

# Систематика уязвимостей и дефектов безопасности программных ресурсов

В статье анализируются причины уязвимостей программных ресурсов и рассматриваются их современные таксономии и систематики. Кроме того, автором предложены принципы таксономии уязвимостей программ, основанной на дефектах безопасности и таксономия уязвимостей программ, связанная с международными стандартами.

**А. С. Марков**, кандидат технических наук, доцент кафедры «Информационная безопасность»  
МГТУ им. Н. Э. Баумана  
mail@сpro.ru

**А. А. Фадин**, главный конструктор  
НПО «Эшелон»

## Введение

Проблема безопасности программ является одной из первостепенных в области информационной безопасности (ИБ), так как наличие уязвимостей в программных ресурсах информационных систем обуславливает возможность реализации промышленных компьютерных атак и вирусных эпидемий, а также причину разного рода непреднамеренных отказов и потери ресурсов. С учетом динамичности и сложности программ и развития технологий информационного противоборства решение указанной проблемы требует непрерывного совершенствования методов контроля, тестирования и испытаний, а именно: статического и динамического анализа, функционального тестирования, экс-

пертиз бюллетеней безопасности, сканирования уязвимостей, антивирусного контроля и др. Синтез и комплексирование указанных подходов подразумевают систематизацию базовых понятий безопасности программного обеспечения (ПО). Но, несмотря на то что подобные работы регулярно проводятся, в практике ИБ остается различное толкование понятия уязвимости ПО, в частности, наиболее часто смешивают определения ошибок безопасного программирования и известных уязвимостей сетевых сервисов, недекларированных возможностей и программных закладок, скрытых каналов и скрытых криптографических каналов и т. п. В результате возникает не только путаница со средствами выявления уязвимостей и базами уязвимостей, но и с целями и результатами оценки соответствия. Отсутствие национального стандарта также ограничивает развитие отечественных инструментальных средств выявления дефектов и уязвимостей. Разработке предложений по иерархической классификации (таксономии) уязвимостей программ и прин-

ципам их построения (систематики) посвящена данная статья.

## Понятие уязвимости и дефекта безопасности программ

Большинство современных классификаций угроз и уязвимостей допускают их разделение по этапу жизненного цикла ПО: проектирование (архитектура), кодирование (реализация), эксплуатация (администрирование) [7]. С точки зрения практики использования двух основополагающих подходов к контролю безопасности ПО – анализа кода и сканирования ресурсов – целесообразно отделить от определения уязвимости понятие дефекта безопасности.

Под *дефектом безопасности* (weakness, bug) будем понимать недостаток создания ПО, потенциально влияющий на степень безопасности информации. В таком случае эксплуатируемый дефект безопасности представляет собой *уязвимость* (vulnerability), реализация которой составляет угрозу ИБ. Надо понимать, что для реализации уязвимости не-

обходимо наличие субъекта, воздействующего на информационную систему и способного эксплуатировать уязвимость.

В российской нормативной базе имеется ряд определений отдельных классов уязвимостей, а именно: программной закладки (ГОСТ Р 50.1.053-2005), скрытого канала (ГОСТ Р 53113.2-2009), бреши/уязвимости (ГОСТ Р 50922-2006) и недекларированной возможности (РД Гостехкомиссии России). В частности, в руководящем документе Гостехкомиссии России недекларированная возможность и программная закладка соответственно трактуются как некая уязвимость безопасности, не описанная в документации, и преднамеренная уязвимость иницилируемого типа.

Справедливости ради заметим, что согласно информации, представленной на сайте Росстандарта (Технический комитет 362), в стране проводятся изыскания по развитию стандартов в области уязвимостей информационных систем вообще. Несомненно это является важной вехой в развитии отечественной нормативной базы в области технической защиты информации. Мы же рассмотрим вопросы классификации уязвимостей программных систем и связанных с ними понятий.

### Классификация уязвимостей программных систем

В настоящее время можно встретить ряд как простых, так и сложных иерархических классификаций (таксономий) в области программной безопасности, которые можно разделить на следующие:

- классификации угроз и атак;
- классификации вредоносных программ;
- классификации и реестры уязвимостей;
- классификации дефектов.

#### Классификации угроз и атак

Данные классификации являются самыми методически проработанными и систематизируют различные виды искусственных и естественных, случайных и злонамеренных, внутренних и внешних угроз по мно-

жеству всевозможных параметров [1–12]. Как правило, классификации выделяют класс угроз, связанный с возможностью реализации нарушителем программных уязвимостей, однако классы уязвимостей описываются только в общем плане. При всем этом данные классификации являются основой для построения моделей угроз безопасности информации.

#### Классификации вредоносных программ

Разработчики средств антивирусной защиты придерживаются классификаций «вредоносного» ПО (malware) по модели распространения, по способу активации, по действию и другим параметрам, что позволяет разрабатывать эффективные тесты и базы сигнатур антивирусов. Данные классификации полезны при описании подкласса уязвимостей эксплуатационного типа, напрямую не касающихся уязвимостей этапа проектирования и кодирования.

#### Классификации и реестры уязвимостей

Исторически реестры уязвимостей были обусловлены потребностью в регулярном распространении бюллетеней и сводок о найденных уязвимостях для каждого типа и версии программных продуктов и сред. Такие реестры поддерживаются как крупными разработчиками ПО (например Adobe, Microsoft, RedHat), так и различными ассоциациями (US-CERT, Secunia, Open Security Foundation). Последние создали ряд реестров, группирующих в единой системе идентификаторов (например, CVE-ID) уязвимости ПО различных разработчиков.

#### Классификации дефектов

Данный вид таксономий касается систематизации дефектов безопасности ПО при исследовании исходного кода ПО. В отличие от известных описанных уязвимостей (внесенных в реестры) дефекты представляют собой внутреннее свойство каждой реализации ПО или системы [10].

Большая часть дефектов возникает в процессе создания ПО. Это

могут быть ошибки проектирования, ошибки кодирования программистов, ошибки, допущенные при сборке дистрибутива и интеграции различных версий компонентов ПО.

Некоторые таксономии включают понятие дефектов информационной системы, которые связаны с конфигурацией системы и вызваны либо ошибками администраторов (например, неверными настройками схемы аутентификации, несвоевременной установкой обновлений операционной системы или сетевых сервисов), либо ошибками операторов информационных систем (например, слабыми паролями в учетной записи, некорректным выключением компьютера).

В табл. 1. представлены популярные классификации в области безопасности ПО.

Из табл. 1 видно, что в настоящее время известно достаточно большое количество таксономий в области ИБ, но в основном они ориентированы на конкретные задачи, будь то сетевые атаки, уязвимости операционных систем или некорректности программирования.

На наш взгляд, среди рассмотренных таксономий лучшим, с точки зрения разработчика, является реестр CWE (по показателям полноты, всесторонности классификации, наличия подробных описаний с примерами кода), а с точки зрения администратора, самой эффективной представляется таксономия CVE (по показателям объема записей, оперативности обновления).

С другой стороны, классификация CWE в общем случае неоднозначна и достаточно сложна, к тому же не отражает в полной мере вопросы безопасности конфигураций. Что касается практического статического анализа программного обеспечения, по оценкам большинства экспертов, более удобна простая таксономия Fortify – «7 разрушительных царств».

Следует отметить, что в академической литературе можно встретить иерархические (включающие группы, виды, типы и т. д.) классификации уязвимостей, заимствованные из области технических систем, в частности, ориентированные на

Таблица 1. Классификации в области безопасности программ

Вид	Примеры	Особенности
Классификации вредоносного программного обеспечения	<i>Mitre MAEC (Malware Attribute Enumeration and Characterization)</i> – перечень и характеристики признаков вредоносного ПО	Язык для описания вредоносного ПО, учитывающий признаки поведения, тип атаки и т. п.
	<i>Kaspersky Classification</i> – классификация Лаборатории Касперского	Классификация вредоносного ПО по способам воздействия
	<i>Symantec Classification</i> – классификация фирмы Symantec	Классификация обнаруженного вредоносного ПО
Реестры и классификации уязвимостей программных систем	<i>MITRE CVE (Common Vulnerabilities and Exposures)</i> – общие уязвимости и «незащищенности»	База данных известных уязвимостей
	<i>NVD (National Vulnerability Database)</i> – национальная база уязвимостей США	База уязвимостей, использующая идентификаторы CVE
	<i>OSVDB (Open Security Vulnerability Database)</i> – база уязвимостей открытого доступа	База данных известных уязвимостей
	<i>US-CERT Vulnerability Notes Database</i> – база уязвимостей	Описание найденных уязвимостей и способов их обнаружения
	Бюллетени разработчиков: • Microsoft Bulletin ID • Secunia ID • VUPEN ID	Сводки найденных уязвимостей
	Таксономия Бишоп и Бейли	Устаревшая классификация уязвимостей Unix-систем
	Классификации угроз безопасности и компьютерных атак на ресурсы системы	<i>OWASP Top Ten</i> – 10 самых распространенных угроз для веб-приложений
	<i>MITRE CAPEC (Common Attack Pattern Enumeration and Classification)</i> – перечень и классификация распространенных типов атак	Всесторонняя классификация типов атак
	<i>Microsoft STRIDE Threat Model</i> – модель угроз Microsoft	Описание пяти основных категорий уязвимостей
	<i>WASC Threat Classification 2.0</i> – классификация угроз Консорциума безопасности веб-приложений	Классификация изъянов, угроз веб-безопасности, нацеленная на практическое применение
Классификации дефектов, внесенных в процессе разработки	<i>MITRE CWE (Common Weaknesses Enumeration)</i> – общая классификация дефектов ПО	Система классификации «изъянов» ПО
	<i>Fortify Seven Pernicious Kingdoms</i> – 7 разрушительных «царств» компании HP Fortify	Классификация дефектов ПО на 8 основных видов
	<i>CWE/SANS Top 25 Most Dangerous Software Errors</i> – 25 наиболее опасных ошибок в разработке ПО	25 наиболее распространенных и опасных ошибок, которые могут стать причиной уязвимости
	<i>OWASP CLASP (OWASP Comprehensive, Lightweight, Application Security Process)</i> – описание процесса безопасной разработки приложений	Принципы безопасности организации процесса разработки приложений
	<i>DoD Software Fault Patterns</i> – образцы программных ошибок Минобороны США	Система типов дефектов ПО, ассоциированная с CWE и разработанная с целью автоматизации их выявления
	Устаревшие классификации: • перечни RISOS/PA • таксономия Ландвера • таксономия Аслама • таксономия Макгоу • таксономия Вебера • перечень PLOVER	Первые проекты по частичной каталогизации известных дефектов безопасности и их классификации
		<i>MITRE Common Configuration Enumeration (CCE)</i> – общий реестр конфигураций
Классификации дефектов, внесенных в процессе внедрения и эксплуатации	<i>DPE (Security-Database Default Password Enumeration)</i> – реестр паролей по умолчанию	База данных паролей по умолчанию для сетевых устройств, ПО и ОС, предназначенная для тестирования с целью выявления слабых конфигураций

всевозможные классы и виды ПО информационно-вычислительных систем (ОС, ППП, ПЗУ, SCADA-системы и т. д.) и далее типы ошибок соответствующих классов и подклассов ПО. В то же время, например,

использование современных мобильных сред программирования приводит к тому, что в таких классификациях присутствуют многократные дублирования описаний одних и тех же ошибок (например, переполнение

буфера). В итоге возникает ситуация, когда на одном уровне классификации сосуществуют понятия разной степени абстракции, описывающие какой-либо редкий частный случай (ошибки процессов и потоков) или

достаточно широкий отвлеченный класс проблем (ошибки структуры и действий).

Подобный подход, конечно, создает проблемы не только для редактора, заполняющего классификацию (зачастую один и тот же объект можно справедливо поместить в несколько таксонов), но и для ее потребителей, которым подчас достаточно сложно понять, каким образом с ней интегрировать инструментальные средства (анализаторы кода, сетевые сканеры уязвимостей).

### Систематика дефектов и уязвимостей

Учитывая опыт существующих классификаций и таксономий, можно сформулировать требования к перспективным таксономиям дефектов и уязвимостей в области безопасности ПО:

- в классификации или свойствах отдельного таксона должна содержаться информация об этапе жизненного цикла, на котором возникает дефект ПО и его области (общая архитектура, код, внутренняя конфигурация, внешнее окружение);
- в классификации уязвимостей или свойствах их отдельных таксонов необходимо указать ссылку на виды угроз или механизмы атак, при которых возможно эксплуатация этой уязвимости (примеры: атаки внедрения данных, атаки подмены идентификатора, атаки физического доступа и т. п.);
- если первопричиной появления уязвимости является связь с конкретными внешними компонентами (СУБД, web-сервер), то в свойствах отдельного таксона должна быть указана ссылка на наименование соответствующей уязвимости внешнего компонента.

Схема возможного разделения таксонов представлена на рисунке.

Для перспективного использования таксономии необходимо дополнить ее ссылками на международные реестры уже найденных уязвимостей и проблем конфигураций, классификации угроз и атак, то есть совместить абстрактную таксономию с результатами анализа реально су-

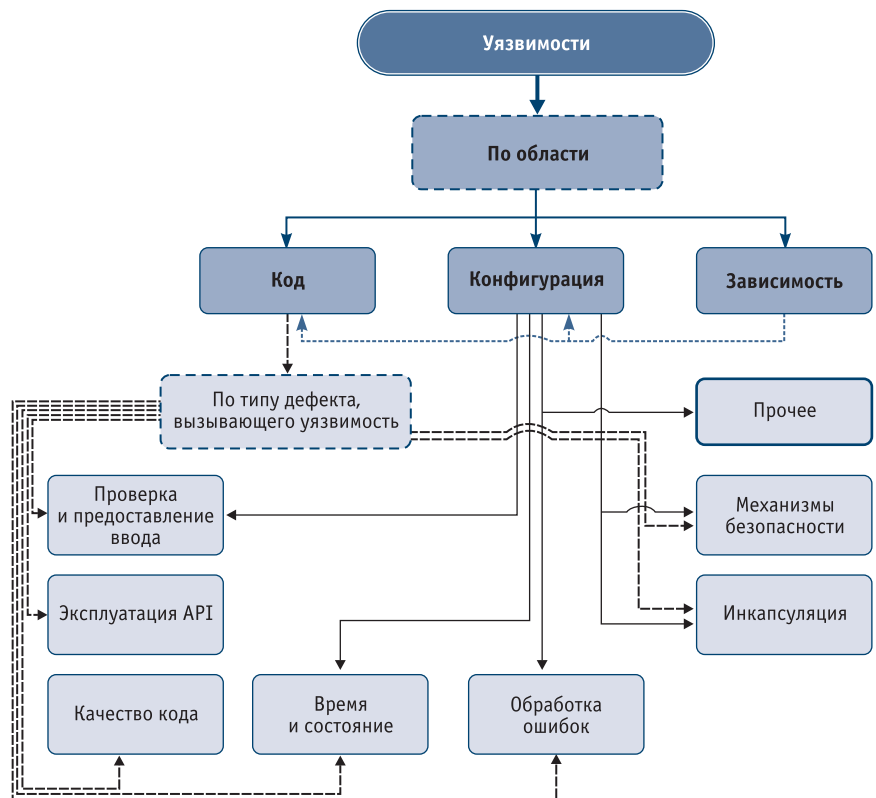


Рисунок. Критерии разделения таксонов

ществующего ПО и компонентов. Это позволило бы понять исследователю природу уязвимости ПО, ее местонахождение и сделать процесс устранения таковой более формализованным.

Дерево предлагаемой классификации уязвимостей на основе причин их возникновения (дефектов) в общем виде представлено в табл. 2. Классификация включает два типа и восемь классов. Типы представляют собой:

- уязвимости, вызванные дефектами проектирования и программирования;
- уязвимости, вызванные дефектами конфигурирования и управления.

Восемь классов соответствуют наиболее применимым с точки зрения практики анализа кода международным таксономиям, а именно включают уязвимости, связанные со следующим:

- обработкой и представлением данных;
- внутренней структурой и зависимостями компонентов;
- обработкой событий и состояний;
- внутренними механизмами и ресурсами;

- преднамеренным внедрением;
- качеством проектирования и документированием;
- конфигурациями;
- окружением.

Элементы дерева классификации имеют вид абстрактных данных, то есть содержат необходимые свойства, отражающие различные связи и ссылки на международные источники и др. Для удобства восприятия ссылки на международные стандарты вынесены в табл. 3.

### Выводы

Развитие программных и информационных технологий обуславливает потребность в национальном стандарте, определяющем принципы систематики, таксономии и классификации уязвимостей и дефектов безопасности программных ресурсов.

Обзор современных зарубежных таксономий в области ИБ показал, что наиболее детально проработанной с точки зрения разработчиков является таксономия CWE, а с точки зрения администраторов – реестр CVE. В то же время, из-за сложности таксономий эксперты в области

Таблица 2. Классификация уязвимостей на основе причин их возникновения

Класс	Класс	Группа	Вид
Тип 1. Уязвимости, вызванные дефектами кодирования и проектирования системы	Класс 1. Обработка и представление данных	Группа 1.1. Обработка входных и выходных данных	Вид 1.1.1. Проверка и представление ввода
			Вид 1.1.2. Некорректное кодирование и экранирование вывода
			Вид 1.1.3. Некорректная обработка синтаксически неверных структур
		Группа 1.2. Внутренние трансформации данных	Вид 1.2.1. Ошибки строк
			Вид 1.2.2. Ошибки типов
			Вид 1.2.3. Ошибки представления
			Вид 1.2.4. Числовые ошибки
			Вид 1.2.5. Проблемы структур данных
		Группа 1.3. Ошибки доступа к данным	Вид 1.3.1. Ошибки управления информацией
			Вид 1.3.2. Неверный доступ к индексируемому ресурсу
			Вид 1.3.3. Модификация постоянных данных
		Класс 2. Внутренняя структура и зависимости	Группа 2.1. Злоупотребление API
	Группа 2.2. Инкапсуляция		
	Класс 3. Обработка событий и состояний	Группа 3.1. Время и внутреннее состояние	
		Группа 3.2. Проблемы с логикой функционирования	
		Группа 3.3. Проблемы с обработчиками	Вид 3.3.1. Обработка ошибок и внештатных ситуаций
	Класс 4. Ресурсы и внутренние механизмы системы	Группа 4.1. Механизмы безопасности	
		Группа 4.2. Ошибки каналов и путей	
		Группа 4.3. Ошибки инициализации и очистки	
		Группа 4.4. Проблемы ссылок и псевдонимов	Вид 4.4.1. Проблемы с указателями
		Группа 4.5. Ошибки свойственные определенному типу функционала	Вид 4.5.1. Пользовательский интерфейс Вид 4.5.2. Проблемы WEB
	Класс 5. Внедренные объекты (закладки)	Группа 5.1. Намеренные внедренные объекты	
		Группа 5.2. Внедренные ненамеренно объекты	
	Класс 6. Качество проектирования, реализации, документирования	Группа 6.1. Качество кода	
		Группа 6.2. Нарушение принципов проектирования безопасного ПО	
		Группа 6.3. Неполная или некорректная документация	
	Тип 2. Уязвимости вызванные дефектами конфигурирования и управления системой и ее окружением	Класс 7. Конфигурация	Группа 7.1. Настройки механизмов безопасности
Группа 7.2. Настройки структуры и функционала			
Группа 7.3. Закладки в настройках			
Группа 7.4. Совместимость версий			
Группа 7.5. Качество настроек			
Класс 8. Окружение		Группа 8.1. Среда компиляции и выполнения программного кода	
		Группа 8.2. Прикладное программное обеспечение	
		Группа 8.3. Системное программное обеспечение (гипервизор, ОС, драйвера)	
		Группа 8.4. Аппаратное обеспечение	

анализа кода на практике склоняются к более простой классификации Fortify.


В работе предложены принципы таксономии, ориентированной на дефекты кода и эксплуатации си-

стем и комплексированной с международными таксономиями CWE и Fortify. К достоинству такого подхода следует отнести учет реальных причин уязвимостей, соответствие наиболее удобным международным

практикам классификации и возможность исключения многократного дублирования отдельных позиций, что свойственно академическим общетехническим классификациям.

Таблица 3. Соответствие международным стандартам

Класс, группа, вид	Ссылка на международные стандарты
Класс 1. Обработка и представление данных	Обработка данных (CWE-19)
Вид 1.1.1. Проверка и представление ввода	Некорректная проверка ввода (CWE-20), Проверка и представление ввода (Fortify-1)
Вид 1.1.2. Некорректное кодирование и экранирование вывода	Некорректное кодирование и экранирование вывода (CWE-116)
Вид 1.1.3. Некорректная обработка синтаксически неверных структур	Неправильная обработка синтаксически некорректных конструкций (CWE-228)
Вид 1.2.1. Ошибки строк	Ошибки строк (CWE-133)
Вид 1.2.2. Ошибки типов	Ошибки типов (CWE-136)
Вид 1.2.3. Ошибки представления	Ошибки представления (CWE-137)
Вид 1.2.4. Числовые ошибки	Числовые ошибки (CWE-189)
Вид 1.2.5. Проблемы структур данных	Проблемы структур данных (CWE-461)
Вид 1.3.1. Ошибки управления информацией	Ошибки управления информацией (CWE-199)
Вид 1.3.2. Неверный доступ к индексируемому ресурсу	Неверный доступ к индексируемому ресурсу («Ошибка диапазона») (CWE-118)
Вид 1.3.3. Модификация постоянных данных	Модификация предположительно постоянных данных – MAID (CWE-471)
Группа 2.1. Злоупотребление API	Злоупотребление API (CWE-227, Fortify-2)
Группа 2.2. Инкапсуляция	Недостаточная инкапсуляция (CWE-485), Инкапсуляция (Fortify-7)
Группа 3.1. Время и внутреннее состояние	Время и состояние (CWE-361, Fortify-3)
Группа 3.2. Проблемы с логикой функционирования	Проблемы поведения (CWE-438)
Группа 3.3. Проблемы с обработчиками	Обработчик ошибок (CWE-429)
Вид 3.3.1. Обработка ошибок и внештатных ситуаций	Обработка ошибок (CWE-388, Fortify-5)
Группа 4.1. Механизмы безопасности	Механизмы безопасности (CWE-254, Fortify-4)
Группа 4.2. Ошибки каналов и путей	Ошибки каналов и путей (CWE-417)
Группа 4.3. Ошибки инициализации и очистки	Ошибки инициализации и очистки (CWE-452)
Вид 4.4.1. Проблемы с указателями	Проблемы с указателями (CWE-465)
Вид 4.5.1. Пользовательский интерфейс	Ошибки пользовательского интерфейса (CWE-445)
Вид 4.5.2. Проблемы web	Проблемы web (CWE-442)
Группа 5.1. Намеренно внедренные объекты	Намеренно внедренные объекты (CWE-505)
Группа 5.2. Внедренные ненамеренно объекты	Внедренные ненамеренно объекты (CWE-518)
Группа 6.1. Качество кода	Индикатор плохого качества кода (CWE-398), Качество кода (Fortify-6)
Группа 6.2. Нарушение принципов проектирования безопасного ПО	Нарушение принципов проектирования безопасного ПО (CWE-657)
Класс 7. Конфигурация	Конфигурация (CWE-16)
Класс 8. Окружение	Окружение (CWE-2, Fortify-*)
Группа 8.1. Среда компиляции и выполнения программного кода	Байт-код/объектный модуль (CWE-503)

Предложенный подход может быть полезен для развития отечественной нормативно-методической базы в области безопасности ПО, а также при разработке инструментария анализа безопасности программных ресурсов. 

#### ЛИТЕРАТУРА

1. Багаев Д. С., Коробкин Д. И., Окрачков А. А., Рогозин Е. А. Таксономия угроз качеству функ-

ционирования компьютерных систем // Вестник Воронежского государственного технического университета. 2008, т. 4, № 10, с. 140–142.  
 2. Баранов А. П., Зегжда Д. П., Зегжда П. Д., Ивашико А. М., Корт С. С., Кузьмич В. М., Медведовский И. Д., Семьянов П. В. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996. – 300 с.  
 3. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

4. Емельянов К. И. Таксономия DOS-атак в беспроводных сенсорных сетях // Информационное противодействие угрозам терроризма. 2010, № 14, с. 53–56.

5. Климовский А. А. Таксономия кибератак и ее применение к задаче формирования сценариев их проведения // Труды Института системного анализа Российской академии наук. 2006, т. 27, с. 74–107.

6. Котенко И. В. Таксономии атак на компьютерные системы // Труды СПИИРАН. 2002, т. 2, № 1, с. 196–211.

7. Котенко И. В., Котухов М. М., Марков А. С. и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности АС и ИВС. – СПб: ВУС им. С. М. Буденного, 2000, 190 с.

8. Марков А. С. Анализ атак на сети Novell Netware, основанный на таксономии угроз информационной безопасности // Известия вузов. Приборостроение. 2000, т. 43, № 4, с. 30–34.

9. Марков А. С. Исследование дефектов операционной системы Windows // Известия вузов. Приборостроение. 2000, т. 43, № 6, с. 46–50.

10. Марков А. С., Фадин А. А., Цирлов В. Л. Систематика дефектов и уязвимостей программного обеспечения // Сборник трудов Второй всероссийской НТК «Безопасные информационные технологии» / под. ред. В. А. Матвева. – М: НИИ РЛ МГТУ им. Н. Э. Баумана, 2011, с. 83–87.

11. Мукминов В. А., Войнов Ю. В. Методика оценки реального уровня защищенности АСУ в условиях компьютерных атак // Известия Института инженерной физики. 2013, т. 1, № 27, с. 80–85.

12. Черешкин Д. С., Кононов А. А. Тищенко Д. В. Принципы таксономии угроз безопасности информационных систем // Вестник РФФИ, № 3(17), 1999, с. 68–72.



**ЗАО «НПО «Эшелон»**

107023, Москва,  
ул. Электровзводская, д. 24, стр. 1,  
тел./факс: (495) 645-38-09, 645-38-10,

e-mail: mail@npo-echelon.ru,  
http://www.npo-echelon.ru