**ИНФОРМАТИКА**

**2006** **июль-сентябрь** **№ 3**

*УДК 681.324.067*

**А.М. Криштофик**

# НОРМАТИВНО-МЕТОДИЧЕСКАЯ БАЗА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

*Проводится анализ нормативно-методической базы в области безопасности информационных технологий, содержания концепций анализа и управления рисками. Обосновываются необходимость и направления развития нормативно-методической базы. Предлагается подход к реализации этих направлений.*

## Введение

Обеспечение безопасности информационных технологий (ИТ) – творческий процесс, зависящий от множества факторов, в том числе от требований применяемых при этом нормативных документов, которые являются юридической основой для проведения работ в области безопасности ИТ. При создании и развитии сложных, распределенных, тиражируемых ИТ требуются гибкое формирование и применение гармонизированных совокупностей базовых стандартов и нормативных документов разного уровня, выделение в них требований и рекомендаций, необходимых для реализации заданных функций ИТ. Такие совокупности базовых стандартов (разработано около 50 только международных стандартов ИСО/МЭК на критерии оценки безопасности ИТ и методы защиты средств и систем ИТ) составляют сбалансированную систему, отвечающую следующим требованиям: универсальность, гибкость, конструктивность, преемственность и расширяемость. Стандарты должны адаптироваться и конкретизироваться применительно к определенным классам проектов, функций, процессов и компонентов ИТ. Ценность использования нормативно-методической базы в области безопасности ИТ заключается в возможности применения мирового опыта и лучших практик для обеспечения безопасности ИТ, проведения аудита. Это приводит к снижению сопутствующих затрат и рисков, уменьшению разногласий и повышению доверия при передаче организацией части своих функций на аутсорсинг, при заключении соглашений об уровне обслуживания между партнерами.

## 1. Общая характеристика нормативной базы по вопросам безопасности информационных технологий

В зависимости от методов и средств защиты ИТ международные стандарты ISO можно разделить на четыре группы (табл. 1).

Первая группа стандартов – ISO/IEC JTC1/SC22 «Поиск, передача и управление информацией для взаимосвязи открытых систем (ВОС)» – посвящена развитию и детализации концепции ВОС. Защита информации в данной группе рассматривается как один из компонентов, обеспечивающих возможность полной реализации указанной концепции. Для этого определены услуги и механизмы защиты по уровням базовой модели ВОС, изданы и разрабатываются стандарты, последовательно детализирующие методические основы защиты информации и конкретные протоколы защиты на разных уровнях открытых систем. Нормативной основой решения задач защиты информации являются стандарты ISO 7498:1989 [1] и ISO/IEC 10181:1996 [2]. Именно эти документы до недавнего времени определяли взгляды специалистов на теоретические подходы обеспечения защиты информации. С практической точки зрения стандарты данной группы определяют вопросы построения системы защиты информации (СЗИ), в то время как вопросы обеспечения безопасности информации в них носят больше абстрактный характер.

Вторая группа стандартов – ISO/IEC JTC1/SC27 – ориентирована преимущественно на конкретные методы и алгоритмы защиты. В эту группу объединены методологические стандарты защиты информации и криптографии независимо от базовой модели ВОС. Делается попытка обобщения конкретных методов и средств защиты в систему организации и управления защитой ИС.

К данной группе относятся стандарты по разработке типовых решений, интерфейсы механизмов безопасности ИТ и стандарты международных криптографических алгоритмов.

Таблица 1

Нормативная база по вопросам безопасности ИТ

| Направления | Функции | Стандарты |
|---|---|---|
| ISO/IEC JTC1/SC22 «Поиск, передача и управление информацией для взаимосвязи открытых систем» | Услуги и механизмы защиты по уровням базовой модели ВОС. Методические основы защиты информации и конкретные протоколы защиты на разных уровнях открытых систем | ГОСТ Р ИСО 7498-99, ISO/IEC DTR 10181, ISO/IEC DTR 10745, ISO/IEC DTR 11586 |
| ISO/IEC JTC1/SC27, конкретные методы и алгоритмы защиты | Методологические стандарты защиты информации и криптографии независимо от базовой модели ВОС по вопросам разработки типовых решений, интерфейсам механизмов безопасности ИТ и криптографическим алгоритмам | ISO/IEC 9798, ISO/IEC 09594-8, ISO/IEC 11577-94, ISO/IEC DTR 10736, ISO/IEC CD 13888, ISO/IEC CD 11770, ISO/IEC 10164-7, ISO/IEC DTR 11586, ISO/IEC 8732-87, ISO/IEC 10118-1,2, ISO/IEC CD 10118-3,4 и др. |
| ISO/TC 68 «Банковское дело и соответствующие финансовые операции» | Защита функционирования банковских систем, шифрование и аутентификация при обмене финансовой информацией в процессе деятельности банков | ISO/IEC 8732, ISO/IEC 11568, SO/IEC 11166, ISO/IEC DIS 13492, ISO/IEC 10126-2, ISO/IEC 10116 и др. |
| Информационные технологии | Методология безопасности ИТ, основанная на процедуре анализа и управления рисками и базирующаяся на двух концепциях управления рисками – для базового уровня и для повышенных требований безопасности | ISO 17799, ISO 27001, URSIT, BSI\IT Baseline Protection Manual, NIST, CIS HB 1400-14, ITS Minimum Baseline Protective Requirement, X/Open Baseline Security Services Specification (XBSS), SCORE и др. |

Третья группа стандартов – ISO/TC 68 «Банковское дело и соответствующие финансовые операции» – направлена на защиту функционирования банковских систем. Стандарты, объединенные в эту группу, ориентированы в основном на шифрование и аутентификацию при обмене финансовой информацией в процессе деятельности банков.

Во всех трех группах этих стандартов почти не уделяется внимания методологии и процессам системного проектирования комплексных равнопрочных систем обеспечения безопасности ИТ. С течением времени в информационном плане перестали делать какие-либо существенные различия между системами обработки, передачи и хранения информации. В связи с сильной интеграцией телекоммуникационных, сетевых и иных технологий, превалированием в проектировании телекоммуникационных и информационных систем идеологии единой информационной магистрали все большее практическое распространение получает термин «информационная технология» и его производные: ИТ-системы, ИТ-продукты, объекты ИТ (ОИТ) и наконец ИТ-безопасность. Под ИТ понимают целенаправленную организованную совокупность информационных процессов, реализованных с использованием средств вычислительной техники и обеспечивающих высокую скорость обработки данных, быстрый поиск информации, распределение данных, доступ к источникам информации независимо от места их расположения [3]. Одновременно с трансформацией взглядов на процессы обработки информации происходит и изменение взглядов на подходы к обеспечению безопасности информации. Исключительно широкая сфера применения ИТ, беспрецедентное расширение функциональных возможностей ИТ-систем и многие другие причины привели к тому, что существующая модель обеспечения информационной безопасности (ИБ) «угроза безопасности – услуга безопасности – механизм безопасности» [4] перестала удовлетворять как потребителей, так и разработчиков. Это вызвало необходимость поиска новой модели безопасности ИТ и соответственно к разработке новых международных стандартов, которые можно объединить в четвертую методологическую группу. Основополагающими

стандартами данной группы являются ISO 17799 [5] и ISO 15408 [6], принятые в качестве национальной нормативной базы по вопросам безопасности ИТ [7, 8].

Международный стандарт менеджмента безопасности ISO 17799 наиболее полно определяет критерии для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты. В нем приведены десять практических рекомендаций по управлению ИБ, разработанных на основе передового мирового опыта, спецификации для проведения сертификации режима ИБ, концептуальные основы управления ИБ. Он не зависит от конкретного средства защиты или технологии и является наиболее распространенным среди организаций и предприятий. В международной практике широко применяется и сертификационный стандарт ISO 27001 [9], разработанный на основе второй части Британского стандарта BS 7799. Он определяет возможные меры по обеспечению защиты в соответствии с требованиями первой части стандарта и по предотвращению реализации угроз безопасности (управление рисками ИБ). Применение данных стандартов позволяет повысить эффективность работ по обеспечению ИТ-безопасности.

Новый взгляд на проблему безопасности ИТ окончательно был закреплен в стандарте ISO/IEC 15408 [6] и ассоциированной с ним методологии (ISO/IEC 18045 [10]), в которых наиболее широко и детально рассмотрены методологические и системные задачи проектирования и оценки комплексной защиты ИТ. Критерии оценки безопасности ИТ содержат систематизированный каталог требований к безопасности ИТ, порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем ИТ по требованиям безопасности. Под безопасностью ИТ понимается состояние, определяющее защищенность ее информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений. Требования к безопасности конкретных продуктов и систем ИТ устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, а также с учетом условий их применения. Критерии дают возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциям безопасности ОИТ и к мерам доверия, применяемым к ним при оценке безопасности. В процессе оценки обеспечивается определенный уровень уверенности в том, что функции безопасности таких продуктов или систем, а также предпринимаемые меры доверия отвечают предъявляемым требованиям.

Таким образом, стандарт играет важную роль в методической поддержке выбора потребителями требований безопасности ИТ для формирования своих потребностей, а также помогает разработчикам при подготовке к оценке своих продуктов или систем защиты информации (СЗИ). Кроме того, он может использоваться для выбора приемлемых мер защиты информации, поскольку в них содержатся критерии оценки требований безопасности. В целом стандарт представляет собой детальное комплексное руководство, охватывающее требования к функциям и методам гарантирования качества основных современных методов и средств обеспечения безопасности ИТ, которое целесообразно использовать при практическом проектировании и эксплуатации систем защиты. Он предназначен для использования в качестве основы при оценке характеристик безопасности продуктов и систем ИТ, а также для практического применения в деятельности заказчиков, разработчиков и пользователей ИТ.

Вопросам анализа и использования стандарта и методологии проведения оценки, а также их развития посвящено множество публикаций, в том числе [11–13]. Анализ этих документов показывает, что совершенствование нормативного обеспечения безопасности ИТ в последнее время все более склоняется в сторону использования философии, базирующейся на признании того факта, что уровень безопасности зависит не столько от выполнения набора формальных требований к конкретным подсистемам, входящим в комплекс средств обеспечения безопасности, сколько от научно обоснованного проектирования самих систем и квалифицированной внешней независимой экспертной оценки результатов работ. Научно обоснованное и экономически целесообразное обеспечение безопасности ИТ проводится с использованием концепции анализа и управления рисками на основании общесистемного критерия «эффективность/стоимость». Концепции анализа и управления рисками на всех стадиях жизненного цикла ИТ были предложены многими крупными организациями, занимающимися проблемами ИБ. На этапе анализа рисков определя-

ется возможность понести убытки из-за нарушения режима информационной безопасности организации, детализируются характеристики (или составляющие) рисков для информационных ресурсов и технологий. Результаты анализа используются при выборе средств защиты, оценке эффективности существующих и проектируемых подсистем информационной безопасности, т. е. на этапе управления рисками. Под управлением рисками понимается процесс идентификации и уменьшения рисков, которые могут воздействовать на ИТ. Методология безопасности ИТ, определяемая данными стандартами, базируется на двух концепциях управления рисками – для базового уровня и для повышенных требований безопасности.

## 2. Концепция, нормативно-методическая и инструментальная база для минимальных требований безопасности

Минимальные требования безопасности (базовый уровень) обеспечиваются совокупностью проверенных практикой правил обеспечения ИБ на всех этапах жизненного цикла ИТ и соответствуют минимальным требованиям к режиму ИБ. Эти правила носят комплексный характер, т. е. охватывают административный, процедурный, программно-технический уровни и все этапы жизненного цикла ИТ. Обычной областью использования этого уровня являются типовые проектные решения.

Существует ряд стандартов и спецификаций (табл. 2), в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов, которые также приводятся в этих документах (рис. 1). Основополагающими документами, определяющими концепцию управления рисками для базового уровня, являются международные стандарты менеджмента безопасности ISO 17799, ISO 27001. Они описывают концептуальные основы управления ИБ, возможные меры по обеспечению защиты для базового уровня защищенности и по предотвращению реализации угроз безопасности (управление рисками ИБ). Для удобства практического использования этих стандартов Британский институт стандартов (BSI) выпустил серию практических рекомендаций, посвященных различным аспектам ИБ, которые существенно дополняют стандарты, а также справочников, посвященных практическим аспектам реализации политики безопасности в соответствии с ISO17799.

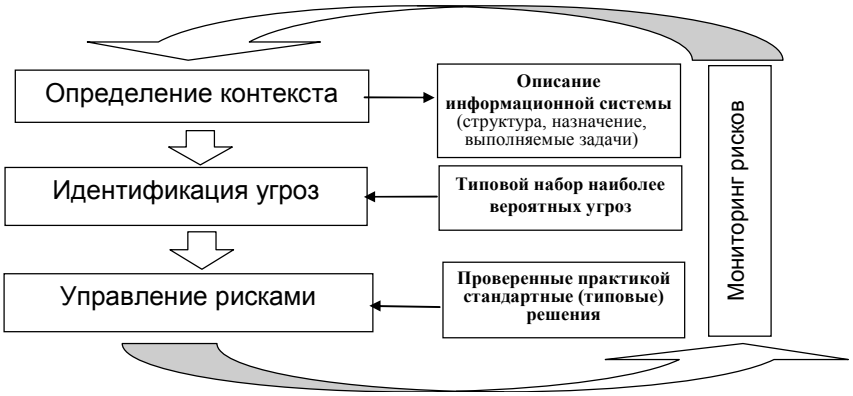


Рис. 1. Концепция управления рисками для базового уровня безопасности ИТ

Широкое распространение получили национальные стандарты, стандарты и спецификации организаций и ведомств, такие как «Руководство по политике безопасности для автоматизированных информационных систем» США, германский стандарт BSI «Руководство по защите информационных технологий для базового уровня», «Спецификации сервисов базового уровня ИБ» консорциума X/Open, ведомственный стандарт NASA «Безопасность информационных технологий. Минимальные требования к базовому уровню защищенности». Указанные стандарты определяют базовый уровень ИБ, при котором проводится качественная оценка рис-

ков, для чего разработаны и используются различными организациями методики качественной оценки эффективности защиты, такие как COBRA, КОНДОР и др. (табл. 2).

Основные положения и использование нормативно-методической базы при минимальных требованиях безопасности детально рассмотрены в научно-технической литературе, например [4, 12]. Достоинствами подобного подхода являются: сравнительно низкая трудоемкость; ориентация на проверенные стандартные решения; простота применения и адаптации на практике; независимость от конкретных технических средств и решений, что обеспечивает свободу выбора платформ, оборудования, производителей и т. п.; возможность использования и адаптации одинаковых базовых защитных мер для многих систем при малых затратах; обеспечение рентабельности решений для большого количества систем организации, действующих в общей среде при сопоставимости целей. Недостатками являются отсутствие оценок параметров, характеризующих режим ИБ, а также вероятность упустить из вида специфические для конкретной ИТ-системы классы угроз.

### 3. Концепции, нормативно-методическая и инструментальная база для повышенных требований безопасности информационных технологий

В случаях когда нарушения ИБ чреваты тяжелыми последствиями, базовый уровень защищенности является недостаточным. Для того чтобы сформулировать дополнительные требования, необходимо определить ценность ресурсов, к стандартному набору добавить список угроз, актуальных для исследуемой ИТ, оценить вероятности угроз и уязвимости ресурсов. Возможные подходы к выбору дополнительных требований рассмотрены в работе [4]. В этом случае должен быть проведен так называемый полный вариант анализа рисков, в рамках которого, в дополнение к базовым требованиям, рассматриваются следующие аспекты: возможность выполнения целей организацией; критичность ИТ с точки зрения ИБ; ресурсы организации и их ценность; уязвимости – слабые места в защите, которые способствуют реализации угроз. На основе этих данных должны быть получены оценки рисков для ИТ-организации, отдельных подсистем, баз данных, отдельных элементов данных. На основании оценок рисков осуществляется выбор контрмер, снижающих риски до приемлемых уровней, по критерию эффективность/стоимость, т. е. управление рисками. В настоящее время разработаны, опубликованы и используются полностью или частично две концепции управления рисками – в соответствии со специальной публикацией NIST США [14] и организацией MITRE [15].

В соответствии с концепцией управления рисками NIST SP 800-30 система управления рисками организации должна минимизировать возможные негативные последствия, связанные с использованием ИТ, обеспечить возможность выполнения основных целей организации и должна быть интегрирована в систему управления жизненным циклом ИТ (табл. 3) [14].

Концепция управления рисками NIST SP 800-30 включает следующие стадии анализа и управления рисками: описание системы, идентификацию угроз, идентификацию уязвимостей, анализ системы управления информационной системой (ИС), оценку параметров угроз, анализ возможных последствий нарушения ИБ, определение рисков, разработку рекомендаций по управлению рисками, разработку отчетных документов.

Таблица 3

Управление рисками на различных стадиях жизненного цикла ИТ

| Фаза жизненного цикла ИТ | Соответствующая фаза управления рисками |
|---|---|
| Предпроектная стадия ИС (концепция данной ИС: определение целей и задач и их документирование) | Выявление основных классов рисков для данной ИС, вытекающих из целей и задач, концепция и политика обеспечения ИБ |
| Проектирование ИС | Анализ рисков, специфичных для данной ИС (вытекающих из особенностей архитектуры ИС) |
| Создание ИС: поставка элементов, монтаж, настройка и конфигурирование | Идентификация всех классов рисков и управление ими |
| Функционирование ИС | Периодическая переоценка рисков, связанная с изменениями внешних условий и в конфигурации ИС |
| Прекращение функционирования ИС и ее утилизация | Соблюдение требований ИБ по отношению к выводимым информационным ресурсам |

Подобная концепция управления рисками получила развитие в техническом отчете ISO TR 13335, который отражает широкий комплекс методологических задач, необходимых при проектировании систем обеспечения безопасности любых ИС (рис. 2) [16]. Стадии управления

рисками концепции этого документа приведены в табл. 4. Изложенную в отчете модель планирования обеспечения безопасности целесообразно конкретизировать и использовать как фрагмент системного проекта ИТ.

В рамках данных концепций широкое распространение получили национальные стандарты и стандарты организаций, такие как Sys Trust, BSI\IT, Baseline Protection Manual, SAC, COSO, SAS 55/78, Cobit, предусматривающие вопросы анализа и управления рисками, и некоторые другие, аналогичные им (табл. 5).

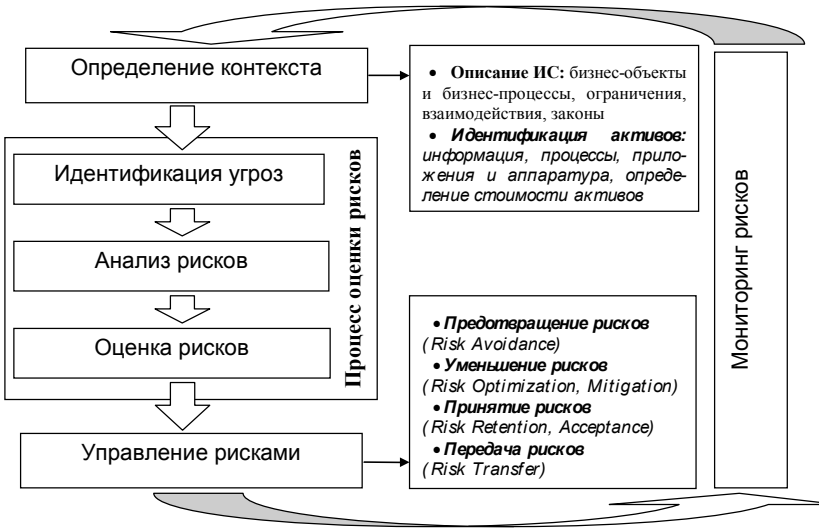


Рис. 2. Концепция управления рисками ISO TR 13335

Для эффективного анализа и управления информационными рисками разработаны и широко используются количественные международные и национальные методики, позволяющие в той или иной степени провести полный или частичный анализ рисков. К таким методикам относятся CRAMM, Risk Watch, MARION, Buddy System, Method Ware и др. (табл. 5). Указанные стандарты и методики, реализующие вопросы анализа и управления рисками, с той или иной мерой полноты и качества предполагают анализ и оценку рисков (активов, угроз, уязвимостей) и управление ими с целью выбора контрмер для снижения ущерба.

Таблица 4

Стадии и содержание концепции управления рисками ISO TR 13335

| Стадии управления рисками | Содержание | |
|---|---|---|
| Идентификация | Угрозы | Агент угрозы (человек, случайность, технология)<br>Природа угрозы (физическая, техническая, логическая)<br>Тип угрозы (случайная/намеренная, активная/пассивная)<br>Источник угрозы (внутренний/внешний)<br>Вероятность и частота возникновения |
| | Уязвимости | Постоянная/при определенном стечении обстоятельств<br>Необходимые ресурсы |
| | Ущерб | Прямой/косвенный<br>Вещественный/нематериальный<br>Немедленный/будущий |
| Анализ | Количественное измерение | Угроз (Threats, T)<br>Уязвимостей (Vulnerabilities, V)<br>Ущерба (Damage, D) |
| | Учет вероятности, осуществимости | |
| | Вычисление рисков: Risk = T*V*D | Базовый метод<br>Информационный метод<br>Детальный анализ рисков<br>Комбинированный метод |
| Оценка | Определение уровня риска | |
| | Сравнение с приемлемым уровнем, бизнес-целями | |
| | Принятие решения | Допустить риск<br>Принять меры по устранению (снижению риска) |
| Управление | Уменьшение рисков | Принятие контрмер<br>Соотношение стоимости/эффективности (ROI – Return of Investments) |
| | Передача рисков | Страховой компании |
| | Допущение (остаточных) рисков | |

Организацией MITRE разработана концепция управления рисками при построении различных систем (не только информационных), в которой риск не разделяется на составляющие части (угрозы и уязвимости), что в некоторых случаях может оказаться более удобным с точки зрения владельцев информационных ресурсов. Для реализации этой концепции MITRE разработала простейший инструментарий для использования на этапе идентификации и оценки рисков, выбора возможных контрмер – «Risk Matrix».

Анализ основных положений и использования нормативно-методической базы при повышенных требованиях безопасности приведен в работах [12, 13, 17]. Достоинствами данного подхода являются научная обоснованность обеспечения ИТ-безопасности и наличие оценок параметров, характеризующих режим ИБ, недостатком – высокая трудоемкость.

**4. Недостатки нормативно-методической базы**

Использование стандартов увеличивает ценность создаваемых ИТ, однако нет таких стандартов, которые охватывали бы все аспекты безопасности. Существующая нормативно-методическая база имеет и существенные недостатки, основными из которых являются:

– игнорирование системного подхода как методологии анализа и синтеза СЗИ;

– отсутствие механизмов полного и достоверного подтверждения качества СЗИ;

– недостаточность проработки вопросов моделей системы защиты, системы показателей и критериев безопасности ИТ, эффективности средств защиты, предъявления требований к их стойкости;

– невозможность обоснования и оценки достаточности безопасности.

Перечисленные недостатки коренятся как в несовершенстве существующей нормативной базы, так и в сложившихся в ИТ подходах, принципиально отличающихся от разработанных в традиционной инженерии. Так, например, принципиальные различия этих подходов к анализу уязвимостей заключаются в том, что в первом случае (семейство требований доверия AVA_VLA стандарта ISO/IEC 15408) доминирует статический подход, цель которого – доказать отсутствие уязвимостей, допускающих практическое использование после использования СЗИ, а во втором наличие уязвимостей не вызывает сомнений: их нужно непрерывно отслеживать, систематизировать их свойства и выбирать контрмеры в зависимости от этих свойств. В соответствии с одним из положений стандарта SSE-CMM (ISO/IEC 21827) при рассмотрении вопросов оценки уязвимостей предусматривается мониторинг непрерывных изменений в наборе системных уязвимостей и в их характеристиках, а также процесс координации безопасности при рассмотрении 11 групп процессов, относящихся к разработке СЗИ [18]. Проблемными являются и такие вопросы, как игнорирование стохастичной природы событий и явлений, возникающих в процессе защиты информации, абстрагирование от их экономического содержания.

Это в полной мере относится и к фундаментальным категориям безопасности ИТ, терминологии основных понятий. Несмотря на широкое использование методов, основанных на применении рисков ИБ, понятие риска в области безопасности ИТ до сих пор не имеет единого общепризнанного определения. В глоссарии терминов по информационной безопасности приводится восемь определений риска, коррелированных в той или иной степени между собой, 16 определений угрозы и 13 определений уязвимостей, взятых из зарубежных источников [19]. Так, в терминологическом словаре Центра компьютерной безопасности США (NCSC) приведены два определения риска безопасности [20], предполагающих использование как доверительного, так и обычного методов оценки рисков [21]. Такое разнообразие определений терминов привело к большому разнообразию подходов, методов и критериев оценки защищенности ИТ [22].

Рассмотренные недостатки обусловливают необходимость развития нормативно-методической базы с учетом существующих недостатков на основе системного подхода, предусматривающего, что СЗИ должна быть комплексной и адаптируемой к изменяющимся условиям.

**Заключение**

Доминирующее влияние на ход работ в направлении стандартизации обеспечения безопасности ИТ оказывают международный стандарт ISO/IEC 15408 и ассоциированная с ним методология ISO/IEC 18045, которые являются современной базой содержательной и, в значительной

степени, формальной оценки безопасности ИТ. Основные достоинства этих документов заключаются в гибкости, учете современного уровня ИТ, а также широте спектра, высоком уровне детализации и параметризации требований безопасности. Однако существующая нормативная база обладает рядом недостатков, не позволяющих обосновать и оценить уровень безопасности ИТ. Вследствие этого она требует дальнейшего развития.

Нормативная и, прежде всего, методическая база требуют разработки моделей системы обеспечения безопасности, критериев и показателей защищенности, методов их оценки и оценки элементов безопасности, методик оценки защищенности на всех этапах жизненного цикла ИТ, динамической оценки рисков на основе системного подхода, при котором первостепенное значение имеют только те свойства элементов защиты, которые определяют взаимодействие друг с другом и оказывают влияние на систему в целом, а также на достижение поставленной цели.

**Список литература**

1. ГОСТ Р ИСО 7498-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1: Базовая модель. Часть 2: Архитектура защиты информации. Часть 3: Присвоение имени и адресация. Часть 4: Основы административного управления.

2. ISO/IEC DTR 10181. Информационные технологии. Взаимосвязь открытых систем. Основы защиты информации для открытых систем. Часть 1: Общее описание основ защиты информации в ВОС. Часть 2: Основы аутентификации. Часть 3: Управление доступом. Часть 4: Безотказность получения. Часть 5: Конфиденциальность. Часть 6: Целостность. Часть 7: Основы проверки защиты.

3. Щербо, В.К. Стандарты вычислительных сетей. Взаимосвязи сетей: справочник / В.К. Щербо. – М.: Кудиц – образ, 2000. – 198 с.

4. Underlying Technical Models for Information Technology Security / G. Stoneburner. – NIST Special Publications, 2001.

5. ISO/IEC 17799:2005. Информационные технологии. Управление информационной безопасностью.

6. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO/IEC 15408-1:2005, Part 2: Security functional requirements. — ISO/IEC 15408-2:2005, Part 3: Security assurance requirements. – ISO/IEC 15408-3:2005.

7. СТБ П ИСО/МЭК 17799-2000/2004. Информационные технологии и безопасность. Правила управления информационной безопасностью.

8. СТБ 34.101.1-3. Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель. Часть 2: Функциональные требования безопасности. Часть 3: Гарантийные требования безопасности.

9. ISO/IEC 27001:2005. Информационные технологии. Средства безопасности. Менеджмент качества в области безопасности информационных систем.

10. Information technology – Security techniques – Methodology for IT Security Evaluation. – ISO/IEC 18045:2005.

11. Information technology – Security techniques – Security assessment of operational systems. – ISO/IEC 2nd PDTR 19791:2004.

12. Галатенко, В.А. Стандарты информационной безопасности / В.А. Галатенко; под ред. академика РАН В.Б. Бетелина. – М.: ИНТУИТРУ, 2004. – 328 с.

13. Hearn, J. Does the Common Criteria Paradigm Have a Future / J. Hearn // IEEE Security & Privacy. – 2004, January/February. – P. 64–65.

14. Risk Management Guide for Information Technology Systems. – NIST, Special Publication 800-30.

15. Systems Engineering at MITRE Risk Management – R1, MP96B0000120, September 1998.

16. ISO TR 13335:1996–1998 – 1–5. IT Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for IT security; Part 2: Managing and planning IT security; Part 3: Techniques for the managing of IT security ИТ; Part 4: Selection of safeguards; Part 5. Management guidance on network security.

17. Симонов, С.В. Технологии и инструментарий для управления рисками / С.В. Симонов // Jet Info. – № 2(117). – 2003. – 32 с.

18. Information technology – System Security Engineering – Capability Maturity Model (SSE-CMM). – ISO/IEC 21827:2002.

19. Глоссарий терминов по информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.garlic.com /-lynn/ secure.htm.

20. NCSC-TG-004 (Aqua Book) Glossary of Computer Security Terms (Version 1, 0/21/88) [Electronic resource]. – Mode of access: www.radium.ncsc.mil/tpep/library/rainbow/index.html.

21. Departament of the Nevy Automated Information Systems Security Program, USA [Electronic resource]. – Mode of access: www.cs.nps.navy.mil/curricula/tracks/security/AISGuide/ navch08.txt.

22. Анищенко, В.В. Методы оценки эффективности защиты активов в объектах информационных технологий / В.В. Анищенко, А.М. Криштофик // Информатика. – № 3. – 2004. – С. 95–105.

**Поступила 17.04.06**

*Объединенный институт проблем*
*информатики НАН Беларуси,*
*Минск, Сурганова, 6*
*e-mail: anath@newman.bas-net.by*

**A.M. Krishtophic**

## NORMATIVE AND METHODICAL BASE IN THE FIELD OF INFORMATION SECURITY. THE CONDITION AND DEVELOPMENT PROSPECTS

We present an analysis of normative and methodical base in the field of information security including concepts for the risk analysis and risk management. We prove also the necessity and directions of normative and methodical base development. We suggest an approach to realization of the direction.