



**РЕЗУЛЬТАТЫ АНАЛИЗА УГРОЗ БЕЗОПАСНОСТИ  
ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ  
(АВТОМАТИЗИРОВАННЫХ) СИСТЕМАХ**

**Начальник отдела  
управления ФСТЭК России  
Гефнер Ирина Сергеевна**

# Нормативное правовое обеспечение, в котором установлена необходимость определения угроз безопасности информации

Федеральный закон  
от 26 июля 2017 г.  
№ 187-ФЗ

«О безопасности критической информации  
инфраструктуры Российской Федерации»

УТВЕРЖДЕНЫ  
приказом ФСТЭК России  
от 25 декабря 2017 г. № 239



Требования  
по обеспечению безопасности  
значимых объектов критической  
информационной инфраструктуры  
Российской Федерации

Федеральный закон  
от 27 июля 2006 г.  
№ 149-ФЗ

«О информации, информационных  
технологиях и о защите информации»

УТВЕРЖДЕНЫ  
приказом ФСТЭК России  
от 11 февраля 2013 г. № 17



Требований о защите информации,  
не составляющей государственную  
тайну, содержащейся в  
государственных информационных  
системах

Федеральный закон  
от 27 июля 2006 г.  
№ 152-ФЗ  
«О персональных данных»

УТВЕРЖДЕНЫ  
приказом ФСТЭК России  
от 18 февраля 2013 г. № 21



Состав и содержание  
организационных и технических  
мер по обеспечению безопасности  
персональных данных при их  
обработке в информационных  
системах персональных данных

Анализ угроз безопасности информации и  
разработка модели угроз безопасности  
информации или ее уточнение

Меры по обеспечению безопасности  
информации должны быть направлены на  
нейтрализацию актуальных угроз безопасности  
информации

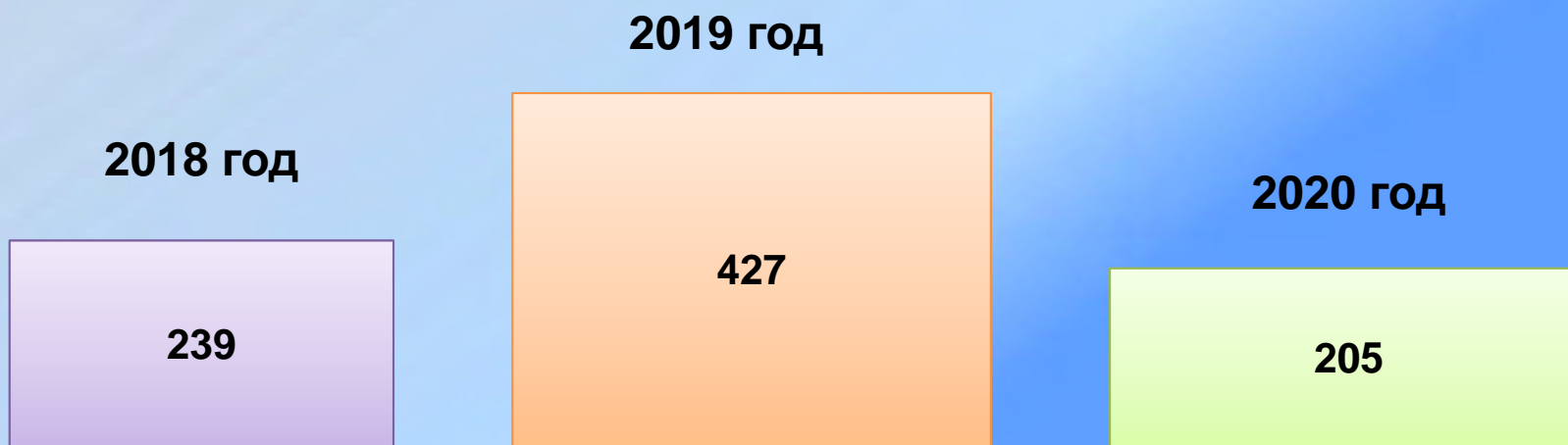


## Статистика по количеству моделей угроз безопасности информации, которые поступают на согласование во ФСТЭК России

О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации

*утверждена постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676  
(в редакции постановления Правительства Российской Федерации от 11 мая 2017 г. № 555)*

Количество рассмотренных  
ФСТЭК России моделей угроз безопасности информации  
государственных информационных систем, информационных  
за **2018, 2019 и 2020** годы



# Цель анализа угроз безопасности информации

## ОБЪЕКТЫ АНАЛИЗА УГРОЗ

Информационные  
системы

Автоматизированные  
системы управления

Информационно-  
телекоммуникационные  
сети

Анализ угроз  
безопасности информации



## ЦЕЛИ

Выявление источников  
угроз безопасности  
информации и их  
потенциала

Анализ возможных  
уязвимостей

Определение возможных  
способов (сценариев)  
реализации угроз

Оценка возможных  
последствий от  
реализации

## Этап определения угроз безопасности информации в информационных (автоматизированных) системах

Построение системы защиты информации

Классификация

Моделирование угроз

Проектирование системы защиты

Внедрение мер защиты информации

Разработка документации

Оценка защищенности

Эксплуатация

1. Описание архитектуры

2. Описание угроз

2.1. Описание нарушителей

2.2. Потенциальные уязвимости

2.3. Способы реализации угроз

2.4. Последствия от реализации угроз

Проведен анализ моделей угроз более 500 государственных и региональных информационных систем

# Описание процесса моделирования угроз безопасности информации

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных  
(утверждена ФСТЭК России 14 февраля 2008 г.)

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных  
(утверждена ФСТЭК России 14 февраля 2008 г.)

Модель угроз безопасности информации информационной (автоматизированной) системы

Описание системы

Описание возможностей нарушителей (модель нарушителя)

Перечень вероятных угроз

Определение актуальности угроз

Перечень актуальных угроз

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации  
ВАУ 474554 ПТЗи ФСТЭК России

Угрозы Уязвимости Документы Термины Обратная связь Обязанности Участники ФСТЭК России

Главная Список угроз

Фильтрация  
Контактный поиск по ключевым словам

Источники угроз

Доступное взаимодействие

Последствия реализации угрозы

Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

Сброс Применить

Выводить по: 10, 20, 50, 100

Идентификатор	Описание угрозы
УБИ_001	Угроза автоматического распространения вредоносного кода в под-системе.
УБИ_002	Угроза взлома данных, передаваемых в под-системе.
УБИ_003	Угроза анализа криптографически зашифрованных и их реализации.
УБИ_004	Угроза аппаратного сброса пароля BIOS.
УБИ_005	Угроза внедрения вредоносного кода в BIOS.
УБИ_006	Угроза внедрения кода ядра данных.
УБИ_007	Угроза воздействия на программы с высоким приоритетом.

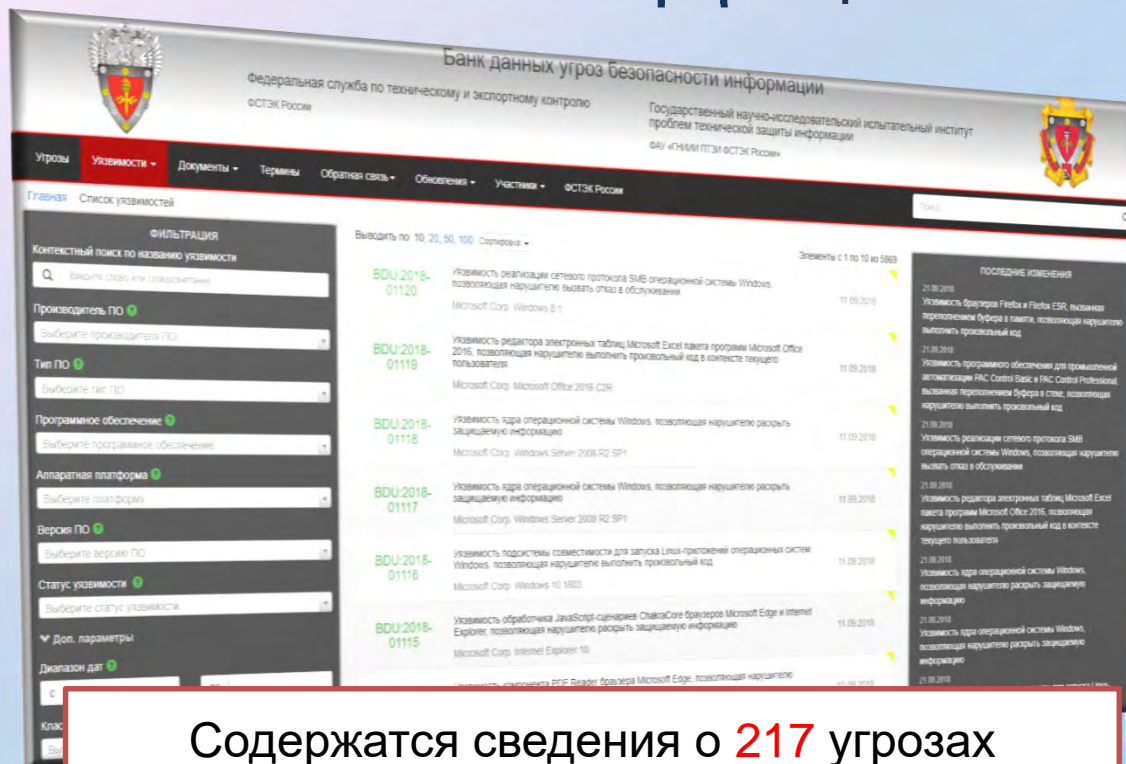
Элементы с 1 по 10 из 216

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

- 11.11.2018 УБИ\_216 Угроза получения несанкционированного доступа к приложениям, установленным на бэкап-сервере.
- 01.08.2018 УБИ\_215 Угроза несанкционированного доступа к системе при помощи сторонних сервисов.
- 01.11.2017 УБИ\_214 Угроза несанкционированного выхищения и раскрытия информации информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации.
- 08.02.2017 УБИ\_213 Угроза обхода многофакторной аутентификации.
- 01.02.2016 УБИ\_212 Угроза перехвата управления информационной системой.
- 08.02.2016

Банк данных угроз безопасности информации ФСТЭК России  
bdu.fstec.ru

# Банк данных угроз безопасности информации ФСТЭК России



Содержатся сведения о **217** угрозах

Содержит сведения о более **26 800**  
уязвимостей

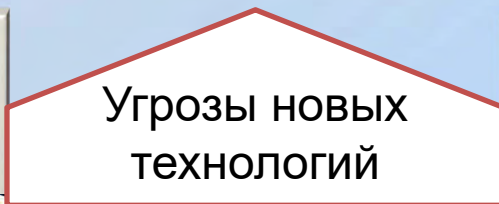
Еженедельное наполнение сведениями об  
уязвимостях (сейчас в среднем **100**  
уязвимостей/неделя)



# Угрозы безопасности информации, содержащиеся в банке данных угроз безопасности информации



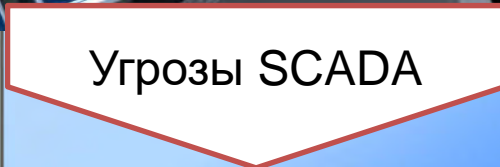
Угрозы АСУ ТП



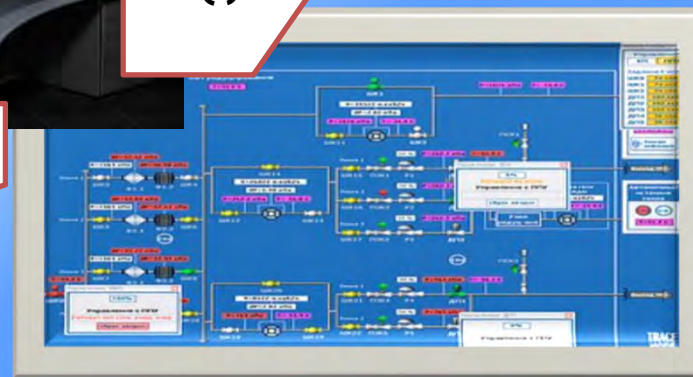
Угрозы новых технологий



Угрозы ИС



Угрозы SCADA



Реализации более **55%** угроз безопасности информации не требует высоких умений и навыков

# Результаты анализа инфраструктуры информационных (автоматизированных) систем



# Развитие информационной инфраструктуры информационных (автоматизированных) систем



## Угрозы безопасности информации, связанные с размещением информационных (автоматизированных) в ЦОД



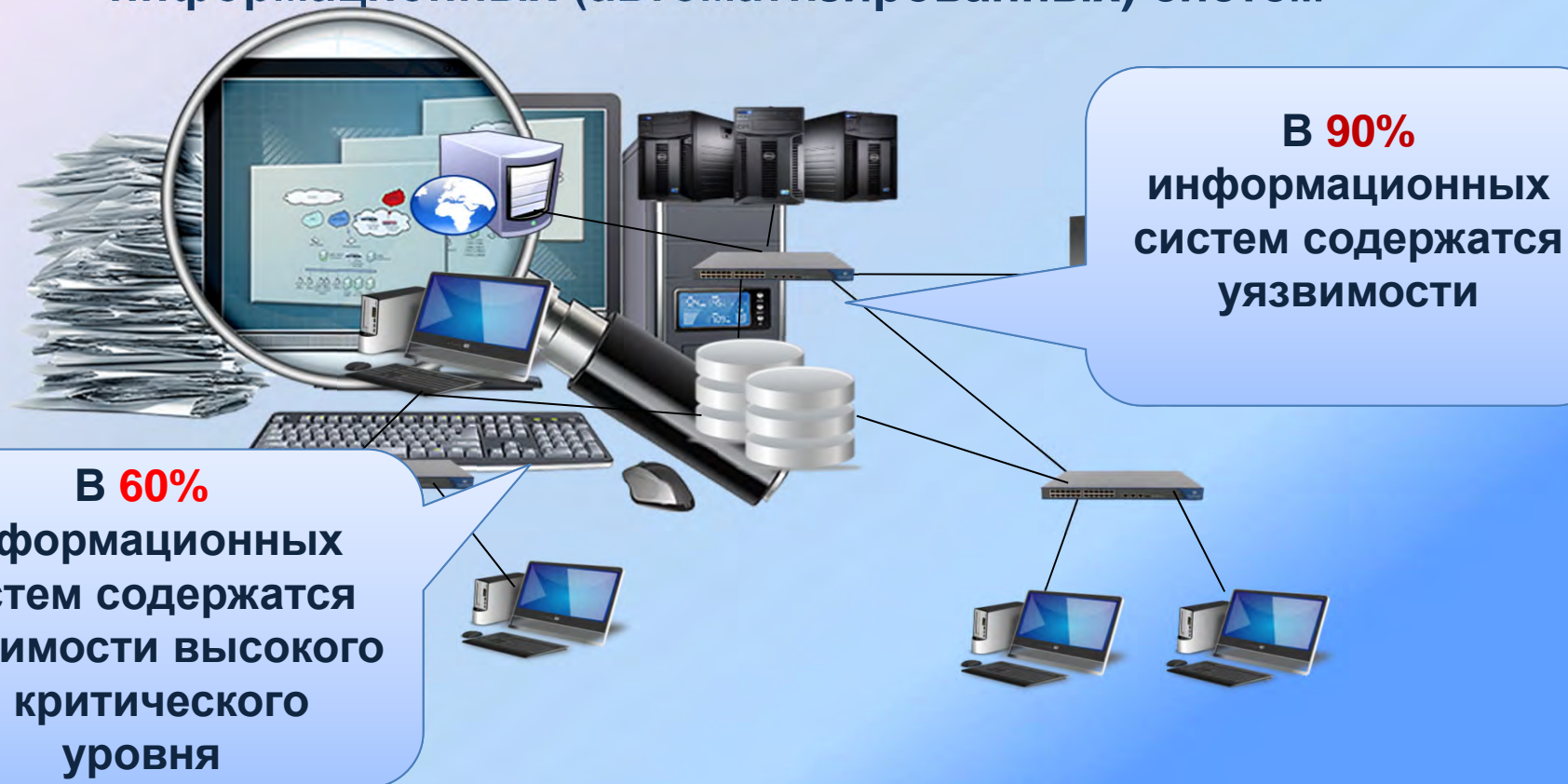
Отсутствие распределения обязанностей между владельцами системы и ЦОДа

Угрозы, актуальные для системы не учтены в модели угроз ЦОДа

Угрозы, связанные с применением технологий виртуализации

Угрозы, связанные с отсутствием мер защиты информации на АРМ администраторов ЦОД

## Угрозы безопасности информации, связанные с уязвимостями информационных (автоматизированных) систем



Внедрение вредоносного ПО



Приведение системы в «отказ в обслуживании»



Утечка, уничтожение или подмена данных

# Классификация уязвимостей информационных (автоматизированных) систем

## • Область происхождения уязвимости

Уязвимости кода

Уязвимости конфигурации

Уязвимости архитектуры

Организационные уязвимости

Многофакторные уязвимости

## • Место возникновения (проявления) уязвимости ИС

в общесистемном (общем) ПО

в прикладном ПО

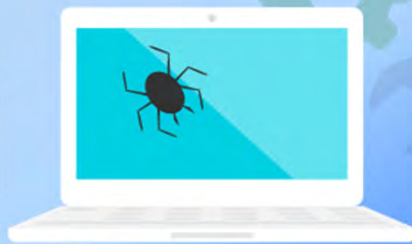
в специальном ПО

в технических средствах

в портативных технических средствах

в сетевом оборудовании

в средствах защиты информации



# Автоматизация поиска сведений об уязвимостях в информационных (автоматизированных) системах

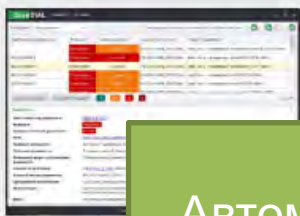
Программа **ScanOVAL** для Linux для автоматизированных проверок наличия уязвимостей программного обеспечения

Программа ScanOVAL для Linux предназначена для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Linux.

В настоящее время проводится опытная эксплуатация программы ScanOVAL для Linux.

Замечания и предложения по работе программы ScanOVAL для Linux просьба направлять в форме обратной связи или посредством электронной почты.

Перед использованием программы, пожалуйста, ознакомьтесь с настоящим Лицензионным соглашением с конечным пользователем программы ScanOVAL для Linux, а также Руководством оператора.



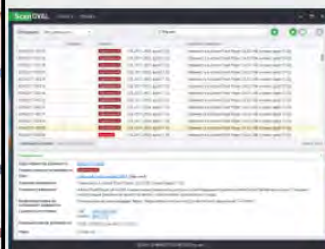
Программа ScanOVAL для Linux обеспечивает выполнение следующих основных функций:

- загрузка XML-файлов с OVAL-описаниями уязвимостей в соответствии со стандартом «The OVAL Language Specification»

Программа **ScanOVAL** для автоматизированных проверок наличия уязвимостей программного обеспечения

Программа ScanOVAL предназначена для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Microsoft Windows.

Перед использованием программы, пожалуйста, ознакомьтесь с настоящим Лицензионным соглашением с конечным пользователем программы ScanOVAL, а также Руководством оператора.



Программа ScanOVAL обеспечивает выполнение следующих основных функций:

- загрузка XML-файлов с OVAL-описаниями уязвимостей, выполненными в соответствии со стандартом «The OVAL Language Specification» версии не ниже 5.10.1;
- обнаружение на основании обработки данных, представленных в XML-файлах, уязвимостей программного обеспечения, установленного на локальной ПЭВМ, работающей под управлением операционной системы семейства Microsoft Windows.

Для работы программы ScanOVAL аппаратная конфигурация компьютера должна соответствовать следующим минимальным требованиям:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или

системы) оперативной

или более поздней версии.

## Автоматизированная проверка уязвимостей ПО, работающего под управлением ОС Windows и ОС Linux

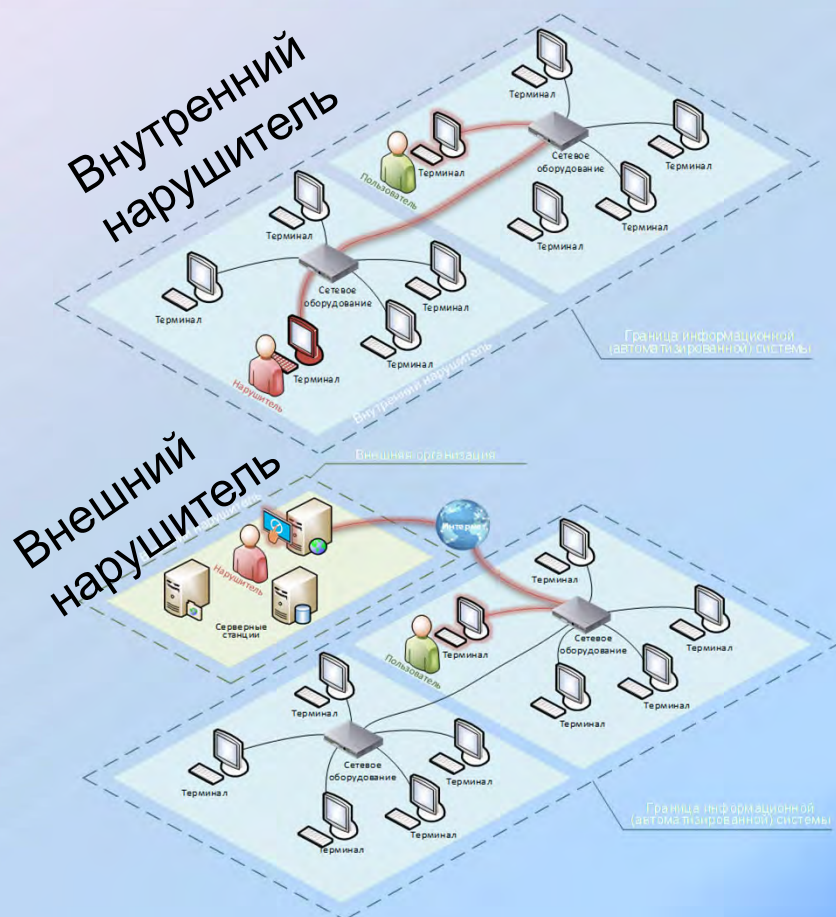
Идентификатор уязвимости	Уровень опасности	Ссылка	Описание
BDU-2014-00004	Высокий	CVE-2014-1757; MS14-017	Уязвимость конвертера форматов файлов Microsoft Office (MS14-017)
BDU-2014-00003	Критический	CVE-2014-1806; MS14-026	Уязвимость TypeFilterLevel (MS14-026)
BDU-2014-00184	Высокий	CVE-2014-0516; arip14-14	Уязвимость в Adobe AIR SDK до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00271	Высокий	CVE-2014-0518; arip14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00364	Средний	CVE-2014-1509; MS14-034	Уязвимость ASLR в MSCOMCTL (MS14-034)
BDU-2014-00280	Высокий	CVE-2014-0919; arip14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00266	Критическая	CVE-2014-0910; arip14-14	Переопределение кучи в Adobe Flash Player 12.0.0.17 (arip14-14)
BDU-2014-00363	Средний	CVE-2014-1808; MS14-023	Уязвимость повторного использования маркеров (MS14-023)
BDU-2014-00278	Высокий	CVE-2014-0517; arip14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00362	Высокий	CVE-2014-1734; MS14-023	Уязвимость Microsoft Office, связанная с проверкой грамматики...
BDU-2014-00279	Высокий	CVE-2014-0520; arip14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00167	Высокий	CVE-2014-1741; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00199	Высокий	CVE-2014-1740; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00212	Высокий	CVE-2014-1742; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00330	Высокий	CVE-2014-1743; stable-channel-up	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update_20)
BDU-2014-00332	Высокий	CVE-2014-1745; stable-channel-up	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update_20)
BDU-2014-00195	Высокий	CVE-2014-1744; stable-channel-up	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update_20)
BDU-2014-00137	Высокий	CVE-2014-1744; stable-channel-up	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update_20)
BDU-2014-00155	Средний	CVE-2014-1740; stable-channel-up	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update_20)
BDU-2014-00157	Средний	CVE-2014-1740; stable-channel-up	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update_20)
BDU-2014-00292	Низкий	CVE-2014-1013; MS14-022	Уязвимость Web Applications, связанная с содержанием страниц...
BDU-2014-00574	Высокий	CVE-2014-4247; cveid2014-19729	Неопределенная уязвимость в Oracle Java SE 6u75, 7u60, и 8u5...
BDU-2014-00542	Средний	CVE-2014-4265; cveid2014-19729	Неопределенная уязвимость в Oracle Java SE 6u75, 7u60, и 8u5...
BDU-2014-00540	Высокий	CVE-2014-4219; cveid2014-19729	Неопределенная уязвимость в Oracle Java SE 6u75, 7u60, и 8u5...

Профиль	Уязвимости
Начало/завершение сканирования	26.09.2018 12:21:44 / 26.09.2018 12:26:08
Формирование отчета	26.09.2018 12:28:51

Уровень опасности	Найдено	Всего
Критический	1	773
Высокий	3	1475
Средний	2	1053
Низкий	0	20
<b>Всего</b>	<b>6</b>	<b>3321</b>

## Формирование отчета по результатам анализа

# Источники реализации угроз безопасности информации в информационных (автоматизированных) системах



Виды нарушителя

Мотивация нарушителя

Уровень возможность

Нарушитель, обладающий высокими возможностями (потенциалом)

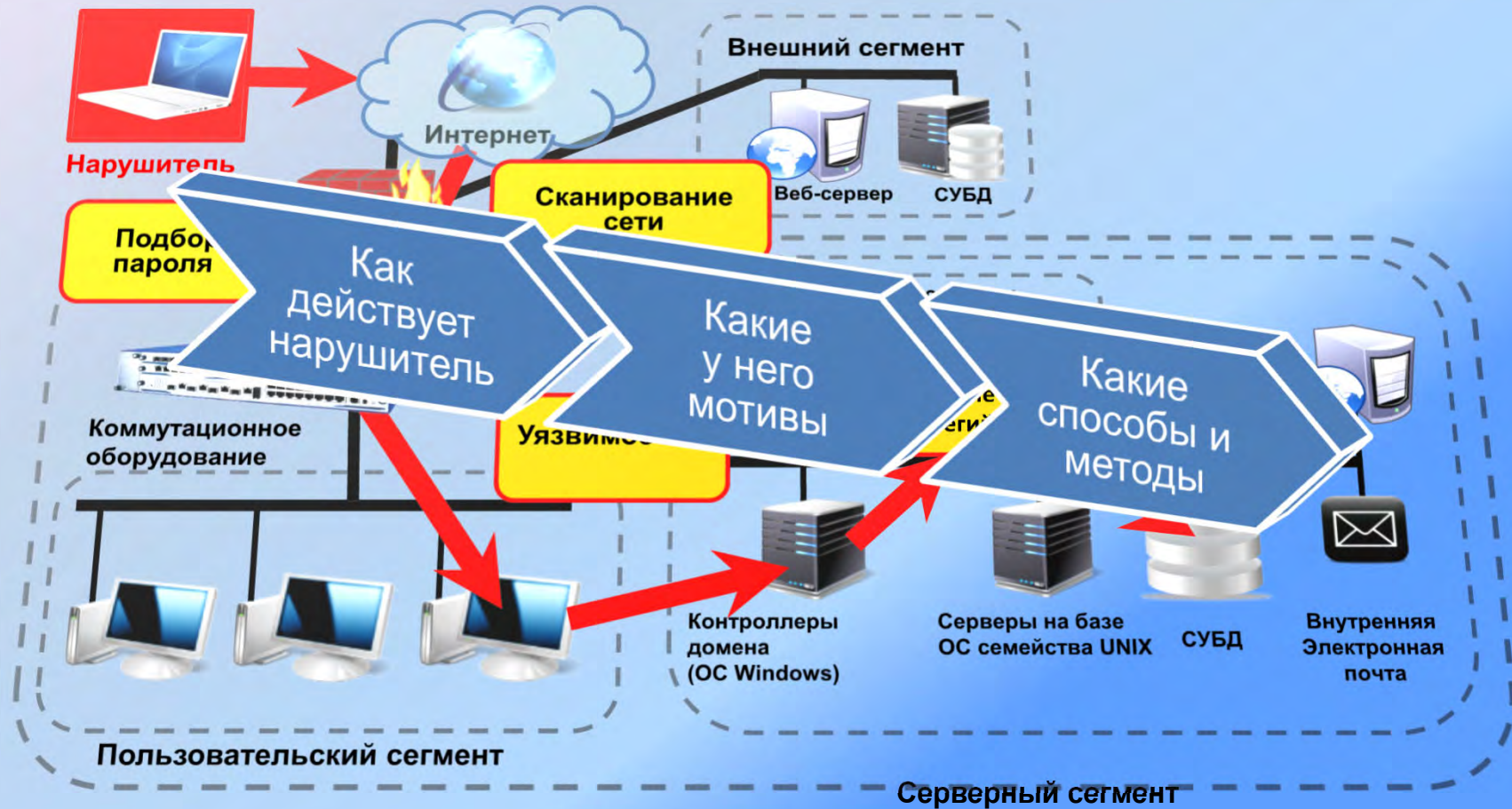
Нарушитель, обладающий средними возможностями (потенциалом)

Нарушитель, обладающий базовыми повышенными возможностями (потенциалом)

Нарушитель, обладающий базовыми возможностями (потенциалом)



# Целенаправленные угрозы безопасности информации в информационных (автоматизированных) системах



# Оценка сценариев реализации угроз безопасности информации в информационных (автоматизированных) системах

Угроза утечки информации о технологии производства на сервере системы автоматизированного проектирования

Удаленный вход по сети внутренним/внешним нарушителем, повышение привилегий с последующей отправкой полученной информации по сети



# Разработка методического обеспечения по моделированию угроз безопасности информации в информационных (автоматизированных) системах

ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ  
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России

« » \_\_\_\_\_ 2020 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**МЕТОДИКА  
МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

ПРОЕКТ

2020

Определение возможных негативных последствий от реализации угроз

Оценка условий реализации угроз безопасности информации

Определение сценариев реализации угроз безопасности информации

Оценка уровня опасности и актуальности угроз

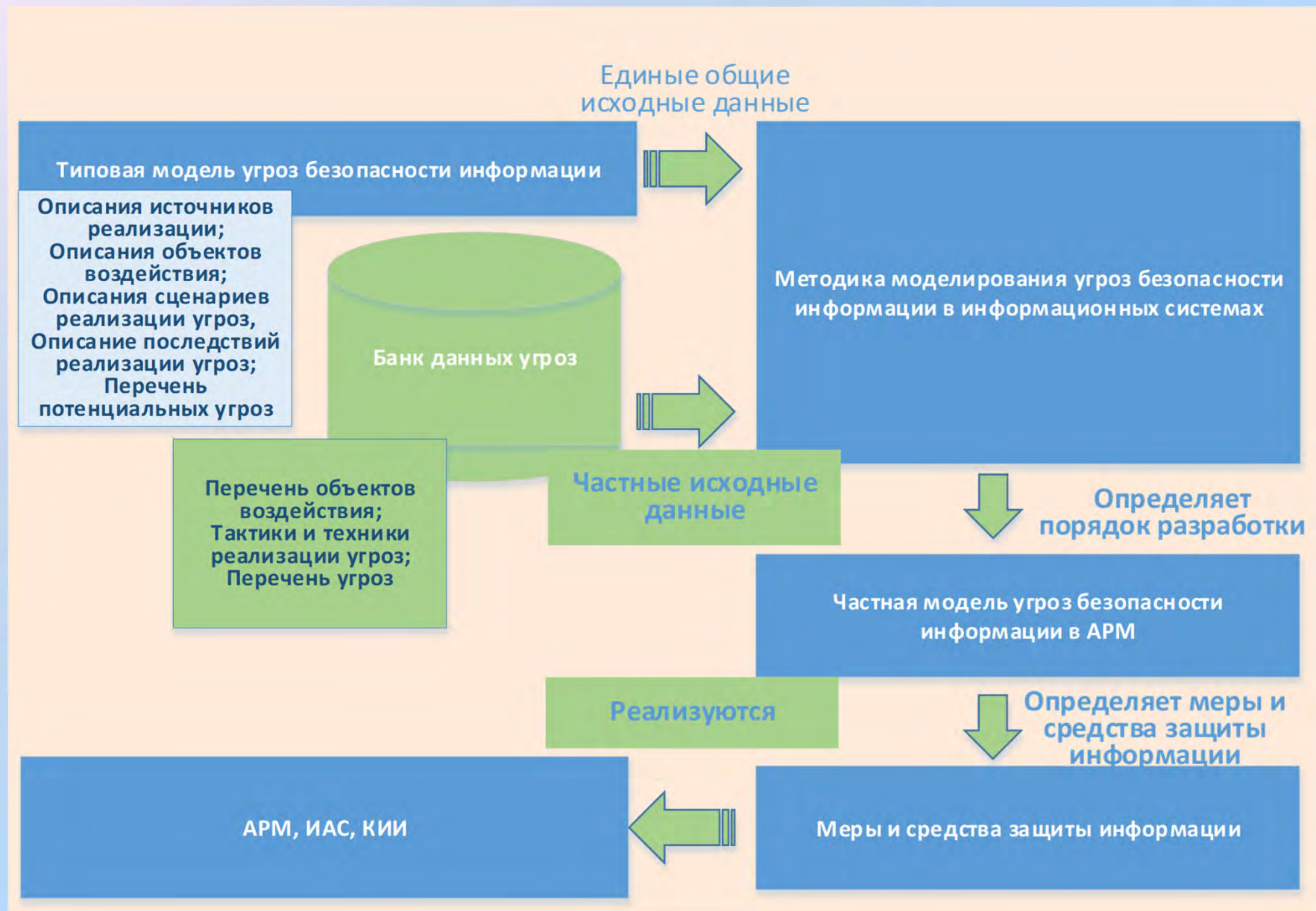
## Разработка типовых моделей угроз безопасности информации в информационных (автоматизированных) системах

Типовая модель угроз безопасности информации в автоматизированных рабочих местах

Типовая модель угроз безопасности информации в вычислительных сетях

Типовая модель угроз безопасности информации в центрах обработки данных

# Подход к применению методических документов по моделированию угроз в информационных (автоматизированных) системах





**Спасибо за внимание!**

**Гефнер Ирина Сергеевна**

**[otd22@fstec.ru](mailto:otd22@fstec.ru)**

**[www.fstec.ru](http://www.fstec.ru)**