



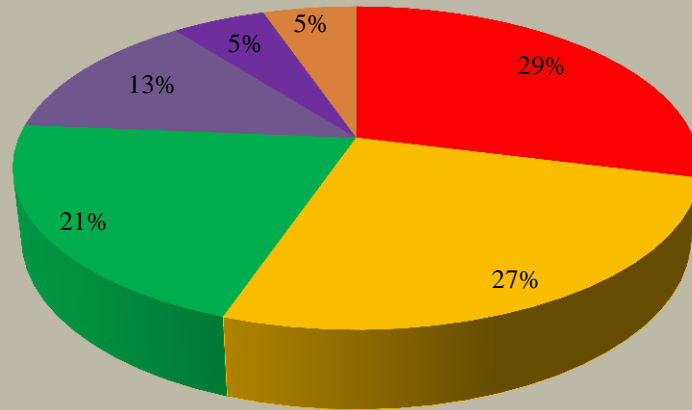
**Подходы к обеспечению безопасности  
программного обеспечения.  
Направления работ по уменьшению уязвимостей**

**ЛЮТИКОВ Виталий Сергеевич  
начальник управления ФСТЭК России**

# УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

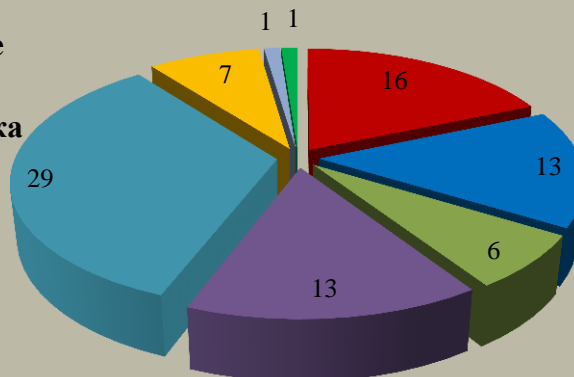
## Распределение уязвимостей программных продуктов (2014 г.)

- MS Windows и её компоненты
- Android
- Acrobat Reader
- MS Internet Explorer
- Flash Player
- MS Office

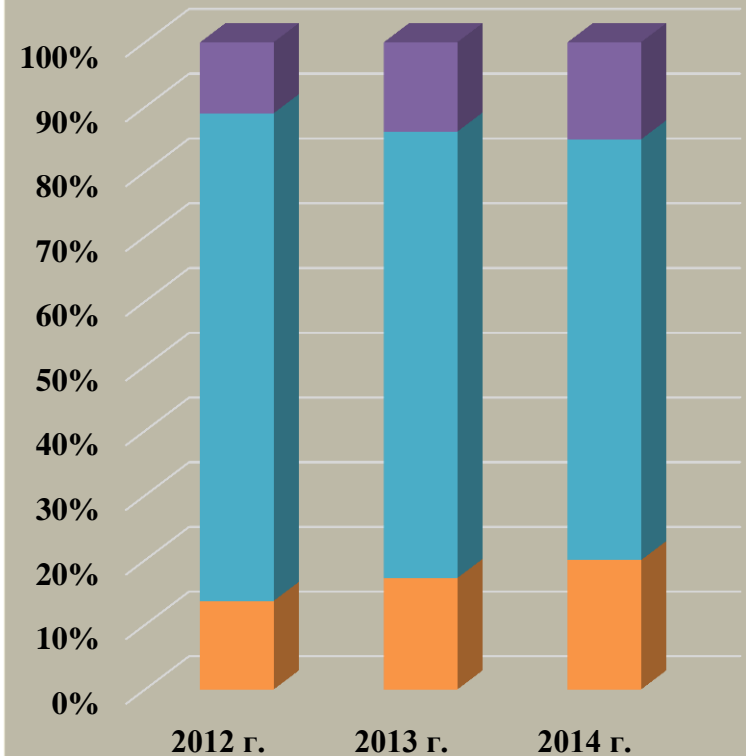


## Сферы деятельности, наиболее подверженные эксплуатации уязвимостей (2014 г.)

- Государственный сектор
- Кредитно-финансовые организации
- Транспорт и энергетика

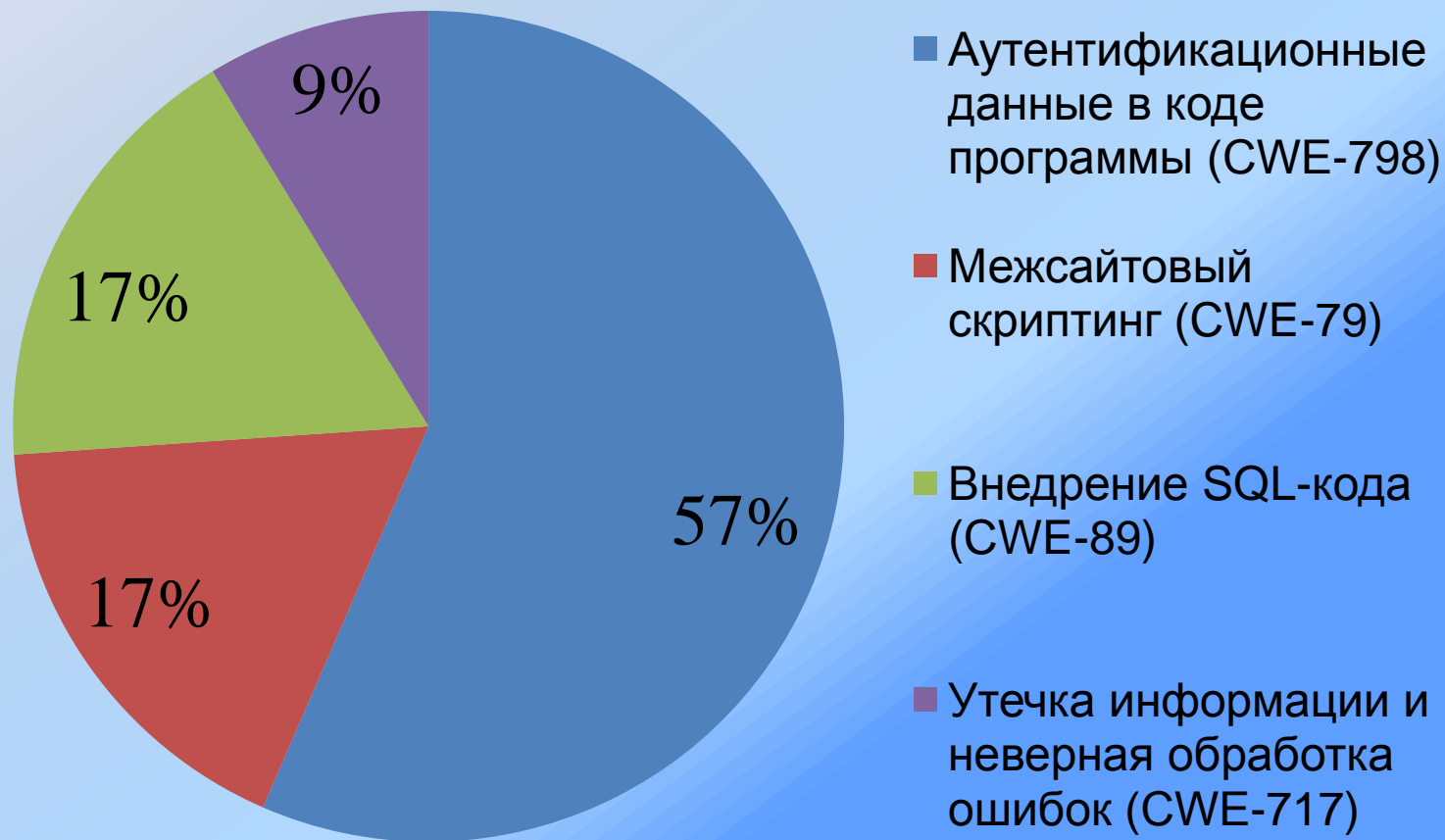


## Динамика роста количества уязвимостей программного обеспечения



- не критические
- умеренные
- критические

# АКТУАЛЬНОСТЬ: РАСПРЕДЕЛЕНИЕ ДЕФЕКТОВ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ТИПАМ



## Непреднамеренные

- недостаток мотивации разработчиков
- отсутствие у разработчиков необходимых знаний
- отсутствие у разработчиков необходимых технологий

## Преднамеренные

- заказ иностранных спецслужб
- «вредительство»
- ...

## В ходе разработки и производства

- ошибки при проектировании и реализации программного и аппаратного обеспечения
- ошибки при проектировании и создании информационной системы

## В ходе эксплуатации

- неумышленные действия пользователей
- несанкционированное внедрение вредоносных программ
- сбои в работе программного и аппаратного обеспечения
- преднамеренные изменения программного обеспечения с целью внесения уязвимостей
- неправильные настройки программного обеспечения, протоколов и служб
- ...

**Microsoft  
SDL**

**Cisco SDL**

**OpenSAMM**

**OWASP  
CLASP**

**ISO 27034**

**...**

# МЕРЫ, ПРИМЕНЯЕМЫЕ ФСТЭК РОССИИ. ЭТАП РАЗРАБОТКИ И ПРОИЗВОДСТВА

## *Оценка программного обеспечения*

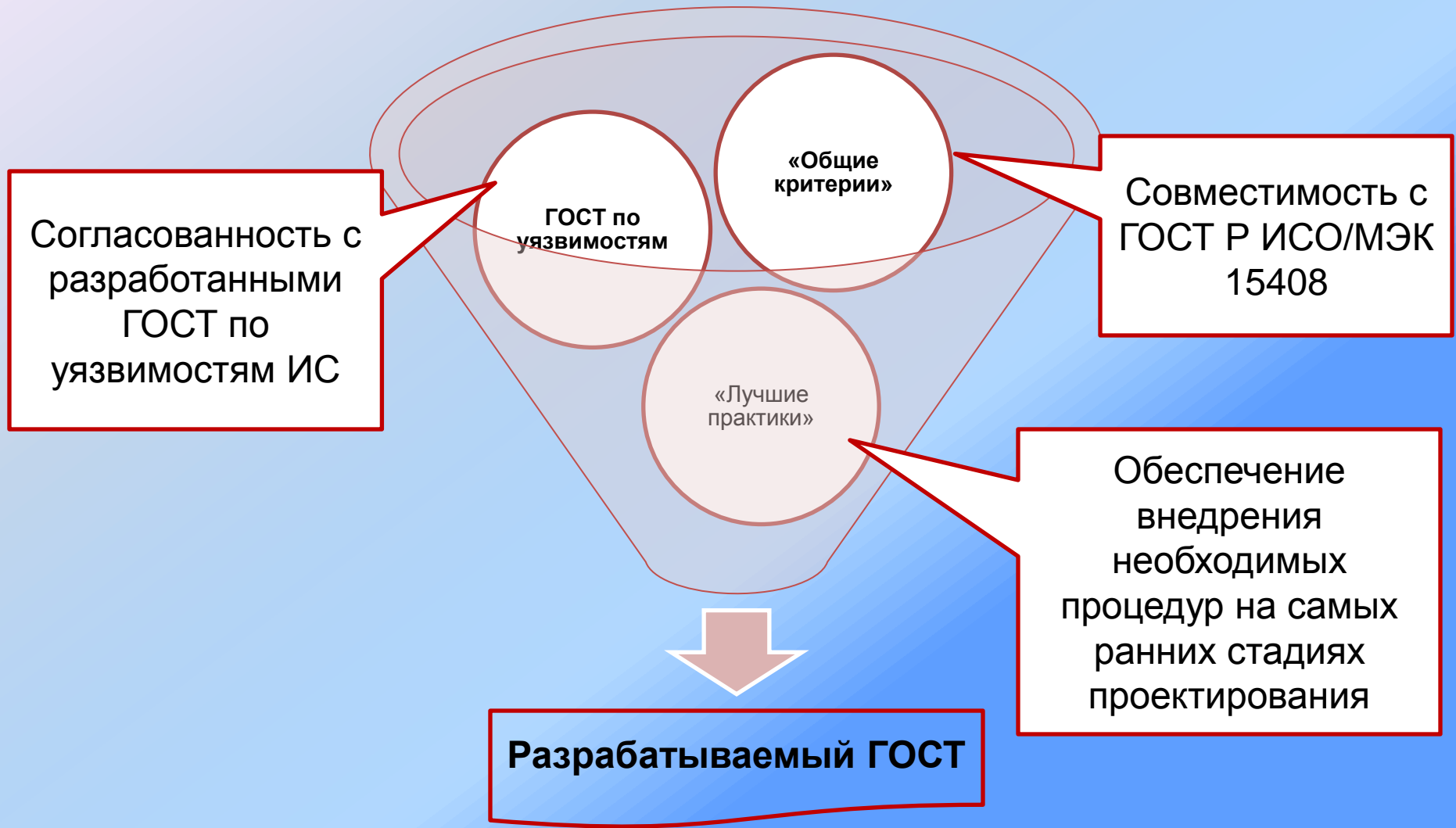


1. Новые требования к СЗИ (требование доверия AVA\_VLA)
2. ГОСТ по описанию и выявлению уязвимостей
3. Рекомендации по проведению обновления ПО

## *Оценка процесса разработки*



ГОСТ Р «Защита информации. Безопасная разработка программного обеспечения. Общие положения»





# МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

## Документы

ГОСТ Р ИСО/МЭК 15408

ГОСТ Р ИСО/МЭК 18045

ГОСТ Р ИСО/МЭК 27001

## Методологии

Microsoft SDL

Cisco SDL

OWASP CLASP

## Предлагаемая номенклатура мер:

1. Меры, применяемые на стадии проектирования ПО
2. Меры, применяемые на стадии разработки ПО
3. Меры, применяемые на стадии тестирования ПО
4. Меры, применяемые на стадии передачи ПО потребителю
5. Меры, применяемые на стадии сопровождения и модернизации ПО
6. *Обучение сотрудников*
7. *Защита инфраструктуры разработки ПО*
8. *Управление конфигурациями ПО*

# ГОСТ Р «ЗАЩИТА ИНФОРМАЦИИ. БЕЗОПАСНАЯ РАЗРАБОТКА <sup>10</sup> ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ОБЩИЕ ПОЛОЖЕНИЯ»

**Начало  
разработки:  
апрель 2013**

**Первая  
редакция:  
май 2014**

**Обсуждения:  
сентябрь-  
ноябрь 2014**

**Окончательная  
редакция:  
апрель 2015**

**Передача в  
Росстандарт:  
конец 2015**

# МЕРЫ, ПРИМЕНЯЕМЫЕ ФСТЭК РОССИИ. ЭТАП ЭКСПЛУАТАЦИИ

## НОРМАТИВНО-ПРАВОВАЯ ОСНОВА АНАЛИЗА УЯЗВИМОСТЕЙ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

«Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

«Об утверждении Составов и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 14 марта 2014 г. № 31

«Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

## НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ПО ВЫЯВЛЕНИЮ УЯЗВИМОСТЕЙ

ГОСТ Р «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»

ГОСТ Р «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»

ГОСТ Р «Защита информации. Уязвимости информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей информационных систем»

# ЗАРУБЕЖНЫЕ СИСТЕМЫ КЛАССИФИКАЦИИ УЯЗВИМОСТЕЙ (БАЗЫ ДАННЫХ УЯЗВИМОСТЕЙ)



Sponsored by  
DHS National Cyber Security Division/US-CERT

**NIST**  
National Institute of  
Standards and Technology

## National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities      Checklists      800-53/800-53A      Pro

Home      SCAP      SCAP Validated Tools

### Mission and Overview

#### National Vulnerability Database Version 2.2


NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

NVD is the U.S. government repository of standards based vulnerability management data representing databases of security checklists, security related software flaws, misconfigurations, products, and other information.

#### Federal Desktop Core Configuration settings (FDCC)

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

#### NVD Primary Resources



## CVE LIST

HOME > CVE LIST > DOWNLOAD CVE

### About CVE

Terminology  
Documents  
FAQs

### CVE List

CVE-ID Syntax Change  
About CVE Identifiers  
Search CVE  
Search NVD  
Updates & RSS Feeds  
Request a CVE-ID

### Download CVE

**CVE downloads data last generated: 2014-04-16**

CVE is available for download in several formats: CVRF, XML, etc.

**NOTE:** To save compressed files, you may need to right-click and save as.

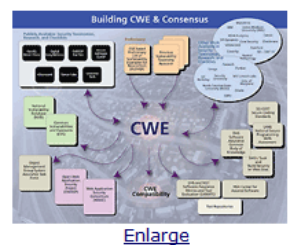
### Download Formats



## Common Weakness Enumeration

A Community-Developed Dictionary of Software Weakness Types

- CWE List
- Full Dictionary View
- Development View
- Research View
- Reports
- Mapping & Navigation
- About
- Sources
- Process
- Documents
- FAQs
- Community



CWE™ International is a community of security researchers and operational systems as well as...



## SecurityFocus™

### Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation >](#)

Vulnerabilities (Page 1 of 2056)

Vendor:

Title:

Version:

Search by CVE

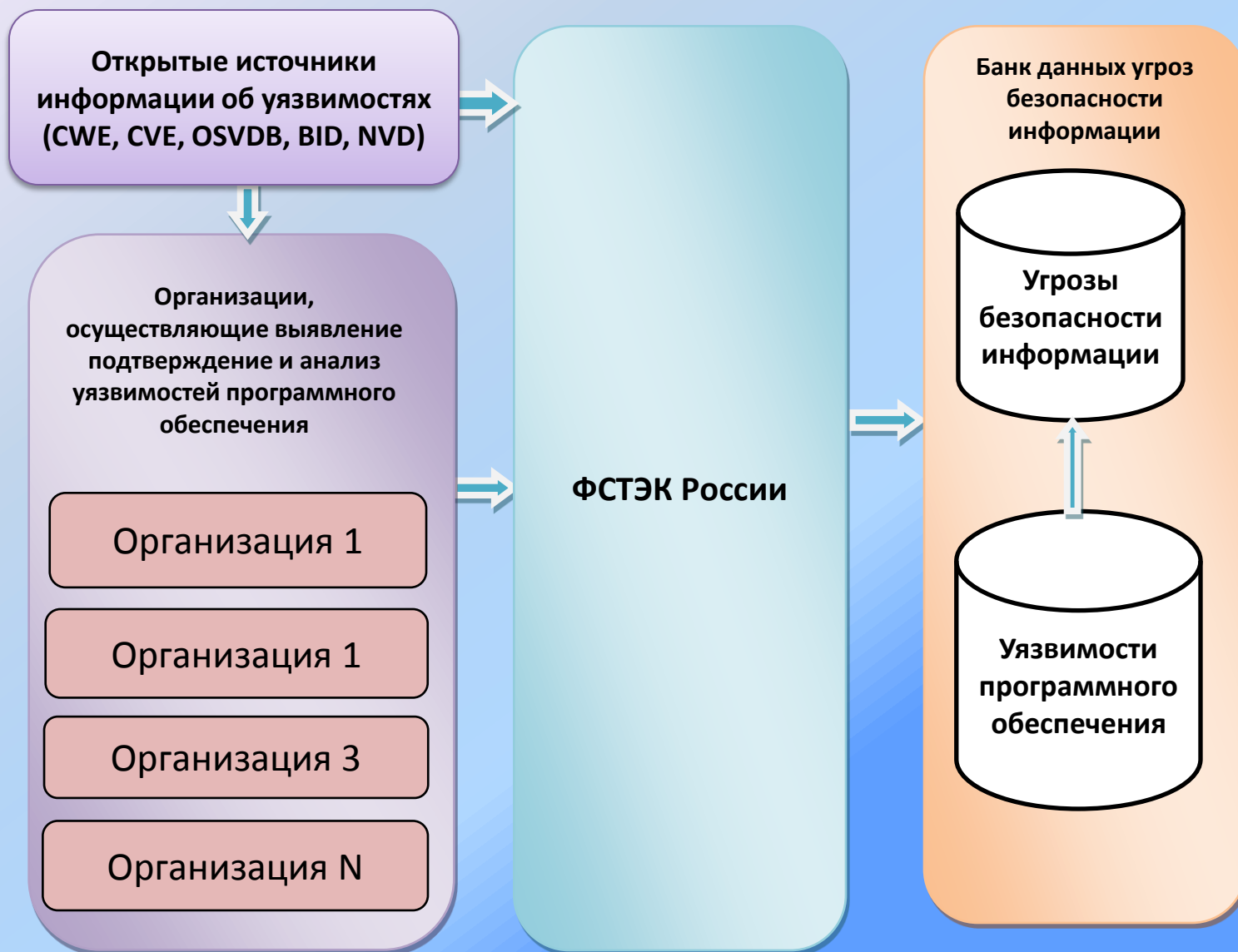
CVE:

---

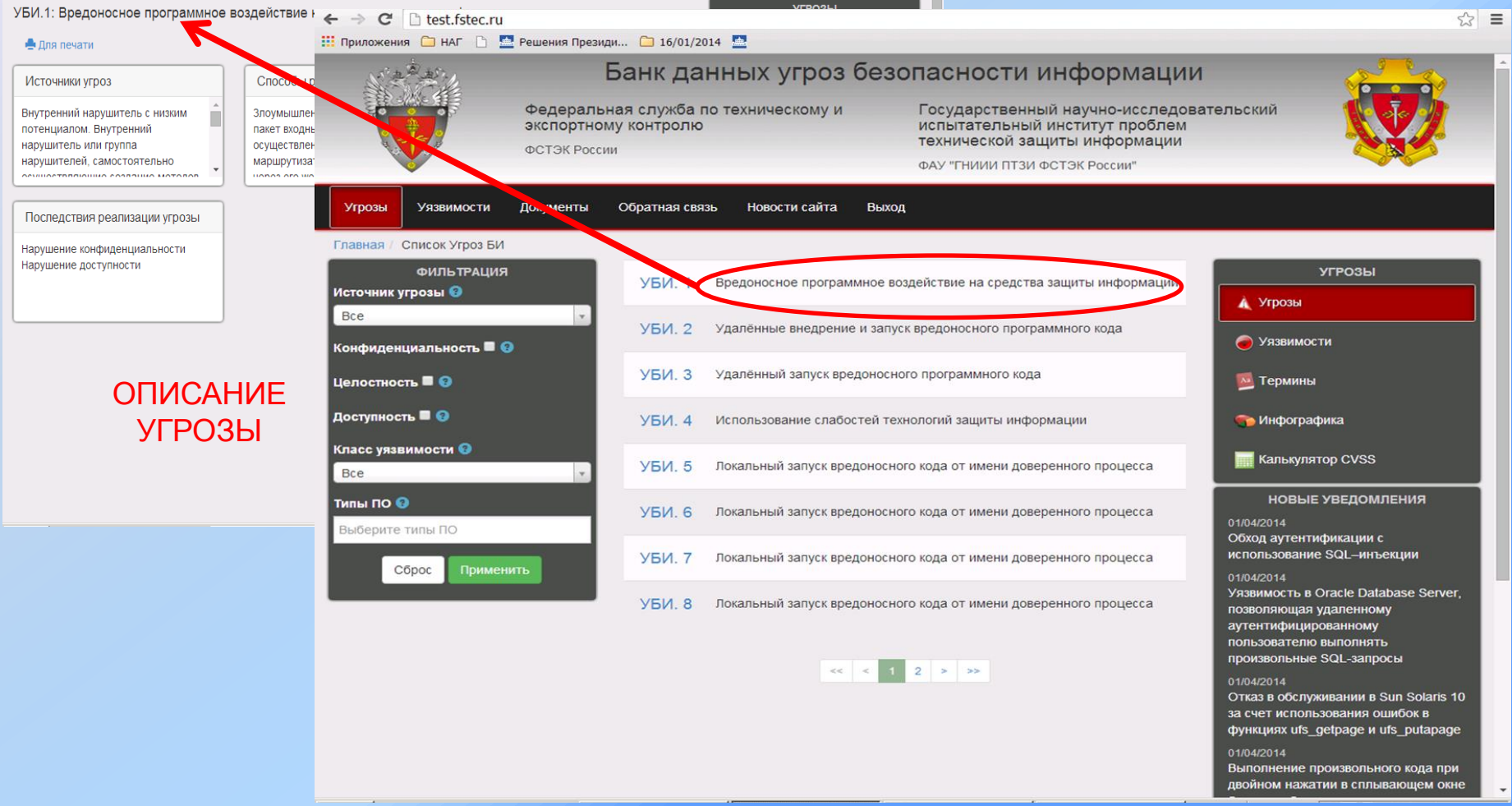
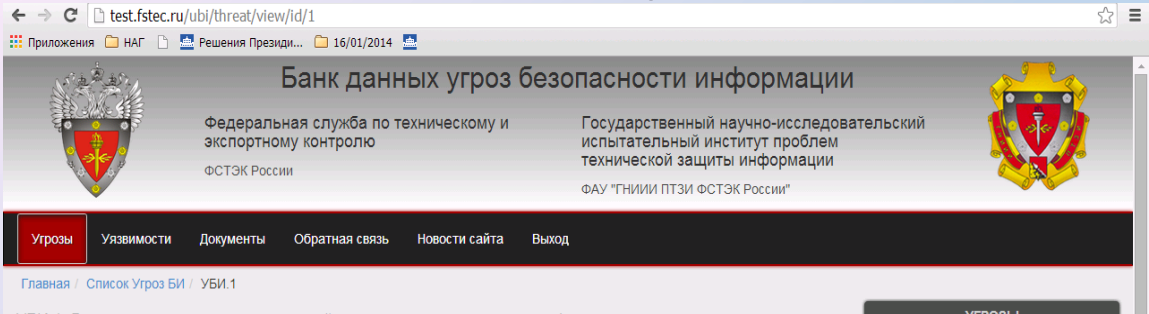
#### Spagent Ruby Gem Remote Command Injection Vulnerability

2014-04-21  
<http://www.securityfocus.com/bid/66935>

# БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СОЗДАВАЕМЫЙ ФСТЭК РОССИИ



# WEB-ИНТЕРФЕЙС ОТКРЫТОГО СЕГМЕНТА БДУ (ПОДСИСТЕМА «УГРОЗЫ»)



ОПИСАНИЕ  
УГРОЗЫ

# WEB-ИНТЕРФЕЙС ОТКРЫТОГО СЕГМЕНТА БДУ (ПОДСИСТЕМА «УЯЗВИМОСТИ»)

test.fstec.ru/ubi/vul/view/id/1030#group-all

Приложения НАГ Решения Президи... 16/01/2014

## Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации  
ФАУ "ГНИИИ ПТЗИ ФСТЭК России"

Угрозы **Уязвимости** Документы Обратная связь Новости сайта Выход

Главная / Список уязвимостей / 2014-001020

### 2014-001020: Выполнение произвольного кода при двойном нажатии в сплывающем окне браузера Opera

Основная информация Программное обеспечение

Описание уязвимости

Браузер содержит уязвимость, связанную с использованием двойных кликов на всплывающих окнах. Это позволяет злоумышленнику создать

Версия ПО

11.65

Тип ошибки

Недостаточная проверка вводимых данных

Дата выявления

14.06.2012

ОПИСАНИЕ  
УЯЗВИМОСТИ

test.fstec.ru/ubi/vul

## Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации  
ФАУ "ГНИИИ ПТЗИ ФСТЭК России"

Угрозы **Уязвимости** Документы Обратная связь Новости сайта Выход

Главная / Список уязвимостей

### ФИЛЬТРАЦИЯ

Диапазон дат: с по

Производитель: Выберите производителя

Тип ПО: Все

Программное обеспечение: Выберите программное обеспечение

Платформа: Все

Версия: Выберите версию

Класс уязвимости: Все

Уровень опасности: Все

Подтвержденные: Все

Платформа ОС: Все

ID	Описание	Дата
2014-001017	Обход аутентификации с использованием SQL-инъекции D-Link Встроенное программное обеспечение маршрутизатора D-Link DSR-500 1.06	01/04/2014
2014-001018	Уязвимость в Oracle Database Server, позволяющая удаленному аутентифицированному пользователю выполнять произвольные SQL-запросы Oracle Oracle Database 11.2.0.3	01/04/2014
2014-001019	Отказ в обслуживании в Sun Solaris 10 за счет использования ошибок в функциях ufs_getpage и ufs_putpage Oracle Solaris 10	01/04/2014
2014-001020	Выполнение произвольного кода при двойном нажатии в сплывающем окне браузера Opera Opera Software ASA Opera 11.65	01/04/2014
2014-001021	Создание новой или получение доступа к имеющейся базе данных в MySQL за счет использования чувствительности к регистру файловых систем MySQL AB MySQL 5.1.12	01/04/2014
2014-001022	Выполнение произвольного программного кода программным обеспечением, использующим библиотеку Libxml2 XMLSoft Libxml2 2.7.7	01/04/2014
2014-001023	Переполнение буфера в памяти в PHP Открытый проект PHP 5 <5.3.14; 5.4.x - 5.4.4	01/04/2014

УГРОЗЫ

- Угрозы
- Уязвимости**
- Термины
- Инфографика
- Калькулятор CVSS

НОВЫЕ УВЕДОМЛЕНИЯ

- 01/04/2014 Обход аутентификации с использованием SQL-инъекции
- 01/04/2014 Уязвимость в Oracle Database Server, позволяющая удаленному аутентифицированному пользователю выполнять произвольные SQL-запросы
- 01/04/2014 Отказ в обслуживании в Sun Solaris 10 за счет использования ошибок в функциях ufs\_getpage и ufs\_putpage
- 01/04/2014 Выполнение произвольного кода при двойном нажатии в сплывающем окне



**Подходы к обеспечению безопасности  
программного обеспечения.  
Направления работ по уменьшению уязвимостей**

**ЛЮТИКОВ Виталий Сергеевич  
начальник управления ФСТЭК России**