УДК 638.235.231

Ю.В. Щербина, К.Б. Айвазова

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ СРАВНИМОСТИ РЕЗУЛЬТАТОВ ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Ю.В. Щербина, К.Б. Айвазова

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПОРІВНЯЛЬНОСТІ РЕЗУЛЬТАТІВ ОЦІНКИ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ

Ju.V. Shherbina, K.B. Ajvazova

REGULATORY SUPPORT COMPARABLE RESULTS SECURITY ASSESSMENT AUTOMATED SYSTEMS

Аннотация. *Показано, что при одновременном влиянии в канале связи разного рода помех и искажений прием полезного сигнала будет неоптимальным и, следовательно, вероятность ошибки будет возрастать при приеме дискретных сигналов. Для уменьшения вероятности ошибки предложена новая процедура передачи сигнала (как функции) с учетом помех и искажений в канале, где процесс представлен в виде математической задачи.*

Ключевые слова: *защищенность автоматизированных систем, анализ рисков, параметры угроз.*

Анотація. *Определены основные проблемы, связанные с нормативно-правовым обеспечением процедур, которые позволяют выполнять анализ рисков в современных автоматизированных системах. Изложены предложения по дальнейшему совершенствованию отечественной нормативной базы в области защиты информации в компьютерных системах.*

Ключові слова: *захищеність автоматизованих систем, аналіз ризиків, параметри загроз.*

Annotation. *Major problems connected with the normative legitimate provision of the procedures that give possibility to use the risks analysis in modern automated system have been determined. The problems concerning the optimization of the national base in the field of data security in the computer systems have been presented.*

Keywords: *automated systems security, risk analysis, the parameters of threats.*

Постановка проблемы и её связь проблемы с важными научными и практическими заданиями. Тенденция перехода на безбумажные технологии с использованием автоматизированного документооборота и развитие открытых глобальных телекоммуникационных систем, требует принятия соответствующих мер по защите происходящих в них информационных процессов. Реализация таких мер предполагает точную оценку действующих в среде эксплуатации автоматизированных систем (АС) угроз и уровня защищенности их информационных ресурсов. Сложность формализации происходящих в АС процессов, к сожалению, не позволяет исключить субъективный фактор при использовании для этих целей различных экспертных систем. Тем не менее, эта задача должна решаться таким образом, чтобы владельцы и пользователи автоматизированных систем были гарантированы от недостоверных оценок защищенности. По этой причине в 90-е годы прошлого столетия в развитых странах мира были разработаны и введены в действие нормативные документы, регламентирующие действия разработчиков и оценщиков защищенных информационных технологий (ИТ) и соз-

даваемых на их основе автоматизированных систем. Обеспечение достоверности оценки защищенности информационных объектов является актуальной задачей и в настоящее время, в виду постоянного развития и совершенствования информационно-телекоммуникационных систем.

Анализ последних исследований и публикаций, в которых положено начало решения проблемы. Вопрос о необходимости законодательного обеспечения деятельности, связанной с защитой информации, встал практически сразу же, как только для ее обработки начали применять распределенные вычислительные системы. Значительная работа в этой области проводилась и в нашей стране. В 1999 был принят документ под названием «Критерии оценки защищенности в компьютерных системах от несанкционированного доступа» [1, 2], регулирующий деятельность по защите информации в компьютерных системах, а также пакет сопутствующих ему нормативных документов [3-6]. Компьютерная безопасность за прошедшее время превратилась самостоятельную область знаний, а быстрые темпы развития открытых телекоммуникационных систем вынудили наиболее развитые страны Западной Европы и Америки объединить свои усилия с целью обобщения накопленного в этой сфере опыта. Они разработали ряд международных документов, позволяющих осуществлять достоверную оценку защищенности современных АС [12-14].

Принятие международных нормативных документов в области защиты информации, ставит перед отечественными разработчиками задачу, суть которой состоит в приведении национальной нормативно-правовой базы в соответствие с их требованиями. Другой, не менее важной задачей является разработка соответствующих методик и инструментальных средств оценки защищенности АС [15, 16]. Поэтому ***целью статьи*** является определение имеющихся расхождений в направлениях развития и мировой и отечественной нормативно-правовой базы в области защиты информации в автоматизированных системах и путей их устранения.

Изложение основного материала. Несоответствие некоторых положений нормативно-правовых документов Украины, регламентирующих решение вопросов связанных с информационной безопасностью современным требованиям, не позволяют отечественным разработчикам использовать результаты оценок информационных технологий получаемых специалистами других стран. Более того, за время, прошедшее с момента приема документа НД ТЗИ 2.5-004-99, архитектура современных распределенных вычислительных систем и сетей, значительно изменились в сторону их усложнения. За это время, Международная Организация по Стандартизации ISO приняла целый ряд документов, аналогичного содержания, которые аккумулируют накопленный в этой сфере опыт.

Наиболее значимым из этих документов является международный стандарт ISO 15408 [7-9]. В научно-технической литературе он также упоминается под названием «Общих критериев» (ОК) или «Единых критериев» (ЕК). В нем наиболее полно представлены критерии оценки механизмов безопасности программно-технического уровня. Использование этого документа позволяет оценить уровень защищенности автоматизированной системы с точки зрения полноты реализованных в ней функций безопасности, а также надежности их реализации. Наряду с Едиными критериями был опубликован ряд других, дополняющих их документов. К их числу относятся «Общая Методика Оценки Безопасности ИТ», «Руководство по Проведению Сертификации и Аккредитации Компьютерной безопасности», а также «Профили защиты для межсетевых экранов и коммерческих систем».

В настоящее время можно говорить о создании единого языка для формулирования утверждений относительно безопасности автоматизированных систем (требований, угроз и целей защиты), а также частичной формализации этой предметной области. Применение содержащихся в этих документах концепций позволяет повысить эффективность проводимых оценок и качество получаемых результатов. Кроме того, это позволяет использовать, накопленный мировым сообществом опыт в этой области. В частности, теперь можно сравнивать между собой результаты сертификационных испытаний, полученных в рамках надежной схемы. Единые критерии поддерживают совместимость с уже существующими аналогичны-

ми документами, и это позволяет разработчикам АС использовать собственный, накопленный в работе, опыт.

Задачи, решаемые в рамках Единых критериев, на территории Украины регламентируются документом НД ТЗИ 2.5-004-99. Также как и Единые критерии, этот документ определяет функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements). Однако толкование аналогичных терминов в этих документов не всегда совпадает. И, самое главное, степень детализации требований к функциям безопасности и требований к адекватности их реализации в этих документах заметно отличается. Так, например НД ТЗИ 2.5-004-99 содержит только четыре группы требований к услугам безопасности, обеспечивающих защиту от угроз определенного типа. Эти группы разделены по признаку последствий от реализации угроз: потере конфиденциальности, целостности, доступности или наблюдаемости информации. Само число предлагаемых функциональных услуг защиты в каждой группе невелико (меньше десяти). Требования к безопасности, обеспечиваемые каждой услугой, описаны в неформальном виде, а способ их реализации не оговаривается.

Что касается Единых критериев, то в их состав входит одиннадцать функциональных классов, определяющих функции защиты. При этом каждый класс включает ряд семейств, которые, в свою очередь, делятся на компоненты, а компоненты на элементы. Требования в пределах каждого семейства отличаются акцентами или строгостью. Само содержание классов заметно отличается от предлагаемой НД ТЗИ 2.5-004-99 классификации. В частности, функции защиты в них разделены в соответствии с иными классификационными признаками. К ним относятся: «аудит», «криптографическая поддержка», «связь», «защита пользователя», «идентификация и аутентификация», «управление безопасностью», «приватность», «защита функций безопасности объекта оценки», «использование ресурсов», «доступ к объекту» и «доверенный канал/маршрут». Это отличие явно в пользу Единых критериев. Оно обусловлено некоторыми отличиями в понимании термина «угроза». В НД ТЗИ 2.5-004-99 на первое место ставится защищаемый информационный объект и последствия от реализации угрозы, а именно потери одного из свойств информации. В Единых критериях во главу угла ставятся уязвимые места в системе защиты и способы ее преодоления. Этим и объясняется разнообразие классов, на которые разделены предлагаемые функциональные требования безопасности и большее их количество. Фактически этот документ предлагает определять слабые места в защите, а затем выяснять какие ресурсы системы это подвергает опасности и в какой степени. Очевидно, такая модель боле эффективна, поскольку результирующий опыт в этой сфере базируется на статистическом анализе атак. Именно поэтому названия классов и охватывают все аспекты защиты: от ее организации и проверки адекватности угрозам до контроля информационных потоков.

Широкий спектр функциональных услуг защиты, предлагаемый этим документом, позволяет противостоять большему числу угроз и строить более гибкие системы защиты. Требования доверия к безопасности также имеют более широкий спектр. Они разделены на восемь классов, каждый из которых имеет многоуровневую иерархическую структуру. В частности, оценку уровней доверия к реализованной системе безопасности предполагается проводить по таким направлениям как: «управление конфигурацией», «поставка и эксплуатация», «разработка», «поддержка цикла», «тестирование», «оценка уязвимостей» и «поддержка доверия». По своему составу эти направления шире и более глубоко детализируют мероприятия, связанные с определением гарантией защиты.

Наконец, в Единых критериях более глубоко прописаны зависимости между отдельными компонентами функциональных требования безопасности и требований к адекватности их реализации.

Проблема, состоящая в преодолении существующих расхождений достаточно сложна. Существует два пути ее решения. Первый из них состоит в принятии новой редакции документа НД ТЗИ 2.5-004-99, которой отвечал бы современному уровню развития информационных технологий. Второй – состоит в том, чтобы принять в качестве государственного

стандарта Единые критерии, как, например, поступили в России. Сложность положения определяется тем, что в нашей стране, в принципе, еще далеко не все правовые проблемы решены, а разрабатываемые нормативно-правовые акты должны вписываться в национальное законодательство. Так, например, не до конца решены вопросы, связанные с цифровой подписью, с правом интеллектуальной собственности и некоторые другие, от которых прямо или косвенно зависит решение проблем информационной безопасности.

Для создания национального документа, соизмеримого по уровню качества с Едиными критериями, требуются значительные интеллектуальные усилия и опыт. Так, например, для создания второй версии Единых критериев, Международная организация по стандартизации создала специальную рабочую группу № 3 в подкомиссии № 27. В нее вошли представители всех заинтересованных стран и организаций, работающих в этой области, и для выполнения этой работы ее участниками было затрачено много сил и средств. Поэтому, очевидно, вряд ли имеет смысл создавать нечто уникальное и отличное от коллективно созданных критериев.

Работы российских специалистов по адаптации Единых критериев к условиям своей страны были сопряжены, в основном, с преодолением несоответствий ее законодательства международным нормам. Очевидно, что те же проблемы возникнут и в случае если по этому пути пойдут специалисты Украины.

Единые критерии, как и НД ТЗИ 2.5-004-99 основной акцент делает на программно-техническом аспекте реализации защиты информации, а вопросы организации управления безопасностью в нем отражены слабо.

В конце 2000 г. международный институт стандартов ISO на базе британского стандарта BS 7799 разработал и выпустил международный стандарт по управлению безопасностью ISO/IEC 17799 [10]. В нем, вопросы, связанные с оценкой механизмов безопасности организационного уровня отражены наиболее полно, по сравнению с тем, как это сделано в Единых критериях. Применение этого документа в странах Британского содружества иногда наталкивается на трудности из-за его противоречий национальному законодательству некоторых из них. Несмотря на это, сегодня эти документы в адаптированном виде приняты в России и Молдове.

В нашей стране в качестве попытки закрепить на законодательном уровне вопросы управления информационной безопасностью можно рассматривать [11]. К сожалению, этот документ уступает по своему содержанию стандарту ISO/IEC 17799. В нем содержаться самые общие определения и, фактически, отсутствует детальная информация о том, как на практике осуществлять деятельность, связанную с проектированием, эксплуатацией и управлением защищенных автоматизированных систем.

Учитывая, что управленческие процессы являются процессами информационными, под защищенностью АС обычно понимают степень адекватности реализованных в ней механизмов защиты информации, существующим в данной среде функционирования, рискам, связанным с осуществлением угроз безопасности. Защищенность АС достигается, во-первых, перекрытием всех путей осуществления угроз механизмами защиты, во-вторых, соответствием прочности механизмов защиты уровням рисков реализации угроз и, наконец, в третьих, соответствием затрат на реализацию механизмов защиты ущербу, ожидаемому от реализации угроз. Простая и понятная, на первый взгляд, схема обеспечения информационной безопасности, на практике оказывается труднореализуемой. Это определяется тем, что автоматизированные системы чрезвычайно сложны. И эта сложность определяется, во-первых, огромным числом объектов, которые входят в состав АС и являются критическими с точки зрения информационной безопасности. Во-вторых, эти объекты оказывают взаимное влиянием друг на друга, и его надо учитывать при оценке защищенности.

Для создания защищенной АС необходимо обеспечить три основные группы требований. Первая и, очевидно, главная состоит в том, чтобы определить уникальный набор рисков и угроз безопасности, существующий в среде эксплуатации системы. Вторая – состоит в определении правовых норм, в рамках которых функционирует организация, использующая

автоматизированную систему. И третья группа требований заключается в формировании уникального набора принципов, целей и требований, в соответствии с которыми осуществляется обработка информации в автоматизированной системе. С учетом этого, работы по проектированию защищенных систем должны начинаться с анализа рисков.

В принципе, процедура анализа рисков сводится к идентификации защищаемых информационных ресурсов, определению слабых мест в защите (уязвимостей) и угроз. Функциональные требования, сформулированные как в Единых критериях, так и в НД ТЗИ 2.5-004-99, сами по себе уже определяют направления, в соответствии с которыми должен выполняться поиск уязвимостей в системе защиты. Таких направлений много и все они имеют различную природу. Это значит, что для оценки уязвимостей по каждому из направлений потребуется привлечение экспертов, которые обладают знаниями и опытом в этих областях, владеют соответствующим математическим аппаратом и располагают необходимыми инструментальными средствами. Такие средства должны, во-первых, в точности соответствовать требованиям, действующего в стране законодательства и нормативно-правовой базы в области защиты информации, во-вторых, они должны полностью определять алгоритм работы эксперта в каждом направлении. Эксперт должен расходовать свои усилия на анализ среды эксплуатации системы и действующих в ней угроз. Что касается методики и способов определения, качественных и количественных величин определяемых параметров, то они должны быть определены заранее и, возможно, быть рекомендованы к использованию соответствующими государственными структурами. При этом такие методики должны существовать не сами по себе, а быть реализованы в виде технологий. Современный рынок предлагает достаточно большое их количество. К их числу можно отнести такие инструментальные средства как CRAMM, COBRA и им подобные, разработанные на Западе. К сожалению, технологий анализа рисков, отвечающих требованиям отечественной нормативной базе и, в частности НД ТЗИ 2.5-004-99, пока нет. Более того, осуществляются попытки реализовать такую методику в виде нормативного документа.

Объединять технологию анализа рисков и нормативный документ недопустимо. Нормативный документ должен регламентировать деятельность в данной области и определять обязательные этапы и процедуры, подлежащие выполнению. Это позволит находить выход из конфликтных ситуаций между разработчиками и заказчиками защищенных систем в случае их возникновения. Кроме того, это даст возможность сравнивать результаты аудита, выполняемые различными субъектами и, более того, сделает результаты аудита, полученные отечественными экспертами, признаваемыми за рубежом. Что касается технологий, используемых при оценке рисков, то они могут разрабатываться как государственными, так и негосударственными организациями. При этом, главным требованием, которое к ним предъявляется, должно быть их соответствие отечественному законодательству. Такие технологии должны в обязательном порядке, проходить государственную аттестацию.

Выводы. Сложившееся к настоящему времени различие в подходах к защите информации, заложенных в нормативной базе Украины и нормативной базе большинства стран с развитыми информационно-телекоммуникационными системами, тормозит развитие технологий оценки защищенности АС и ограничивает применение тех из них, что апробированы и получили распространение за рубежом. Именно на преодолении сложившихся расхождений и должны быть направлены усилия отечественных специалистов в области информационной безопасности.

Список литературы

1. Волков, С. Л. Вимоги щодо стандартизації захищених інформаційно-вимірювальних систем [Текст] / С. Л. Волков, О. О. Скопа, С. Д. Асабашвілі // Сучасний стан та перспективи розвитку системи технічного регулювання, метрології та якості : VI Всеукр. наук.-практ. конф. молодих учених і студентів, 21-22 травня 2015 р. — ОДАТРЯ, Одеса. — 4 с.

2. НД ТЗИ 1.1-003-99. Терминология в сфере защиты информации в компьютерных системах от несанкционированного доступа [Электронный ресурс] // Портал : Агентство технической защиты информации. — Режим доступа \www/ URL: http://afa.biz.ua/documents/ 31-infobezopasnot/28-how-do-i-install-joomla-15. — Заглавие с экрана, доступ свободный, 10.09.2015.

3. Щербина, Ю. В. Проблемы объективной оценки параметров защищенных автоматизированных систем [Текст] / Ю. В. Щербина, Н. Ф. Казакова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні : IV наук.-техн. конф., 1-3 березня 2006 р. : матер. конф. — К., НТУУ «КПІ». — С. 60-61.

4. НД ТЗИ 1.1-002-99. Общие положения по технической защите информации в компьютерных системах от несанкционированного доступа [Электронный ресурс] // Портал : Агентство технической защиты информации. — Режим доступа \www/ URL: http://afa.biz.ua/ documents/31-infobezopasnot/33-what-is-uncategorised-article. — Заглавие с экрана, доступ свободный, 10.09.2015.

5. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Электронный ресурс] // Портал : ДСТЗІ. — Режим доступу \www/ URL: http://dstszi.kmu.gov.ua/ dstszi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407. — Заголовок з екрану, доступ вільний, 10.09.2015.

6. НД ТЗИ 3.7-001-99. Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе [Электронный ресурс] // Портал : Агентство технической защиты информации. — Режим доступа \www/ URL: http://afa.biz.ua/documents/31-infobezopasnot/12-why-does-joomla-15-use-utf-8-encoding. — Заглавие с экрана, доступ свободный, 10.09.2015.

7. Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. — ISO/IEC 15408-1.1999.

8. Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements. — ISO/IEC 15408-2.1999.

9. Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements — ISO/IEC 15408-3.1999.

10. Information technology — Security techniques — Code of practice for information security management ISO/IEC 17799-2005.

11. НД ТЗИ 1.4-001-2000. Типовое положение про службу защиты информации в автоматизированной системе [Электронный ресурс] // Портал : Агентство технической защиты информации. — Режим доступа \www/ URL: http://www.afa.biz.ua/documents/31-infobezopasnot/25-what-are-the-requirements-to-run-joomla-15. — Заглавие с экрана, доступ свободный, 10.09.2015.

12. Щербина, Ю. В. Проблемы оценки защищенности автоматизированных систем [Текст] / Ю. В. Щербина, А. А. Скопа // Захист інформації. — 2008. — № 4(41). — С. 23-29.

13. Казакова, Н. Забезпечення порівнянності результатів оцінки захищеності автоматизованих систем [Текст] / Н. Казакова, Ю. Щербина, О. Соловйов // Захист інформації і безпека інформаційних систем : II міжнар. наук.-техн. конф., 30 травня - 01 червня 2013 р. — НУ «Львівська політехніка», Львів. — С. 158-160.

14. Щербина, Ю. В. Вопросы оценки информационной безопасности автоматизированных систем [Текст] / Ю. В. Щербина, А. А. Скопа, С. Д. Асабашвили // Сучасний стан та перспективи розвитку системи технічного регулювання, метрології та якості : VI Всеукр. наук.-практ. конф. молодих учених і студентів, 21-22 травня 2015 р. — ОДАТРЯ, Одеса. — С. 81-88.

15. Щербина, Ю. В. Принципи вибору формальних параметрів при побудові профілей захисту інфоресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Восточно-Европейский журнал передовых технологий. — 2012. — №5/2(59). — С. 31-33.

16. Волков, С. Л. Вимоги щодо стандартизації захищених інформаційно-вимірювальних систем [Текст] / С. Л. Волков, А. А. Скопа, С. Д. Асабашвили // Сучасний стан та перспективи розвитку системи технічного регулювання, метрології та якості : VI Всеукр. наук.-практ. конф. молодих учених і студентів, 21-22 травня 2015 р. — ОДАТРЯ, Одеса. — С. 89-91.