих стандартов.

Стандарт определяет общие критерии, которые используются в качестве основы для оценки свойств безопасности информационных продуктов и технологий. При этом под продуктами и системами информационных технологий понимаются совокупности аппаратных и/или программных средств, которые представляют собой поставляемое конечному потребителю готовое к использованию средство обработки информации [10].

Единые критерии направлены на обеспечение сравнимости результатов оценок, полученных различными экспертами, путем введения общего множества требований к функциям безопасности продуктов и систем информационных технологий, а также к показателям этих функций. Используя стандарт, можно решить задачу выбора соответствующих требований и показателей безопасности информационных технологий.

Основными потенциальными угрозами безопасности и типовыми задачами защиты от них в Единых критериях приняты:

- защита от угроз целостности (несанкционированного изменения) информации;
- защита от угроз конфиденциальности (несанкционированного получения) информации по всем возможным каналам утечки;
- защита от угроз доступности информации, в смысле несанкционированного или случайного ограничения доступа к ресурсам и информации системы;
- защита от угроз аудиту системы (декларируется 12 потенциальных угроз).

Стандарт также может быть использован для решения других вопросов обеспечения безопасности информации, при этом особое внимание уделяется угрозам информации, порождаемым действиями человека.

Одним из основных понятий Единых критериев есть понятие компонента информационной безопасности. Компонентами Единых критериев являются:

- продукт информационных технологий;
- политика безопасности;
- потенциальные угрозы безопасности;
- типовые задачи защиты;
- профиль защиты;
- проект защиты;
- функциональные требования к средствам защиты;
- требования адекватности средств защиты;
- стандартные уровни адекватности средств защиты.

Политика безопасности определена как совокупность законов, норм и правил, регламентирующих порядок обработки, защиты и распространения информации.

Задача защиты – потребность потребителя продуктов информационных технологий в противостоянии множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты – совокупность задач защиты, функциональных требований, требований адекватности и их обоснования. Оформляется в виде специального нормативного документа. Профиль защиты служит руководством для разработчика информационной технологии (ИТ- продукта), на основании которого и предложенных в нем технических рекомендаций разрабатывается проект защиты.

Проект защиты – совокупность задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования. Проект защиты служит руководством для квалификационного анализа и сертификации ИТ- продукта.

Структура этих документов практически совпадает. Основными разделами профиля и проекта защиты являются:

1. Введение, которое содержит информацию, необходимую для идентификации проекта защиты, определения назначения и обзора его содержания. Во введении содержатся идентификатор проекта (профиля) - уникальное имя проекта защиты, используемое для поиска и идентификации проекта защиты и ИТ-продукта, обзор содержания, т.е. аннотация проекта защиты, на основании которой потребитель может определить пригодность ИТ- продукта для применения в своих целях, и заявка на соответствие требованиям CCITSE, в которой описываются все свойства ИТ- продукта, подлежащие квалификационному анализу по CCITSE.

2. Описание ИТ-продукта, которое содержит его краткую характеристику, назначение, принципы работы, методы исследований и др. Эта информация не подлежит анализу и сертификации, но представляется разработчикам и экспертам для пояснения и обоснования безопасности продукта и определения соответствия продукта задачам, решаемым с его использованием.

3. Среда эксплуатации. В данном разделе описываются характеристики среды эксплуатации ИТ-продукта, включая всевозможные угрозы.

4. Задачи защиты, решение которых позволит реализовать Политику безопасности.

5. Требования безопасности проекта защиты. Этот раздел содержит требования безопасности к ИТ-продукту, которыми руководствовался разработчик ИТ-продукта в ходе его разработки. Это позволяет декларировать разработчику факт успешного решения задач защиты. Раздел содержит типовые требования CCITSE и специфические требования для ИТ-продукта и среды его эксплуатации в формате CCITSE и требования адекватности, которые могут содержать уровни адекватности, а они содержат четкое, непротиворечивое описание уровней адекватности с соответствующей детализацией, в формате CCITSE.

6. Общие спецификации ИТ-продукта отражают вопросы реализации требований безопасности с использованием высокоуровневых спецификаций функций защиты, реализующих функциональные требования и требования адекватности CCITSE. Кроме того, в данном разделе содержатся:

– описание функциональных возможностей средств защиты ИТ-продукта, заявленных его разработчиком посредством декларирования требований безопасности. Спецификации должны позволять установить соответствия между требованиями защиты и функциями защиты;

– спецификация уровня адекватности, содержащая заявленный уровень адекватности защиты ИТ-продукта и его соответствие требованиям адекватности посредством представления параметров технологии проектирования и создания ИТ- продукта. Параметры должны быть представлены в формате, позволяющем определить их соответствие стандартным требованиям адекватности по CCITSE.

7. В проекте защиты содержится заявка на соответствие профилю защиты по одному или нескольким уровням. В данном разделе содержатся:

– ссылки на профиль защиты, на который претендует проект безопасности, а также случаи, в которых уровень защиты превосходит требования профиля, но с корректной реализацией всех его требований;

– результаты определения соответствия возможностей ИТ-продукта профилю защиты;

– возможности усовершенствования профиля защиты, в смысле выхода за рамки задач защиты и требований, установленных в профиле защиты.

8. В обосновании показывается, что проект защиты содержит полное и связное множество требований и что реализующий проект ИТ-продукт будет эффективно противостоять угрозам безопасности среды эксплуатации, а общие спецификации функций защиты соответствуют требованиям безопасности. Обоснование также содержит материалы, подтверждающие соответствие реального профиля заявленному и детализируются следующие вопросы:

– показано, что решение задач защиты, заявленных в проекте защиты, позволит эффективно противодействовать угрозам безопасности и реализовать сформулированную под них Политику безопасности;

– обоснование и разъяснение необходимых и достаточных условий обеспечения безопасности, в том числе что: функциональные требования безопасности соответствуют задачам защиты; требования адекватности соответствуют функциональным требованиям и усиливают их; набор всех стандартных и специфических функциональных требований обеспечивает решение задач защиты; все требования безопасности успешно реализованы; все взаимосвязи между требованиями CCITSE учтены либо путем их указания в самих требованиях, либо путем предъявления соответствующих требований к среде эксплуатации; заявленный уровень адекватности может быть подтвержден;

– доказано соответствие функций защиты функциональным требованиям безопасности и задачам защиты. Для этого должно быть показано, что выбранные функции защиты согласуются с заявленными задачами защиты; совокупность выбранных функций защиты обеспечивает эффективное решение совокупности задач защиты; заявленные возможности функций защиты соответствуют действительности.

– осуществляется обоснование уровня адекватности того, что заявленный уровень безопасности соответствует требованиям адекватности;

– обосновывается то, что требования проекта защиты реализуют все требования профиля защиты. Для этого должно быть показано, что все усовершенствования, реализованные в задачах защиты, по сравнению с профилем защиты, корректны, конкретизируют и развивают их; все усовершенствования требований безопасности по сравнению с профилем защиты реализованы корректно, конкретизируют и развивают исходные; все задачи защиты профиля решены и все требования профиля защиты выполнены; дополнительно введенные в проект защиты специальные задачи защиты и требования безопасности не противоречат профилю защиты.

Функциональные требования в Единых критериях разбиты на 9 классов и 76 разделов. Каждый раздел имеет свое уникальное имя и шестибуквенный идентификатор, состоящий из трехбуквенного обозначения раздела. Ранжирование функциональных требований осуществляется по множеству критериев (более 280). Набор этих критериев представляет собой иерархическую структуру в виде неупорядоченного списка сравнимых и несравнимых требований, в котором усиление требований безопасности происходит монотонно от низших уровней к высшим. Структура имеет вид направленного графа, усиление требований безопасности происходит при движении по его ребрам. Набор же принятых функциональных требований обобщает все существующие ранее стандарты информационной безопасности.

В Единых критериях вводится понятие *адекватность* – показатель реально обеспечиваемого уровня безопасности, отражающий степень эффективности и надежности реализованных средств защиты и их соответствия задачам защиты. Требования адекватности средств защиты в Единых критериях структурированы и детально регламентируют все этапы проектирования, создания и эксплуатации ИТ-продукта. Структура требований адекватности аналогична функциональным требованиям.

Всего определено семь стандартизированных уровней адекватности. Каждый из уровней определяет степень соответствия ИТ-продукта каждому требованию адекватности. По существу, названия уровней отражают возможности средств контроля и верификации, применяющихся в процессе разработки, анализа и совершенствования ИТ-продукта. Требования адекватности средств защиты разбиты на 7 классов и 26 требований. Требования адекватности, в смысле контроля и верификации ИТ- продуктов, разбиты на 7 уровней адекватности.

Наконец *Объект оценки* (ОО) в Единых критериях определен как продукт или система информационных технологий, а также связанные с ними управляющая и пользовательская документация, являющиеся объектом процесса оценки безопасности.

Концепция, представленная в стандарте, направлена на удовлетворение интересов трех основных групп – потребителей ОО, разработчиков ОО, и экспертов по оценке безопасности ОО. Необходимо отметить, что применение ЕК создает условия эффективного взаимодействия всех сторон, принимающих участие в разработке, эксплуатации и оценке систем безопасности, в частности и систем информационных технологий вообще. Применение и реализация положения стандартов позволяет различным категориям специалистов решить следующие задачи.

Потребитель, используя общие критерии, решает следующие задачи:

– выбора и формулировки требований по обеспечению безопасности определенного объекта;

– принятия на основе результатов процесса оценки решения о степени удовлетворения оцениваемого продукта или системы предъявленным им требованиям безопасности;

– сравнения различных продуктов и систем выбора адекватного продукта или системы;

– формулировки особых требований к показателям безопасности ОО на основе профиля защиты.

Разработчик, используя общие критерии, решает задачи:

– подготовки и осуществления процесса оценки разрабатываемых продуктов и систем;

– определения полного и непротиворечивого множества требований безопасности, которым должен удовлетворять разрабатываемый продукт или система;

– обоснования адекватности оцениваемого продукта или системы на основе проекта защиты;

– определения степени ответственности за оценку и доказательство необходимости оценки продукта или системы.

Эксперт по оценке решает задачи:

– выработки и принятия решения о степени соответствия (удовлетворения) объекта оценки требованиям безопасности;

– определения мероприятий и комплекса работ, необходимых для осуществления оценки продуктов или систем.

Единые критерии направлены не только на решение задачи оценки свойств объектов оценки, но и на описание этих свойств. Поэтому с использованием этого документа могут решать свои задачи и другие лица, например офицер безопасности, аудиторы, администраторы оценки, лица ответственные за аккредитацию и сертификацию продуктов и систем, и другие.

Для обеспечения наибольшей степени соответствия между результатами процессов оценивания, осуществляемых различными экспертами, очень важно, чтобы оценка осуществлялась на единой методологической основе с использованием надежных и апробированных схем и методик оценки.

Немаловажное значение имеет организация постоянного управления и контроля за процессом оценки. Именно здесь особенно четко проявляется регулятивная роль нормативных документов, которая направлена на обеспечение однозначности и взаимного соответствия результатов оценки.

На рисунке 1 представлена диаграмма, характеризующая взаимосвязь процесса оценки, критериев и методологии оценки безопасности.

Здесь под ***методологией оценки*** понимают систему принципов, процедур и процессов, применяемых при оценке безопасности информационных технологий.

Под ***схемой оценки*** понимают совокупность нормативных и руководящих документов, обеспечивающих интерпретацию и применение критериев оценки администратором оценки в рамках определенной общности экспертов.

Администратор оценки есть лицо, уполномоченное и ответственное за реализацию общих критериев в рамках отдельной общности экспертов через схему оценки и следовательно через совокупность стандартов и других нормативных документов, а также ответственное за организацию и контроль качества оценки.

Из приведенного следует, что разработка общих вопросов относительно критериев и методологии оценки безопасности информационных технологий является прерогативой международной сообщности, в то время как разработка конкретных схем и методик оценки осуществляется национальными и другими организациями конкретного государства. Эти схемы оценки, очевидно, должны определять взаимосвязанную совокупность методов и методик оценки показателей и свойств продуктов/систем, которые разрабатываются, с одной стороны, на единой методологической основе, что обеспечивает повторяемость и объективность результатов оценки, а с другой, на основе правовых и нормативных документов отдельного государства или организации.

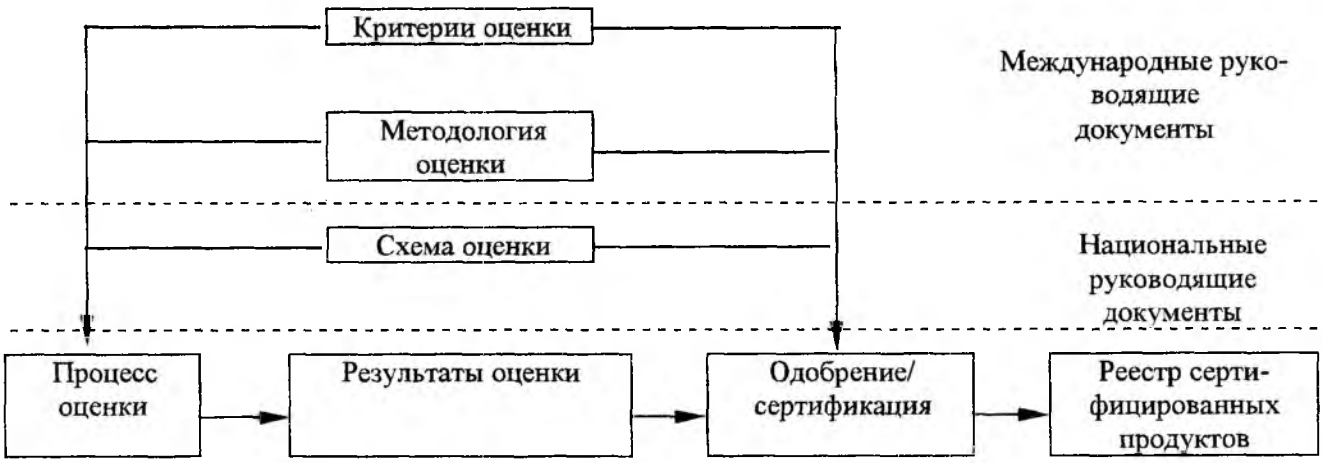

Рис. 1

Необходимо отметить еще одну особенность, а именно наличие такого этапа как одобрение и сертификацию результатов оценки. Дело в том, что большинство критериев оценки требуют привлечения знаний множества экспертов и скорее всего многие показатели могут быть определены только или с применением неформальных методов, в частности методов экспертного опроса. В этом случае неизбежно возникает задача определения степени согласованности мнений экспертов и обеспечения требуемой степени непротиворечивости мнений. Ясно, что не совсем просто обеспечить постоянство и согласованность уровня базовых знаний экспертов. Процесс сертификации в данном случае выступает как средство обеспечения большей степени согласованности мнений и принятых решений экспертов при применении ЕК с последующим оформлением сертификата.

Общий подход критериев безопасности можно охарактеризовать следующим образом.

Уверенность и доказательство безопасности продукта или системы можно получить в процессе разработки, оценки или эксплуатации системы (рис. 2). Разработчики стандарта опираются на общую модель поэтапной разработки системы – от формирования целей функционирования и ограничений к системе до её реального воплощения в "металле". Однако, как показали исследования [11], основной причиной неудач в защите информации является то, что вопросы ЗИ рассматривались без органической связи с проектированием и технологией функционирования систем. Стандарт рекомендует формировать требования по безопасности одновременно и во взаимосвязи с формированием технических, эксплуатационных, экономических и других требований к разрабатываемой системе. На основе сформулированных требований безопасности разрабатываются профиль и проект защиты. В ходе разработки объекта ранее сформулированные требования могут быть уточнены и модифицированы.

Процесс оценки объекта может выполняться либо параллельно с разработкой, либо после неё. Ожидаемыми результатами оценки являются, во-первых, подтверждение того, что объект оценки удовлетворяет требованием безопасности, изложенным в проекте защиты и, во-вторых, обеспечение степени уверенности в полученной оценке, через выполнение требований адекватности и установление уровня адекватности оценки. Полученные результаты оформляются соответствующими документами и могут быть использованы разработчиками и потребителями для решения своих задач.

Необходимо отметить, что процесс оценки оказывает сильное позитивное влияние на формирование требований, процессы разработки и оценки, а также на эксплуатацию продукта. Оценка объекта, прежде всего, предназначена для выявления ошибок и уязвимых мест в системе, которые в дальнейшем будут устранены разработчиком и, тем самым, будет уменьшена вероятность нарушения безопасности в ходе эксплуатации объекта. С другой стороны, разработчик, зная концептуально-методологический подход оценки безопасности, уже на этапе формирования требований и проектирования будет проявлять большое внимание на решение вопросов безопасности.

Этап эксплуатации, с точки зрения обеспечения защиты информации, интересен тем, что здесь могут быть выявлены новые неизвестные ошибки, которые могут появиться при изменении условий эксплуатации. Кроме того, могут появиться и новые угрозы безопасности. Данные ошибки будут учтены разработчиками и экспертами в ходе усовершенствования и модификации объекта.

Стандарт различает три типа оценки: оценку профиля защиты, оценку проекта защиты и оценку объекта защиты.

Целью оценки профиля защиты является подтверждение того, что профиль защиты является полным, согласованным, а также технически применимым и пригодным к использованию в качестве требований для оцениваемого объекта.

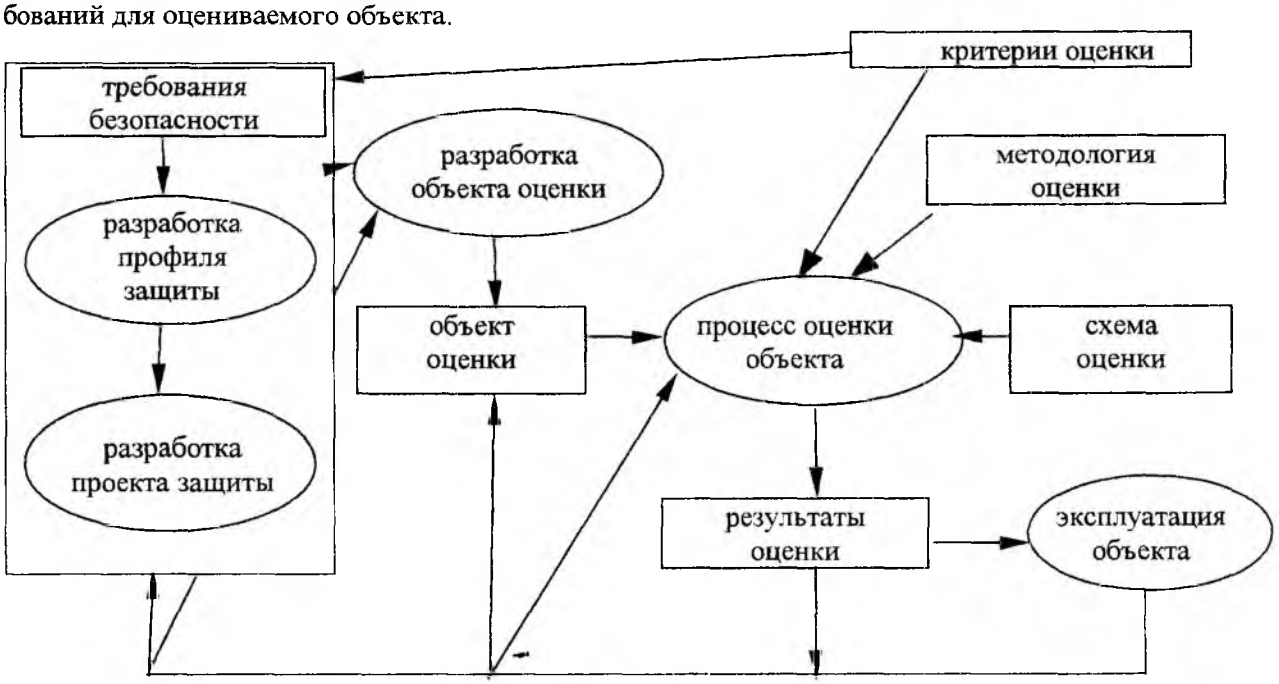

Рис. 2

Целью оценки проекта защиты является: во-первых, подтверждение того, что проект защиты полный, согласованный, а также технически применимый и пригодный для использования его в качестве основы для оценки соответствующего объекта оценки; во-вторых, для подтверждения того, что проект защиты удовлетворяет требованиям профиля защиты (при необходимости).

Целью оценки объекта является подтверждение того, что объект оценки удовлетворяет требованиям безопасности, содержащимся в проекте защиты.

На рисунке 3 представлены возможные варианты использования результатов оценки, которые предлагает стандарт.

Как видно из рисунка, разработка и оценка объекта требует наличия требований безопасности и может опираться на каталоги профилей защиты и продуктов, которые уже были ранее оценены. В зависимости от того, что являлось объектом оценки (продукт или система), результаты оценки используются для формирования каталога продуктов, либо для аккредитации системы. В последнем случае результаты оценки должны быть доступны лицу или организации, ответственным за аккредитацию систем. Важным здесь является то, что предполагается создание международного реестра (каталога) оцененных профилей защиты, проектов защиты, продуктов и сертификатов, которые будут доступны разработчикам и могут быть использованы или при разработке новых, или при усовершенствовании старых систем. Это приведет к значительной экономии материальных, финансовых и людских ресурсов при разработке новых систем, что является одной из основных задач международной стандартизации.

Рис. 3

4. Общая методология оценки безопасности информационных технологий

Общие критерии оценки безопасности могут и должны применяться на единой методологической основе. Поэтому вполне естественно, что сразу же после появления версии ISO/IEC 15408 начались работы по разработке нормативного документа, определяющего общую методологию оценки безопасности информационных технологий. На данный момент таким документом является CEM-97/017 – "Общая методология оценки безопасности информационных технологий" [8].

Данный нормативный документ предназначен в основном для экспертов по оценке безопасности систем, а также необходим разработчикам, заказчикам оценки и контролирующим органам. Именно эти стороны определены в качестве пользователей общей методологии (ОМ).

С точки зрения разработчика профиля защиты применение ОМ позволяет выполнить независимую и последовательную оценку и обоснование профиля защиты.

Для разработчика объекта оценки важно то, что применения ОМ позволит:

– независимо обосновать и проверить задокументированные в профиле и проекте защиты показатели безопасности;

– убедить потребителя в том, что объект оценки обладает заявленными показателями безопасности;

– более эффективно использовать при построении систем безопасности результатов, полученных при оценке других продуктов и систем;

– уменьшить затраты временных и материальных ресурсов на осуществление процесса оценки безопасности.

Заказчик оценки – это организация, которая дает поручение на осуществление оценки безопасности объекта. В роли заказчика могут выступать разработчик, системный интегратор, потребитель (пользователи, аудиторы, системный администратор и т.д.). Здесь применение ОМ позволяет задокументировать, независимо и последовательно обосновать и проверить показатели безопасности и обеспечить возможность сравнения и обоснованного выбора различных объектов оценки.

Для экспертов ОМ выступает как руководство по применения критериев оценки безопасности.

Наконец контролирующий орган, т.е. организация, которая гарантирует, что процесс оценки осуществляется в соответствии с критериями оценки, определяет из CEM-97/017 совокупность документов, их форму и содержание, представляемых экспертом по оценки безопасности продукта или системы.

Таким образом, нормативный документ, определяющий общую методологию оценки безопасности информационных технологий, направлен на обеспечение взаимодействия между различными субъектами, заинтересованными в оценке безопасности объекта, упорядочение процесса оценки безопасности продуктов и систем, всемерное и полное информационное обеспечение заинтересованных сторон о ходе выполнения процесса оценки.

Областью применения положений CEM-97/017 являются принципы, процедуры и процессы оценки безопасности, а также мероприятия и комплекс работ, выполняемые в ходе оценки, разработки и контроля оценки безопасности.

Данный документ определяет следующие общие принципы оценки безопасности.

1. Принцип соответствия прилагаемых усилий и заданного уровня адекватности оценки.

Для обеспечения заданного уровня адекватности оценки все стороны должны выполнять свои задачи с той степенью ответственности и строгости, которая соответствует требованиям уровня адекватности.

2. Принцип беспристрастности оценки.

Любая оценка должна быть получена в условиях, исключающих влияние на нее каких-либо личных предубеждений экспертов.

Ни одна из сторон не должна иметь каких-либо предубеждений к объекту оценки или профилю защиты, которые могут быть основаны на ранее известных результатах оценки других профилей защиты или объектов оценки или на давлении одной стороны на другую. С целью уменьшения взаимных влияний сторон и экспертов друг на друга в процессе оценки продуктов и систем организуется надлежащий организационно-технический надзор и применяются схемы, устраняющие какие-либо конфликты между сторонами и экспертами.

3. Принцип объективности оценки.

Результаты оценки должны быть получены в условиях, обеспечивающих минимальное влияние каких-либо индивидуальных субъективных мнений и решений на общую оценку.

Очевидно, что отдельный эксперт не может быть свободен от влияния каких-либо субъективных факторов при принятии решений. Соответствующий организационно-технический надзор над процессом оценки, основанный на хорошо продуманной методологии, организации процесса оценки и интерпретации результатов оценки, должен обеспечит уменьшение влияния личных взглядов и решений отдельных экспертов на общую оценку до приемлемого уровня.

4. Принцип повторяемости и воспроизводимости.

Повтор процесса оценки одного и того же объекта оценки или профиля защиты с одними и теми же требованиями и при одном и том же информационно-техническом обеспечении должны приводить к одним и тем же результатам.

Любое действие должно приводить к одним и тем же результатом независимо от того, кто выполняет это действие. Воспроизводимость направлена на обеспечение соответствия и согласованности результатов оценки, полученных в различное время (например, на различных этапах жизненного цикла системы безопасности), в то время как повторяемость направлена на обеспечение соответствия и согласованности результатов оценки, полученных различными экспертами и, возможно, при условии использования ими различных схем оценки безопасности.

5. Принцип достоверности.

Результаты оценки должны быть полными и технически корректными.

Результат оценки должен показать высокую степень рассудительности принятого решения и тщательности технической экспертизы объекта оценки и профиля защиты. Процесс оценки и полученные результаты должны быть объектами организационно-технического надзора для того, чтобы гарантировать выполнение требований общих критериев, методологии и схем оценки безопасности.

Реализация вышеперечисленных принципов предполагает выполнение следующих условий.

1. Стоимостная эффективность оценки, заключающаяся в том, что ценность результатов оценки должна компенсировать затраты временных, материальных и других ресурсов на проведение оценки. В процессе оценки баланс между ценностью оценки и затратами на ее проведение должен постоянно отслеживаться. Данное условие порождает ограничения на количество показателей, которые входят в оценку безопасности. То есть в оценку могут входить наиболее весомые показатели. Однако тут же возникает вопрос, каким образом определить степень важности того или иного показателя? Скорее всего это тема отдельного обсуждения.

2. Изменение технических и других условий применения систем безопасности, развития информационных технологий, методов оценки и криптоанализа должны отражаться в методологии оценки. Методология оценки должна иметь возможность адаптации к изменяющимся условиям и быть применимой к развивающимся технологиям в области защиты информации. Это позволит обеспечить требуемый уровень эффективности методов оценки и гарантировать их пригодность к оценке профилей защиты и объектов оценки.

3. Обеспечение возможности эффективного использования известных результатов оценки существующих профилей защиты и систем играет важную роль при выполнении последовательной оценки в одних и тех же условиях. Повторная доступность результатов особенно важна в тех случаях, когда оцениваемые объект оценки или профиль защиты являются интегрированными частями других объектов или профилей защиты.

4. И наконец, важно обеспечить, чтобы все стороны в процессе оценки пользовались единой терминологией. На это и направлена разработка нормативных документов и стандартов.

Каждая из сторон, участвующих в процессе оценки на основе общей методологии, несет определенную ответственность за выполнение определенных задач. СЕМ-97/017 определяет такую ответственность в рамках общих принципов и допускает, что схемы оценки могут вводить дополнительные требования к сторонам, с учетом особенностей национального законодательства и положений руководящих документов. Ответственность распределяется следующим образом.

Заказчик оценки несет ответственность за:

– заключение необходимых соглашений для осуществления оценки;

– обеспечение экспертов необходимыми материально-техническими и информационными ресурсами для осуществления оценки.

Разработчик несет ответственность за:

– поддержку процесса оценки;

– разработку и сохранение необходимых ресурсов для оценки.

Эксперт по оценке несет ответственность за:

– получение необходимых ресурсов для оценки (документация, профиль и проект защиты, копия (образец) объекта оценки);

– выполнение работ по оценке в соответствии с требованиями общих критериев;

– формирование запроса и получение дополнительной помощи или материалов для оценки (обучение у разработчика, интерпретация требований контролирующего органа);

– обеспечение условий для организации надзора за процессом оценки;

– документирование и утверждение промежуточных и окончательного решений;

– создание условий, при которых гарантируется согласованность процесса оценки с общими принципами и требованиями соответствующих схем оценки.

Контролирующий орган несет ответственность за:

– мониторинг процесса оценки;

– получение и рассмотрение материалов контроля;

– создание условий, гарантирующих согласованность процесса оценки с общими принципами положениями СЕМ;

– поддержку процесса оценки через разработку и внедрение схем, методик и правил интерпретации результатов, а так же различного рода руководящих документов;

– одобрение или опровержение окончательных решений;

– документирование и юридическое закрепление решений администратора оценки.

Методология оценки предполагает, что оценка будет осуществляться в три этапа: предварительный, основной и заключительный.

На предварительном этапе основными действующими лицами являются заказчик оценки и эксперт Заказчик информирует все стороны относительно необходимости оценки профиля защиты или объекта оценки, обеспечивает эксперта необходимой документацией, материалами по профилю защиты и объекту оценки. Задачей эксперта является определение возможности успешного осуществления оценки на основе полученных материалов и по необходимости затребовать дополнительного обеспечения заказчика или разработчика.

Итогом подготовительного этапа является заключение между заказчиком и экспертом соглашения на осуществление работ по оценке объекта или профиля защиты.

Непосредственная оценка осуществляется на основном этапе. В процессе оценки эксперт рассматривает представленные ему материалы, профиль защиты или объект оценки. Эксперт может составлять ряд обзорных отчетов в которых могут содержаться его требования по предоставлению пояснений относительно применения требований контролирующего органа, запросы на дополнительную информацию по профилю защиты или объекту оценки у заказчика или разработчика, выявленные слабости недостатки и другая информация о ходе оценки.

Контролирующий орган осуществляет непрерывный мониторинг процесса оценки в соответствии со схемой оценки.

Результатом основного этапа является разработка и предоставление экспертом Технического отчета оценки (ТОО), который содержит обоснование принятого экспертом решения.

На заключительном этапе осуществляется рассмотрение и анализ ТОО всеми сторонами. Основным действующим лицом на этом этапе выступает контролирующий орган. Он осуществляет всесторонний анализ ТОО на предмет его соответствия общим критериям общей методологии и требования

схем оценки безопасности. Контролирующий орган принимает решение о согласии или несогласии с решением, изложенном в ТОО и готовит Итоговый отчет оценки на основе ТОО. При этом все стороны, вовлекаемые в процесс оценки, имеют право ознакомление с материалами Итогового отчета и могут требовать соответствующих пояснений.

5. Перспективы практической реализации положений ISO/IEC 15408 и CEM – 97/017

Выше рассматривались задачи, на решение которых направлено использование положений рассматриваемых нормативных документов. Эти задачи сформулированы и изложены в самих этих документах. Важно оценить перспективы применения положений документов на практике. При этом важно сделать эту оценку с позиций системного подхода к решению проблемы защиты информации.

В работе [11] изложены три основных задачи, решаемые в рамках системного подхода к решению сложной проблемы. В контексте рассмотренных документов эти принципы можно сформулировать следующим образом:

1) системный анализ сущности проблемы защиты информации;

2) разработка и обоснование полной и непротиворечивой концепции и методологии решения проблемы защиты информации, в рамках которой решение задачи защиты продукта или системы в конкретных условиях определяется в виде частного случая – разработкой профиля и проекта защиты;

3) системное использование методов и механизмов защиты информации при решении задачи синтеза (проектирования, разработки) безопасных продуктов и систем информационных технологий.

Видно, что предложенные документы направлены на решение первых двух задач. В стандарте ISO/IEC 15408 осуществлена полная декомпозиция проблемы защиты информации. Механизмы профиля и проекты защиты отражают суть концепции решения проблемы защиты информации.

Однако в документах нет методологии решения третьей задачи – задачи синтеза систем. Функциональные требования и требования адекватности, как и методология оценки безопасности, направлены в первую очередь на решение задачи оценки безопасности продукта или системы. Хотя их применение оказывает определенное регламентирующее влияние на проектирование, разработку и эксплуатацию систем. Здесь необходимо решать задачу установления соответствия целям защиты (которые выражаются через требования) и множеством средств и механизмов, которые имеются в нашем распоряжении для реализации этих целей.

Стандарт ISO/IEC 15408 предполагает создание электронного каталога профилей защиты, прошедших оценку и сертификацию, что позволит разработчикам использовать известные профили защиты при разработке новых продуктов и систем. Однако нужно сказать, что профиль (проект) защиты является не чем иным как сертифицированным и обоснованным решением задачи защиты информации в конкретных условиях эксплуатации продукта. Таким образом, можно сделать вывод, что последовательное применение положений стандарта при решении практических задач создает базу для разработки и создания экспертных систем в области защиты информации. А это в свою очередь позволяет перейти к разработке автоматизированных средств поддержки принятия решений в данной области и средств автоматизированного проектирования систем защиты информации. Одним из направлений использования результатов оценки разработанных профилей защиты, которые могут рассматриваться как управляющее воздействие на систёму при возникновении определенных угроз безопасности (ситуации), является применение модели ситуационного управления системами защиты информации. Это в перспективе может привести к созданию самомодифицирующихся систем защиты информации, которые с помощью администратора или автоматически будут модифицировать свою структуру и функции в зависимости от складывающихся условий эксплуатации и угроз.

Другим важным результатом разработки данных документов является отражение системности подхода к решению проблемы защиты информации и создание единой методологической базы решения задач защиты информации. Важно то, что не только схемы оценки безопасности должны разрабатываться в рамках единой методологии, но процессы проектирования и разработки новых продуктов и систем должны осуществляться с учетом норм и положений данных документов. Это является хорошим подспорьем и для отечественных специалистов.

Заключение

На наш взгляд, рассмотрение документов требует внимательного изучения и внедрения в отечественную практику разработки и оценки соответствующих изделий, продуктов и систем. Поскольку эти документы являются продуктом работы ряда организации и объектом международной стандартизации, то им можно доверять. Тем более Украина также является членом группы P Международной организации по стандартизации и участвует в голосовании решения по принятию этих документов.

Одной из особенностей стандартизации в области защиты информации является интернационализация стандартизации. Гиперскоростное развитие информационных технологий, создание всемирного единого информационного пространства, интеграция в это пространство нашего государства являются непреложными фактами. Создание адекватных и надежных систем защиты информации в таких условиях не под силу отдельному государству. И по этой причине необходимо осваивать и применять данный методологический аппарат в отечественной практике, адаптировать или разработать новые нормативные документы, которые будут учитывать положения международных стандартов.

Разработка отечественных уникальных схем оценки безопасности в рамках общих критериев и методологии позволит нам не только оценить собственные продукты и системы, но активно участвовать в сертификации изделий, продуктов и систем зарубежного производства, тем самым защитить свой рынок от низкопробной продукции.

На наш взгляд, реализация и применение норм и положений этих документов в отечественной и мировой практике даст новый толчок в развитии теории и методов защиты информации.

Список литературы: **1.** *Trusted* Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985. **2.** *Information* Tecnhology Security Evaluation Criteria, v. 1.2. –Office for Official ublications of the European Communities, 1991. **3.** *Canadian* Tusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993. **4.** *Federal* Criteria for Information Technology security. – NIST, NSA, US Government, 1993. **5.** *ISO/IEC 15408-1:1999* – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. **6.** *ISO/IEC 15408-2:1999* – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. **7.** *ISO/IEC 15408-3:1999* – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. **8.** *CEM-97/017.* Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model. **9.** *ISO/IEC 7498-2:1989.* – Information processing systems – Open Sistems Interconnection – Basic Reference Model – Part 2: Security Architecture. **10.** *Зегжда Д.П., Ивашко А.М.* Как построить защищенную информационную систему. – СПб: Мир и семья – 95, 1997. – 312 с. **11.** *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. Кн.1. – М.:Энергоатомиздат, 1994. – 400 с.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 21.03.2000