*В. К. Цимбалюк В. С. та ін. /Заг. ред. Р. Калюжного та В. Філонова – Київ – Донецьк: Донецький інститут внутрішніх справ МВС України. Інститут економіки та права "КРОК", 2001.* ***10.*** *Е-будущее и информационное право /Брижко В. М., Орехов А. А., Гальченко О. Н., Цимбалюк В. С. /Под.ред Р. А. Калюжного и Н.Я. Швеца - К.: "Интеграл", 2002.* ***11.*** *Інформаційне суспільство. Дефініції… /Брижко В. М., Орехов А. А., Цимбалюк В. С., Гальченко О. Н., Чорнобров А. М. ) /Під ред. Р. А. Калюжного і М. Я. Швеца. - Київ: "Інтеграл", 2002.*

**УДК 638.235.231**

# ПРОБЛЕМЫ НОРМАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

***Петр Воробиенко, Олег Нечипорук, Юрий Щербина***
*Одесская национальная академия связи им. А. С. Попова*

*Анотація:* **Визначені основні проблеми, пов'язані із нормативно-правовим забезпеченням процедур, які дають змогу виконувати аналіз ризиків у сучасних автоматизованих системах. Викладені пропозиції щодо подальшого удосконалення вітчизняної нормативної бази у галузі захисту інформації в комп'ютерних системах.**
*Summary:* **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.**
*Ключевые слова:* **Защищенность автоматизированных систем, анализ рисков, параметры угроз.**

## I Введение

Вопрос о необходимости законодательного обеспечения деятельности, связанной с защитой информации, встал практически сразу же, как только для ее обработки начали применять распределенные вычислительные системы. Тенденция перехода на безбумажные технологии с использованием автоматизированного документооборота и развитие открытых глобальных телекоммуникационных систем многократно усложняют процесс исследования среды эксплуатации автоматизированных систем (АС) и оценку действующих в ней угроз. 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 создаваемых на их основе автоматизированных систем.

Значительная работа в этой области проводилась и в нашей стране. В 1999 году был принят документ под названием «Критерии оценки защищенности в компьютерных системах от несанкционированного доступа» (НД ТЗИ 2.5-004-99) [1], регулирующий деятельность по защите информации в компьютерных системах, а также пакет сопутствующих ему нормативных документов, которые действуют до сих пор. Компьютерная безопасность за прошедшее время превратилась в 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.

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.

## II Направления совершенствования нормативной базы в области оценки защищенности автоматизированных систем

Расхождения, имеющиеся в положениях нормативно-правовых документов Украины, регламентирующих решение вопросов, связанных с информационной безопасностью, не позволяют

отечественным разработчикам использовать результаты оценок информационных технологий, получаемых специалистами других стран. Более того, за прошедшие пять лет 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 учитывают эти изменения и аккумулируют накопленный в этой сфере опыт.

Наиболее значимым из этих документов является международный стандарт ISO 15408 [2 – 4] под названием «Общие критерии оценки безопасности информационных технологий» (Common Criteria for Information Technology Security Evaluation). В научно-технической литературе он 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 реализации этих функций. 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 аналогичными документами. 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 насколько. 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 гарантий защиты.

Наконец, в Единых критериях более глубоко прописаны зависимости между отдельными компонентами функциональных требований 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, которая отвечала 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 делают на программно-техническом аспекте реализации защиты информации, а вопросы организации управления безопасностью в них 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 под названием "Практические правила управления информационной безопасностью" (Code of Practice for Information Security Management). В нем вопросы, связанные с оценкой механизмов безопасности организационного уровня, отражены более полно в 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 ведутся разговоры о том, что в будущем возможно принятие этого документа в адаптированном виде в России и Молдове.

В нашей стране в качестве попытки закрепить на законодательном уровне вопросы управления информационной безопасностью можно рассматривать "Типовое положение о службе защиты информации в автоматизированной системе" – НД ТЗИ 1.4-001-2000 [5]. К сожалению, этот документ уступает по своему содержанию стандарту ISO/IEC 17799. В нем содержатся 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, задача 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 группа 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, а также российские технологии "КОНДОР+" и "АванГард". 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.

Недопустимо объединять технологию анализа рисков и нормативный документ. 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, выполненного различными субъектами. Что касается технологий, используемых при оценке рисков, то они могут разрабатываться как государственными, так и негосударственными организациями и главным требованием к ним должно быть их соответствие отечественному законодательству. Такие технологии должны в обязательном порядке проходить государственную аттестацию.

## III Заключение

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, недопустимо. Оно должно быть преодолено, несмотря на имеющиеся в этом вопросе трудности. Сложность проблемы не допускает попыток ее решения любительскими методами. Она может быть решена только с привлечением серьезных интеллектуальных и материальных ресурсов государственных и негосударственных организаций, а также иностранных специалистов. Совершенствование нормативной базы Украины предполагает наряду с современными и качественными нормативными документами создание современного методического обеспечения и инструментальных средств, позволяющих реализовать принципы, заложенные в таких документах.

*Литература: **1**. НД ТЗИ 1.1-003-99. Критерии оценки защищенности в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины. **2**. Information technology - Security techniques - Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO/IEC 15408 - 1. 1999. **3**. Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements. - ISO/IEC 15408 – 2.1999. **4**. Information technology - Security techniques - Evaluation criteria for IT security – Part 3: Security assurance requirements – ISO/IEC 15408 - 3. 1999. **5**. НД ТЗИ 1.4-001-2000. Типовое положение о службе защиты информации в автоматизированной системе НД ТЗИ 1. 1-002-99. 3.*

**УДК 343.13:004**

# УЧАСТИЕ СПЕЦИАЛЬНЫХ ПОНЯТЫХ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С КОМПЬЮТЕРАМИ

***Геннадий Кожевников, Вячеслав Бабенко*, Татьяна Громыко*****
*Национальный университет внутренних дел*
**Светловодский ГРО УМВД Украины в Кировоградской области*
***Национальная юридическая академия Украины имени Ярослава Мудрого*

*Аннотация:* **Показано, что при расследовании и производстве следственных действий, связанных с компьютером, необходимо присутствие специальных понятых. Это позволит достаточно профессионально реализовать данные им законом права.**
*Summary:* **In the article is exhibited, that at investigation and execution of investigators actions for investigation of e-crimes, the presence of the special attesting witnesses is necessary. It will allow them professionally to realize the rights from the law.**
*Ключевые слова:* **Расследование компьютерных преступлений, понятые, специальные понятые, защита информации, информационная безопасность, авторские права.**

## I Введение

Преступление, связанное с компьютером – это предусмотренное Уголовным кодексом Украины общественно опасное виновное деяние (действие или бездействие), требующее знаний в области компьютерных технологий. Без этих специальных знаний невозможны расследование и преследование в судебном порядке субъекта, совершившего преступление в сфере использования электронно-вычислительных машин (компьютеров).

Компьютерная наука и компьютерные технологии складывались и развивались десятилетиями. Они впитали в себя плоды деятельности множества учёных и их научных школ. Список основоположников велик и разнообразен: Клод Шеннон – создатель теории информации, Алан Тьюринг – математик, разработавший теорию программ и алгоритмов, Джон фон Нейман – автор конструкции вычислительных устройств. Пройден большой путь от вычислительных машин первого поколения (1945 – 1954 г.) до устройств с элементами искусственного интеллекта. С начала 80-годов прошлого столетия вычислительная техника становится по-настоящему массовой и общедоступной. Пользователи объединяются корпоративными и коммерческими сетями в единый информационный организм, состояние и работоспособность которого становится зависимым от функционирования как общей структуры, так и от действий отдельных её элементов. Ежедневно во всём мире с помощью компьютеров через телекоммуникационные сети передаётся огромное количество информации, осуществляется электронный документооборот. В обиход вошли такие термины, как электронные деньги, Интернет- магазин, электронный бизнес и др.

Под влиянием прогресса в сфере информационных технологий изменился и характер преступности в этой сфере. Возрастает число случаев использования в качестве инструмента преступления новейших средств связи, корпоративных компьютерных сетей, Интернета, электронной почты и др. Многие преступники достаточно хорошо знакомы с компьютером. Они используют персональные компьютеры для планирования и совершения преступлений [1].

## II Постановка задачи

Всё чаще правоохранительные органы сталкиваются с преступлениями, получившими название "компьютерные". Это требует от следователей и других должностных лиц, ведущих уголовный процесс, без которых невозможна уголовно-процессуальная деятельность, не только совершенствования существующих знаний в области компьютерных наук, но и разработки новых методик расследования данного вида преступлений. Это относится в полной мере и к субъектам, деятельность которых в ходе производства досудебного следствия носит вспомогательный, а в некоторых случаях, и эпизодический характер. При расследовании преступлений в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей, следует большее внимание уделить форме, способам и особенностям участия в производстве следственных действий по данному виду преступлений **понятых**, присутствие которых подтверждает законность производства следственного действия и соответствие его результатов записям в протоколе [2]. Привлечение незаинтересованных лиц в качестве понятых имеет целью создание необходимых условий для объективного и правильного производства многих следственных действий. К