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

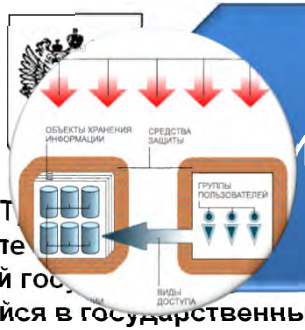
Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

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

Направления анализа угроз безопасности информации в информационных (автоматизированных) системах

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



Анализ угроз безопасности информации в отношении значимых объектов КИИ, ГИС, ИСПДН

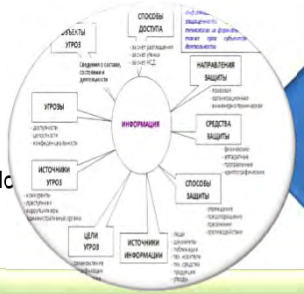
Т
о защите
составляющей гос
содержащейся в государственных информационных системах

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

критической информационной инфраструктуры российской федерации

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

содержание
ационных
р по обеспечению безопасности персональных данных при их обработке в информационных
ональных данных



Разработка модели угроз безопасности информации

М

ва, 2013

Анализ угроз бе
разработку
инфор

Информирование работников о возможных угрозах безопасности информации

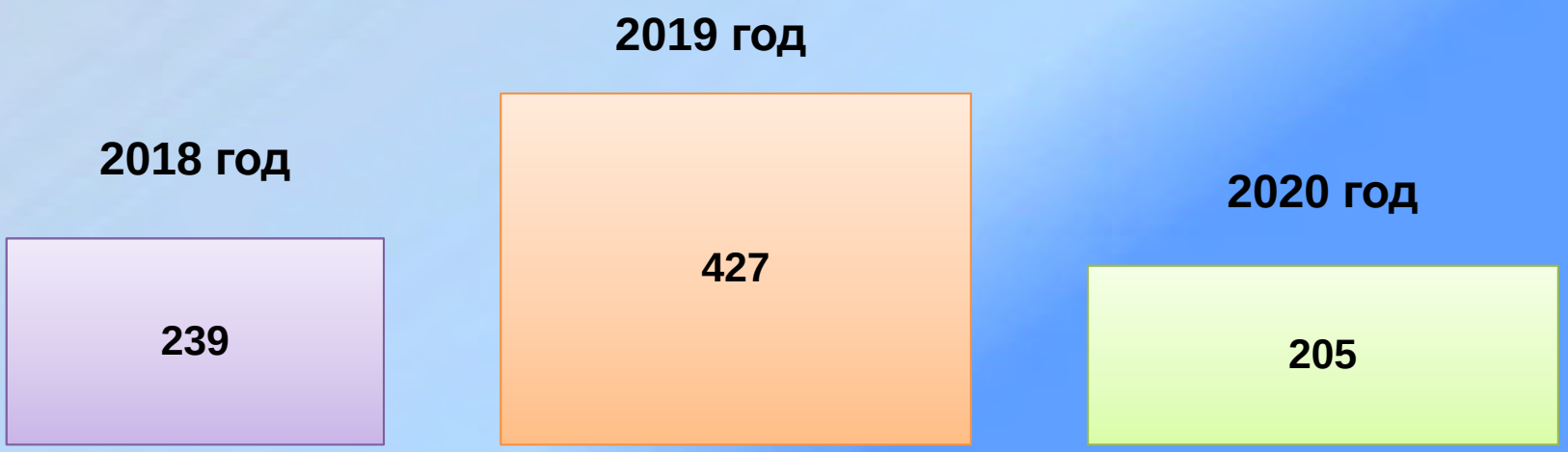
пасности
кны быть
актуальных
ных данных

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

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

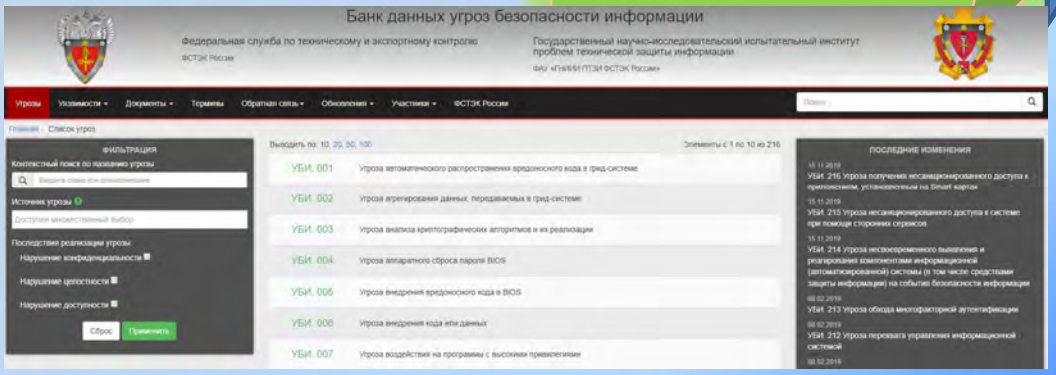
1. Описание архитектуры
2. Описание угроз
   - 2.1. Описание нарушителей
   - 2.2. Потенциальные уязвимости
   - 2.3. Способы реализации угроз
   - 2.4. Последствия от реализации угроз

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.)

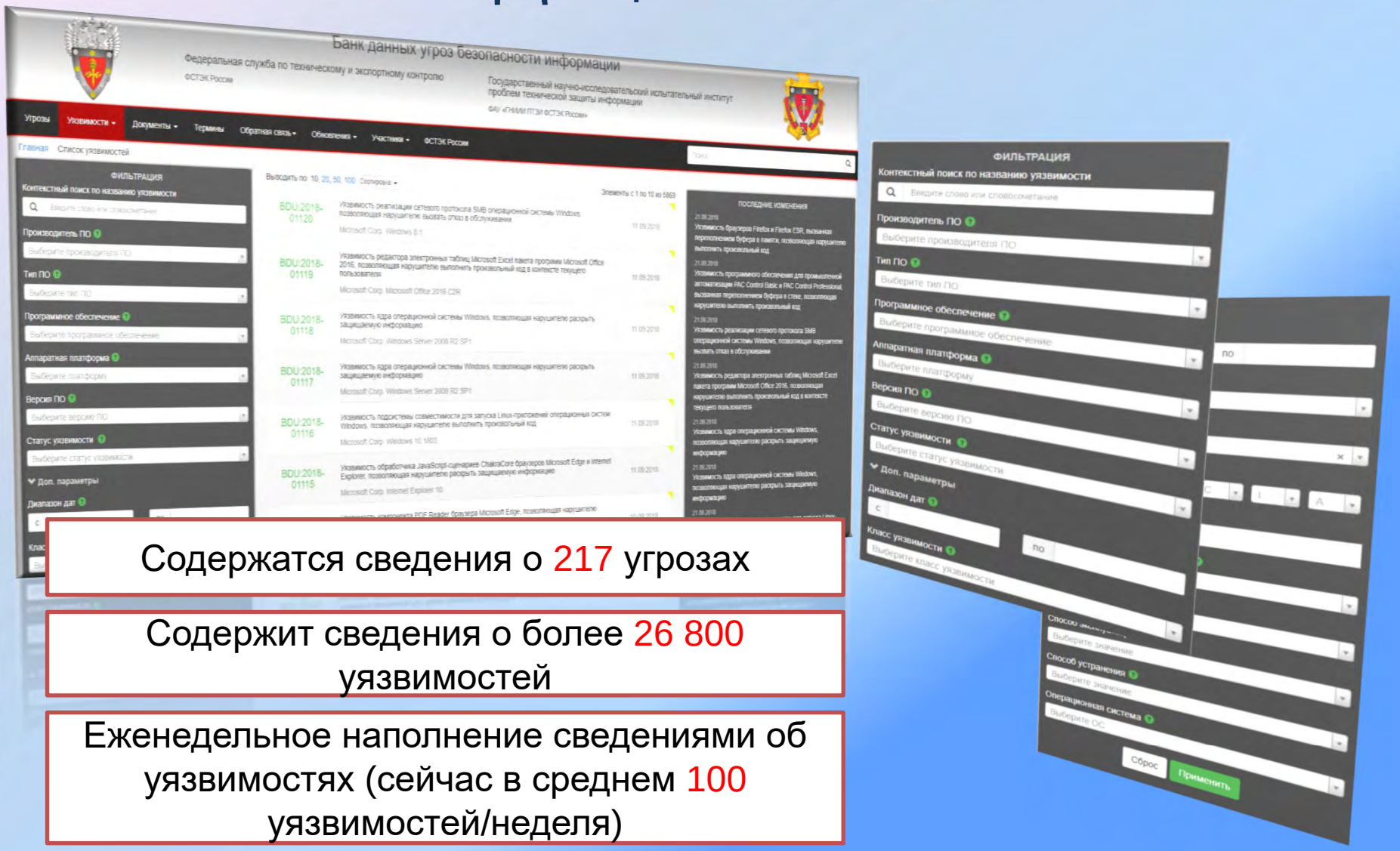


Банк данных угроз безопасности информации ФСТЭК России bdu.fstec.ru

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 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)

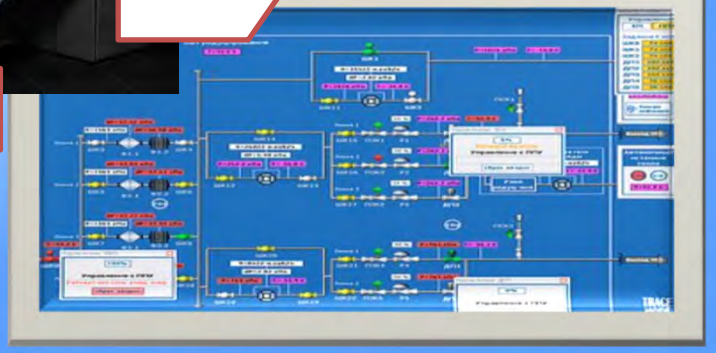
Угрозы безопасности информации, содержащиеся в банке данных угроз безопасности информации

Угрозы новых технологий

Угрозы АСУ ТП

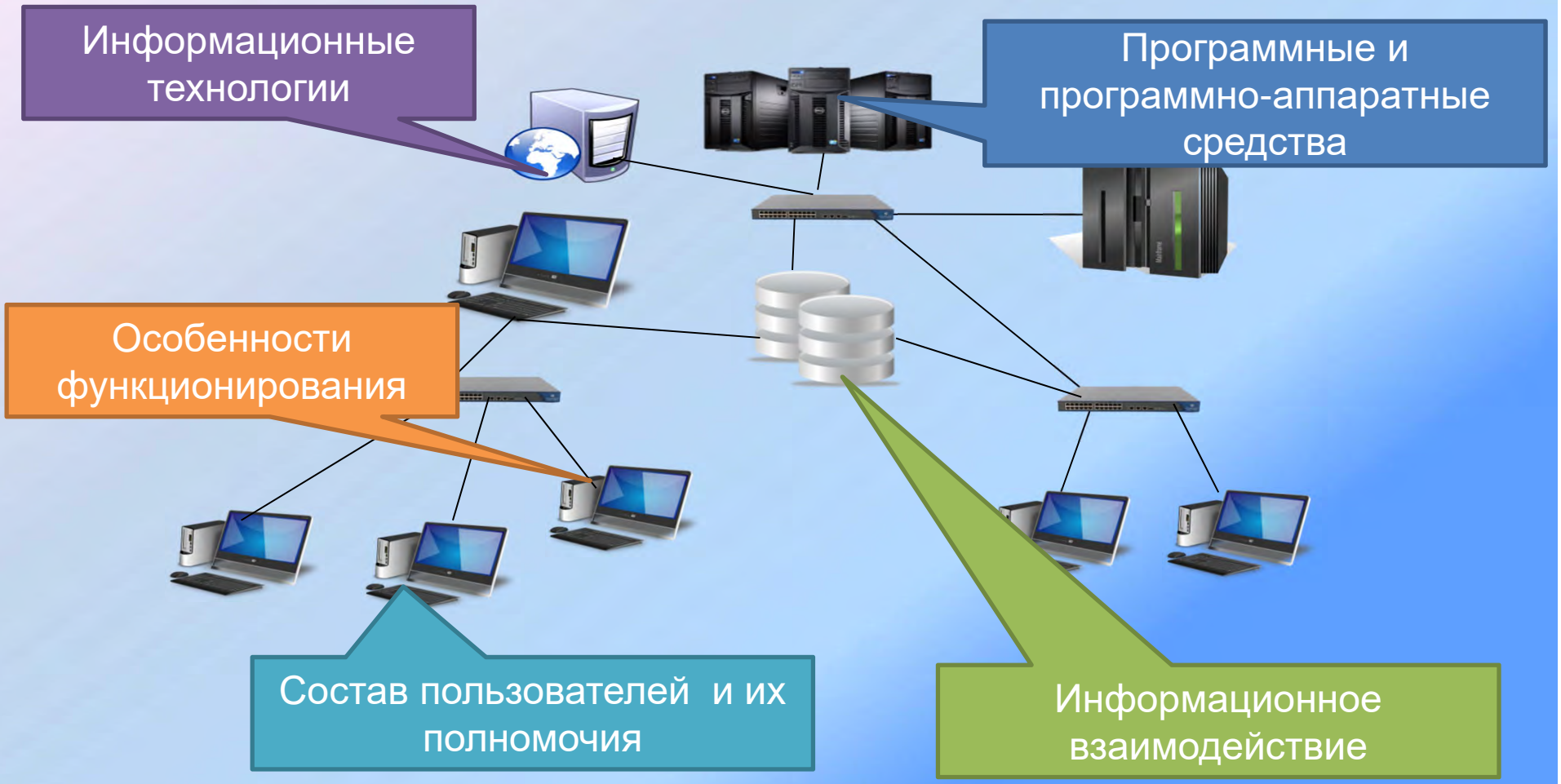
Угрозы ИС

Угрозы SCADA



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

Результаты анализа инфраструктуры информационных (автоматизированных) систем



Автоматизированные системы управления

Информационные системы

Информационно-телекоммуникационные сети

Развитие информационной инфраструктуры информационных (автоматизированных) систем

Более 30% государственных информационных систем функционирует на базе ЦОД

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

В **90%** информационных систем содержатся уязвимости

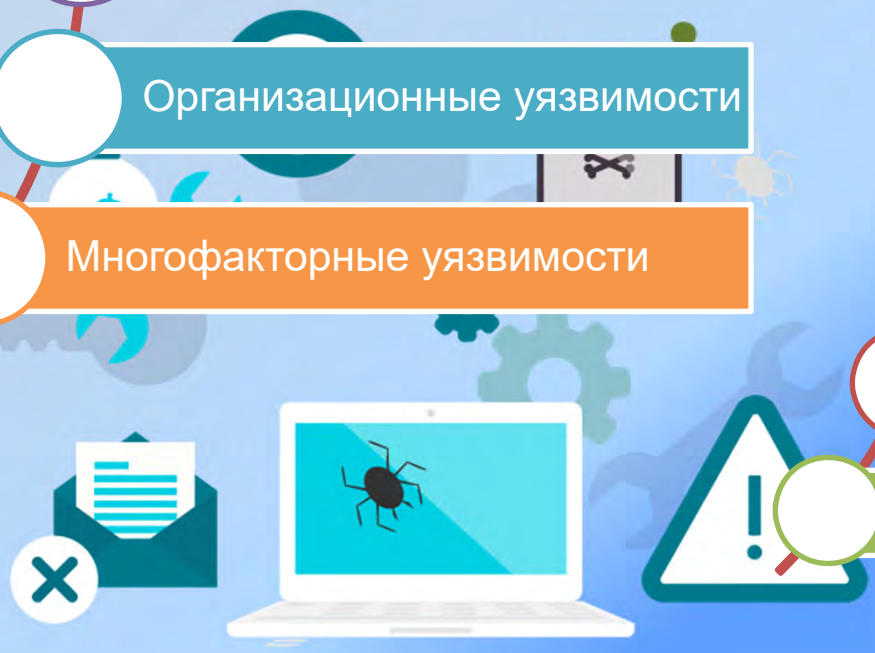
В **60%** информационных систем содержатся уязвимости высокого и критического уровня

- Внедрение вредоносного ПО
- Приведение системы в «отказ в облуживании»
- 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

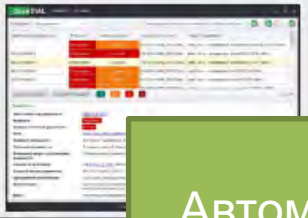
Программа **ScanOVAL для Linux** для автоматизированных проверок н
уязвимостей программного обеспечения

Программа ScanOVAL для Linux предназначена для оперативного автоматизированного обн
уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующи
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 с
формы обратной связи или посредством электронной почты.

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



Программа ScanOVAL для Linux обеспечивает выполн
основных функций:

- загрузка XML-файлов с OVAL-описаниями уязвимост
соответствии со стандартом «The OVAL Language Spe

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.

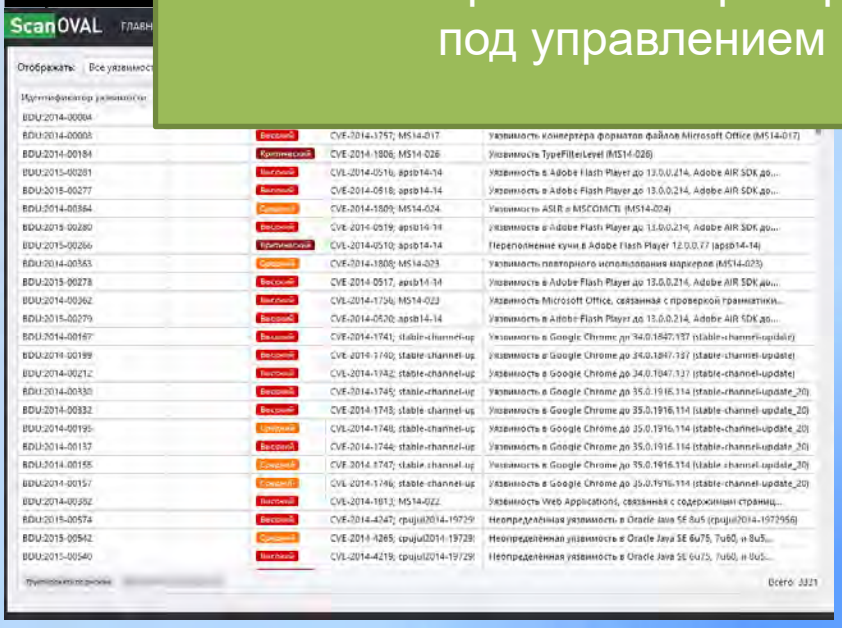
Для работы программы ScanOVAL аппаратная конфигурация компьютера должна соответствовать следующим минимальным требованиям:

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

системы) оператив-ной

и более поздней версии.

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

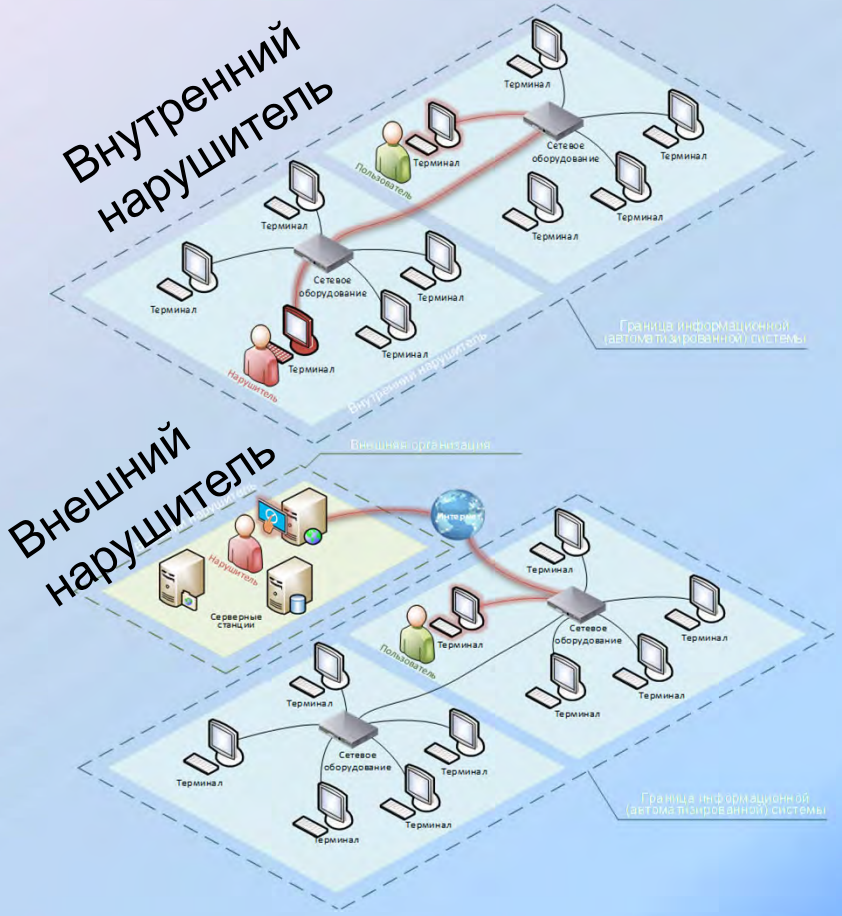


Профиль	Уязвимости
Начало/завершение сканирования	26.09.2018 12:21:44 / 26.09.2018 12:26:08
Формирование отчета	26.09.2018 12:26:51

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

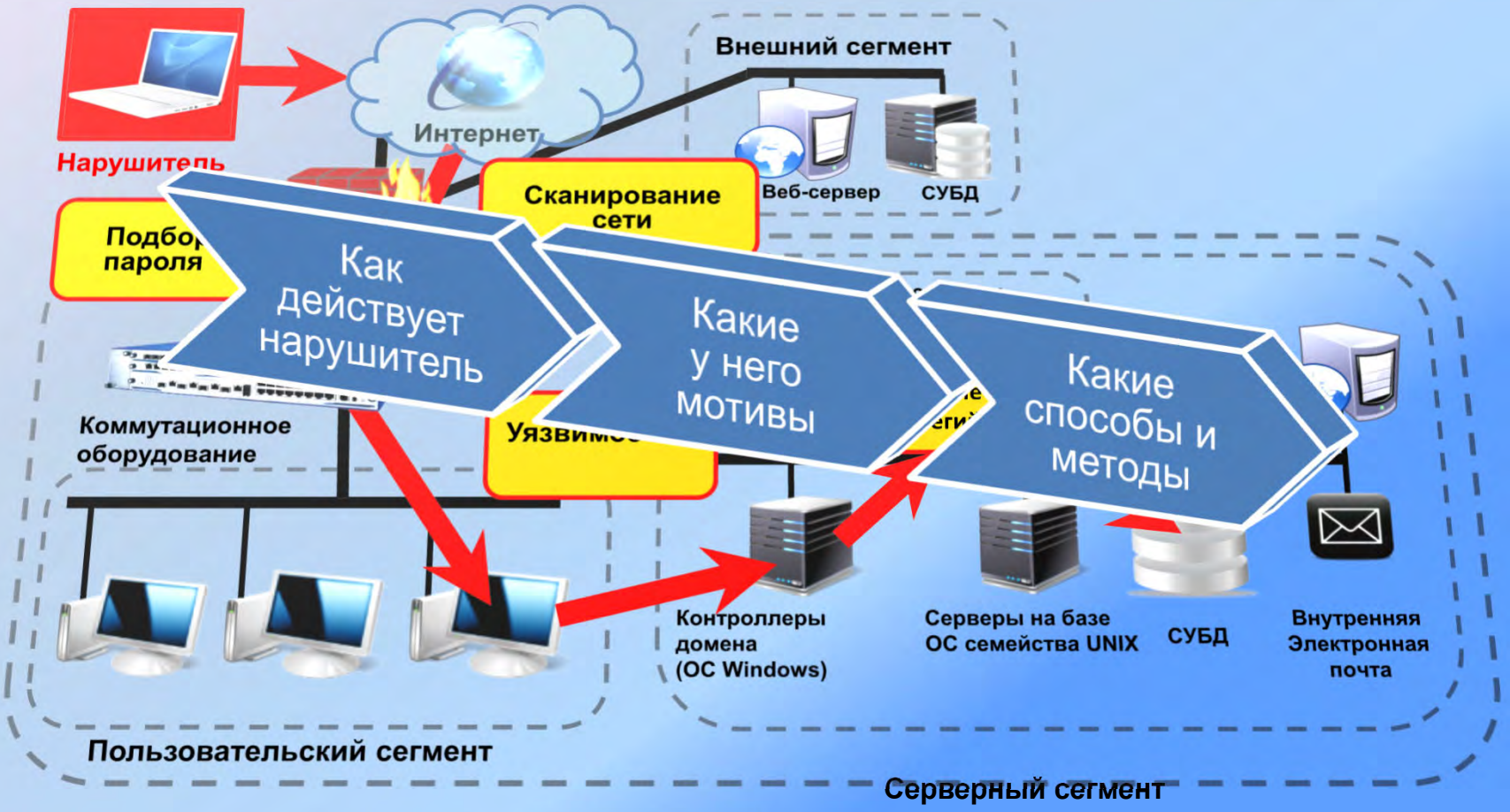
Формирование отчета по результатам анализа

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

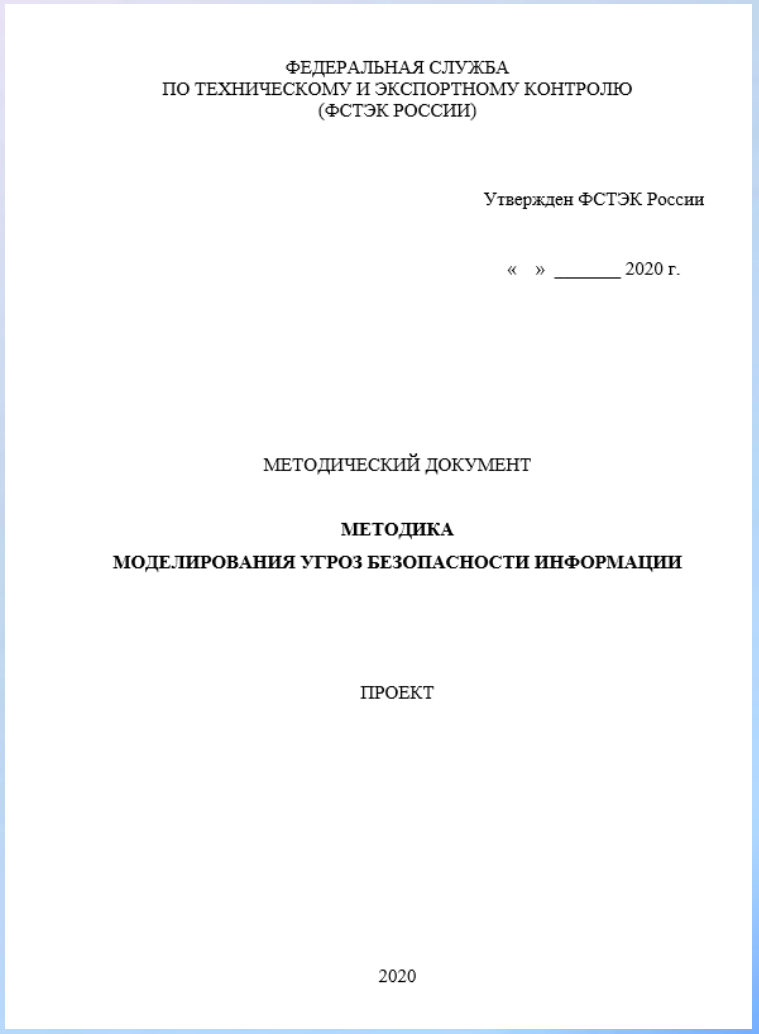


Оценка сценариев реализации угроз безопасности информации в информационных (автоматизированных) системах

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

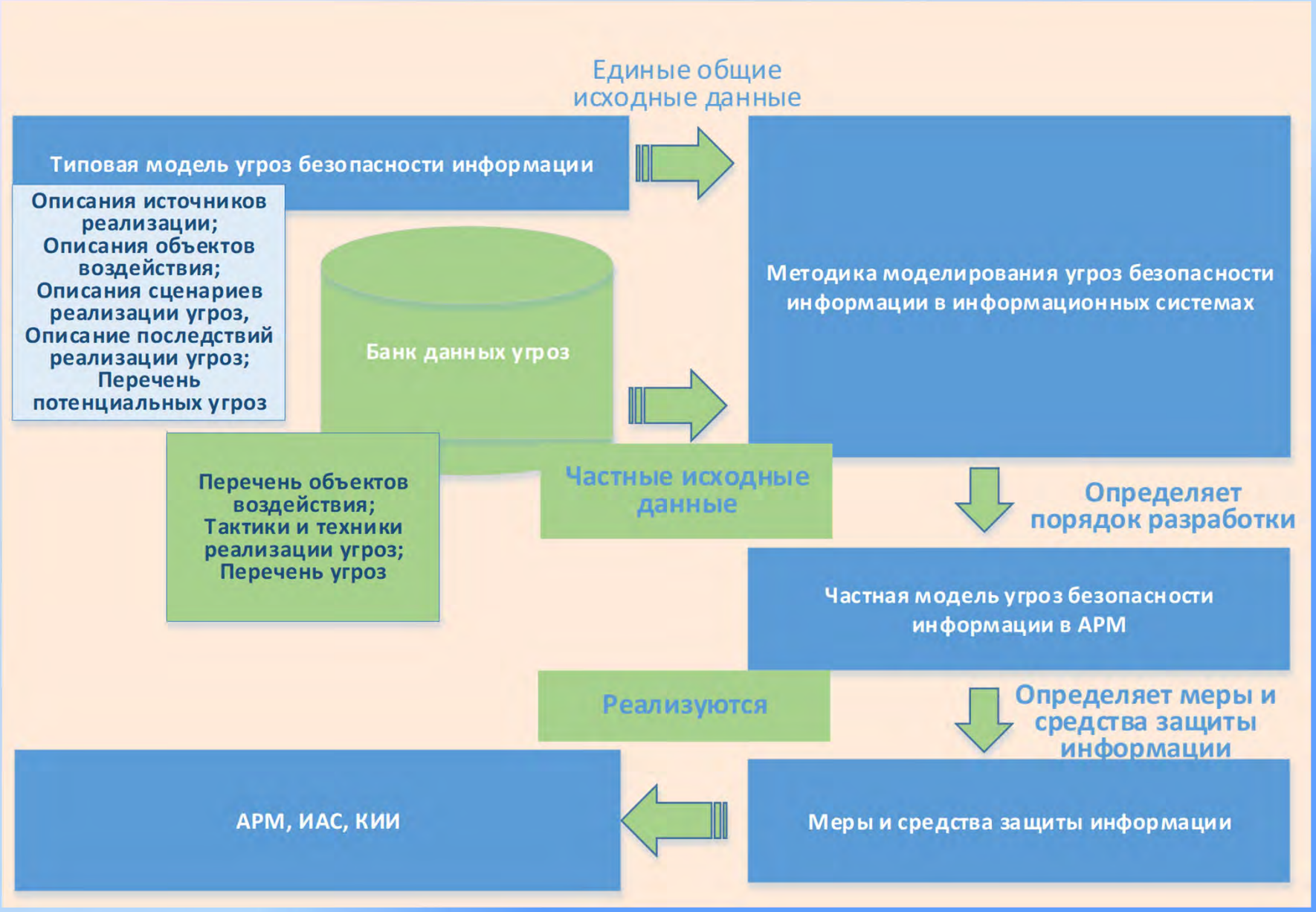
Разработка типовых моделей угроз безопасности информации в информационных (автоматизированных) системах

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

www.fstec.ru