Проект методического документа ФСТЭК России «Методика моделирования угроз безопасности информации»

Начальник отдела управления
ФСТЭК России Гефнер Ирина Сергеевна

Моделирование угроз безопасности информации

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

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

Москва, 2013

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

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации

Москва, 2017

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

Москва, 2013

Анализ угроз безопасности информации и разработка модели угроз безопасности информации

Меры по обеспечению безопасности персональных данных должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных

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

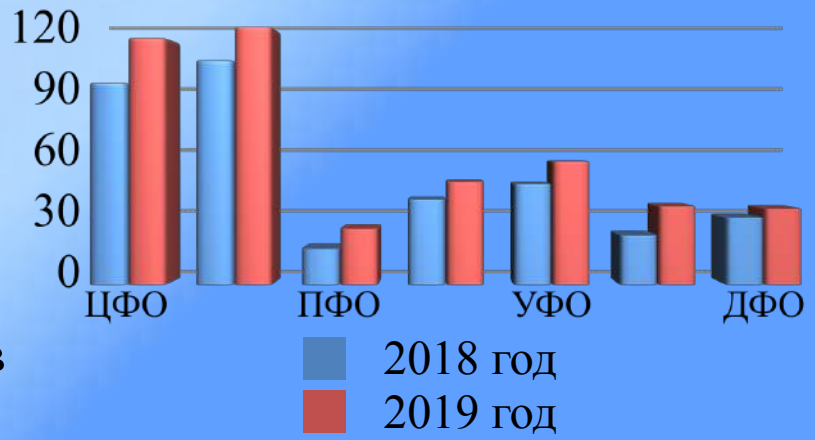
О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации

утверждены 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 документов по защите информации государственных информационных систем

2018 год	2019 год
439	827

Количество рассмотренных документов в управлениях ФСТЭК России по федеральным округам

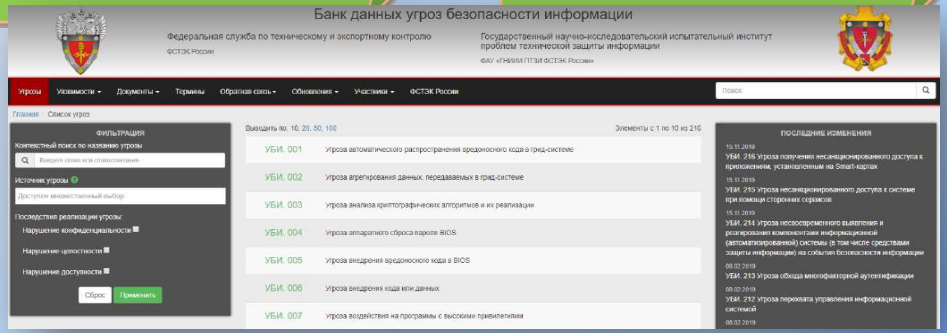


Количество рассмотренных документов в 2019 году увеличилось в 1,8 раза

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.)

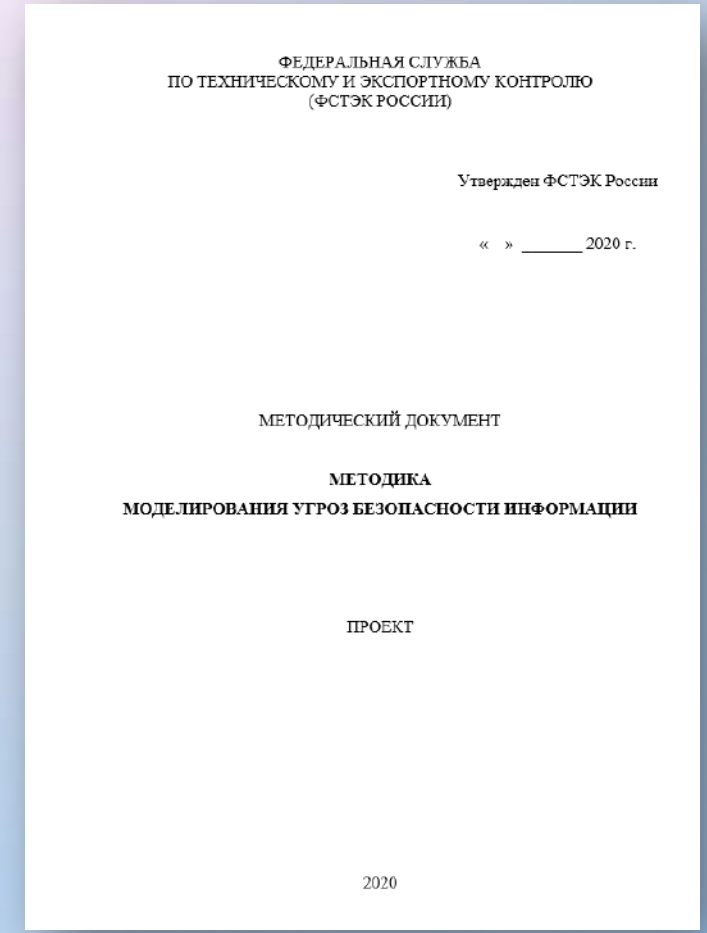
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК России 14 февраля 2008 г.)



Модель угроз безопасности информации государственной информационной системы

- Описание системы
- Описание возможностей нарушителей (модель нарушителя)
- Перечень вероятных угроз
- Определение актуальности угроз
- Перечень актуальных угроз

Разработка методического обеспечения по моделированию угроз безопасности информации



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России

« » _____ 2020 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ПРОЕКТ

2020

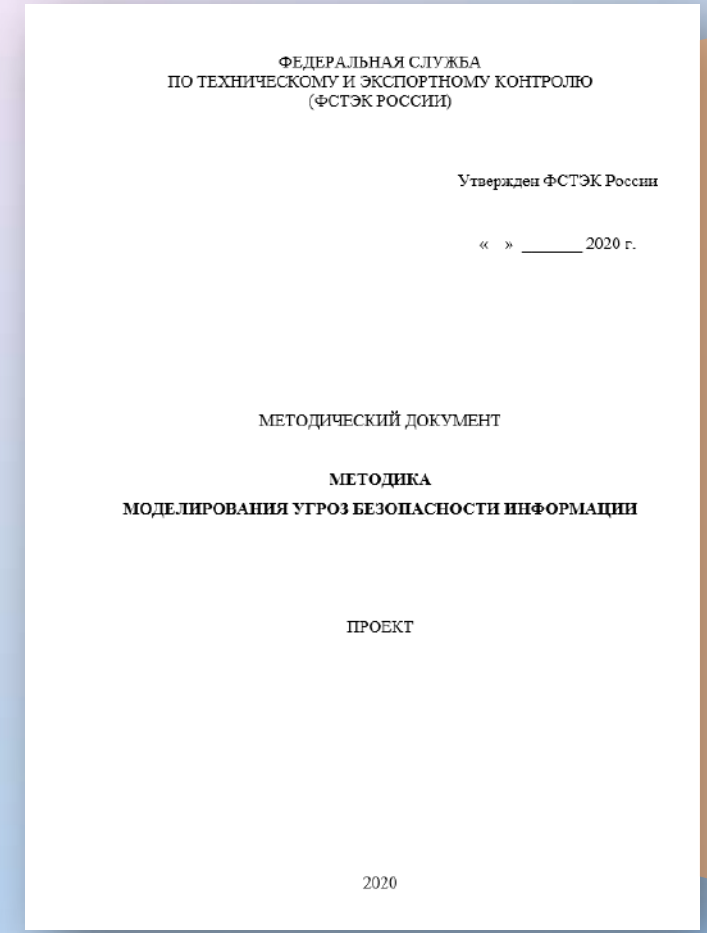
Обсуждение с экспертами

Размещение на сайте ФСТЭК России для общественного обсуждения

Доработка проекта методического документа по результатам общественного обсуждения

Утверждение проекта методического документа

Содержание проекта Методики моделирования угроз безопасности информации



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России

« » _____ 2020 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ПРОЕКТ

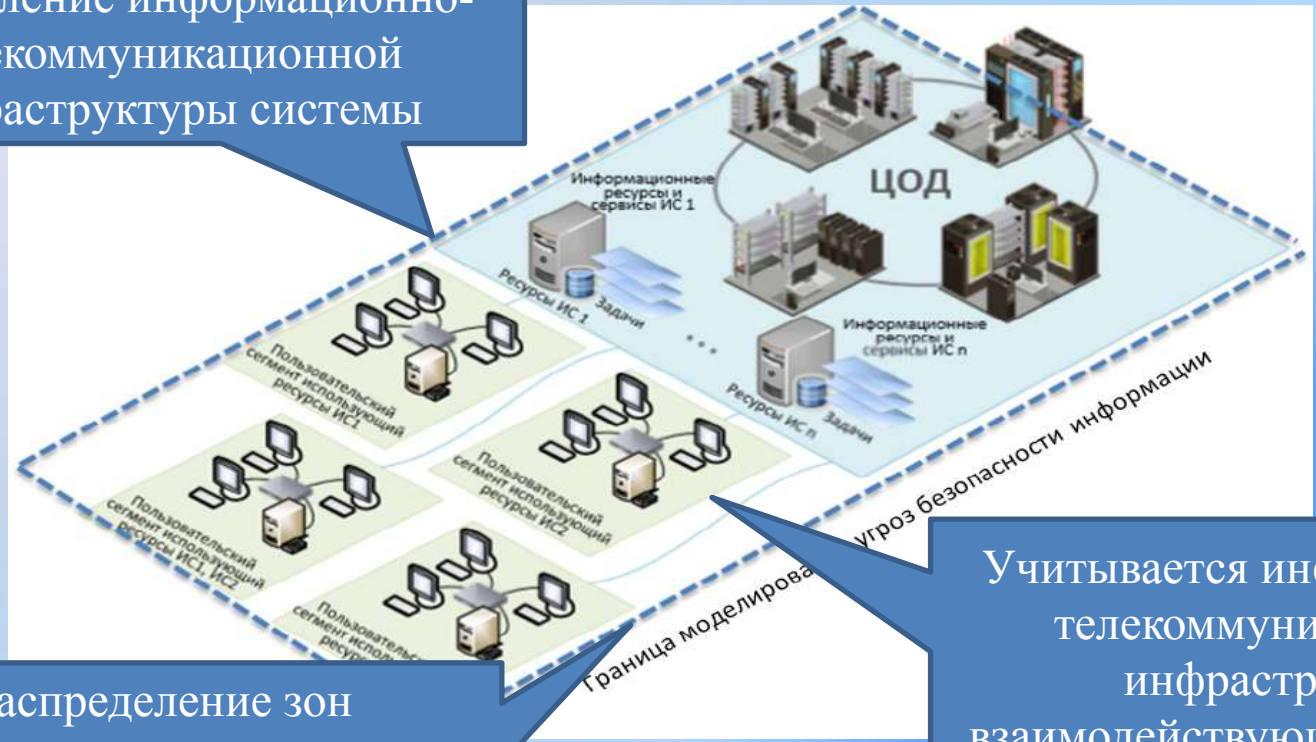
2020

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
2. **Порядок моделирования угроз безопасности информации и разработки моделей угроз безопасности информации**
3. **Выявление информационных ресурсов и видов воздействий, которые могут привести к недопустимым негативным последствиям**
4. **Источники угроз безопасности информации и оценка возможностей нарушителей**
5. **Определение сценариев реализации угроз безопасности информации**
6. **Выявление способов воздействия на информационные ресурсы и условий, необходимых для реализации этих воздействий**
7. **Оценка уровня опасности и актуальности угроз безопасности информации**

Алгоритм моделирования угроз безопасности информации

Этап 1.1. Выявление информационных ресурсов и видов воздействия

Определение информационно-телекоммуникационной инфраструктуры системы



Распределение зон ответственности между поставщиком услуг и оператором системы

Учитывается информационно-телекоммуникационная инфраструктура, взаимодействующая с системой системы

Этап 1.1. Выявление информационных ресурсов и видов воздействия

1

Определение видов ущерба и недопустимых негативных последствий

- невозможность (прерывание) предоставления социальных услуг (сервисов)
- разглашение персональных данных граждан;
- потеря клиентов, поставщиков и др.

2

Инвентаризация информационных ресурсов

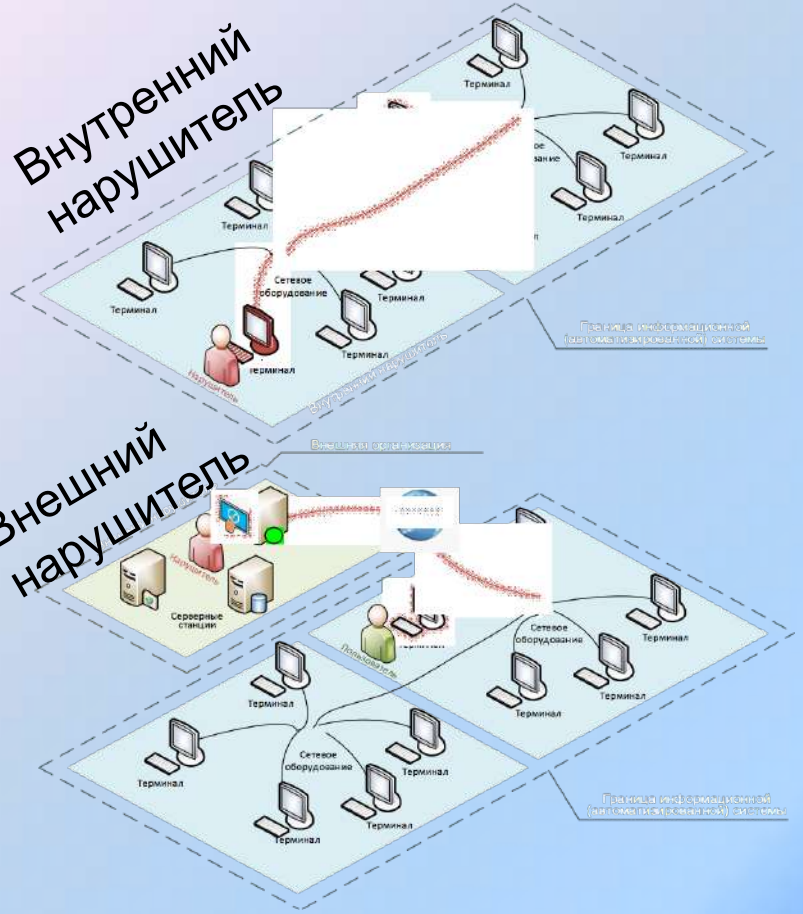
- веб-приложений
- баз данных
- сервисы
- почтовые сервера
- сервера приложений и др.

3

Определение видов воздействий на информационные ресурсы, которые могут привести к недопустимым негативным последствиям

- отказ в обслуживании
- несанкционированный доступ к компонентам, интерфейсам, сервисам;
- утечка защищаемой информации, системных, конфигурационных, иных служебных данных и др.

Этап 1.2. Определение источников угроз безопасности информации и оценка возможностей нарушителей



Виды нарушителя

Мотивация нарушителя

Уровень возможность

Нарушитель, обладающий высокими возможностями (потенциалом)

Нарушитель, обладающий базовыми повышенными возможностями (потенциалом)

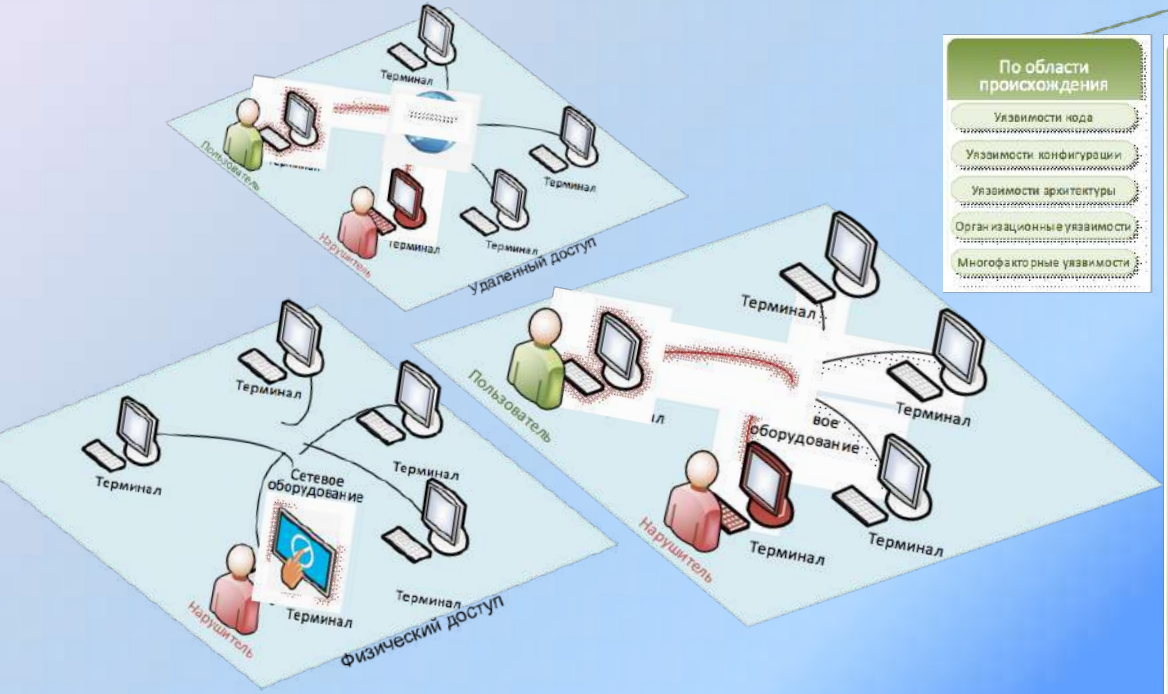
Нарушитель, обладающий базовыми возможностями (потенциалом)

Этап 1.3. Определение сценариев реализации угроз безопасности информации

Этап 1.3. Определение сценариев реализации угроз безопасности информации

Этап 1.4. Определение условий, необходимых для реализации угроз

Тип доступа



Наличие уязвимостей

Классификация уязвимостей информационных (автоматизированных) систем

По области происхождения

- Уязвимости кода
- Уязвимости конфигурации
- Уязвимости архитектуры
- Организационные уязвимости
- Многофакторные уязвимости

По типам недостатков ИС, связанных

- С неправильной настройкой параметров ПО
- С возможностью прослеживания пути доступа к каталогам
- С неполнотой проверки вводимых (входных) данных
- С возможностью перехода по ссылкам
- С возможностью внедрения команд ОС
- С межсайтовым скриптингом (выполнением сценариев)
- С внедрением интерпретируемых операторов языков программирования или разметки
- С внедрением произвольного кода
- С переполнением буфера памяти
- С неконтролируемой форматной строкой
- С вычислениями
- С утечкой/раскрытию информации ограниченного доступа
- С управлением полномочиями (учетными данными)
- С управлением разрешениями, привилегиями и доступом
- С аутентификацией
- С криптографическими преобразованиями (недостатки шифрования)
- С подменой межсайтовых запросов
- С «состоянием гонки»
- С управлением ресурсами

По месту возникновения (проявления)

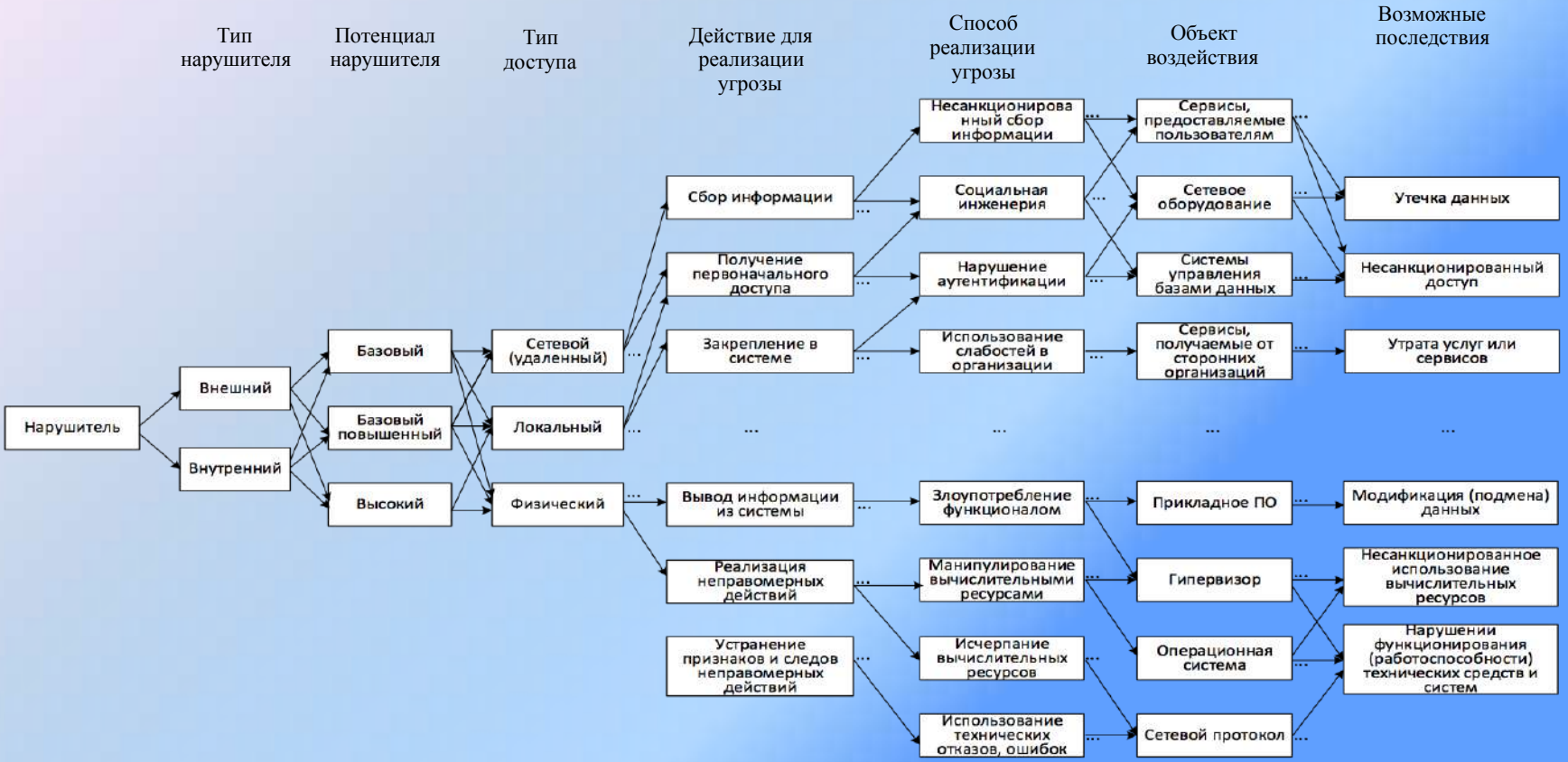
- Уязвимости в общесистемном (общем) программном обеспечении
- Уязвимости в прикладном программном обеспечении
- Уязвимости в специальном программном обеспечении
- Уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании
- Уязвимости в технических средствах
- Уязвимости в средствах защиты информации
- Уязвимости в портативных технических средствах

Этап 1. Формирование перечня потенциальных угроз безопасности информации

$УБИ_i$ = [источник угрозы; сценарий реализации угрозы; условия реализации; негативные последствия]

Угроза безопасности информации	**Сценарий реализации угрозы**		**Негативные последствия**
	Действие (тактика)	Способ (техника)	
Блокирование доступа к учетным записям **Блокирование доступа к web-ресурсу** **Несанкционированный доступ к системе управления базами данных и др.**	1) сбор данных о системах и сетях; 2) получение первоначального доступа; 3) закрепление в системе или сети; 4) исследование систем; 5) получение доступа к учетным записям; 6) повышение привилегий; 7) обход средств защиты информации; 8) реализация воздействия на информационные ресурсы и др.	1) фишинг; 2) уязвимость в сервисе; 3) шифрование данных; 4) перебор пароля; 5) прослушивание трафика и др.	1) отказ в обслуживании; 2) несанкционированный доступ; 3) нарушение доступности; 4) модификация данных и др.

Этап 1. Формирование перечня потенциальных угроз безопасности информации



Возможные сценарии реализации угроз безопасности информации

Сбор данных	Получение первоначального доступа	Закрепление	Исследование	Получение доступа к учетным записям	Повышение привилегий	Управление и контроль	Обход средств защиты	Вывод информации	Реализация воздействия
Идентификация уязвимостей									
							Обфускация файлов или информации		
	Использование эксплойтов публичных приложений								
		Использование Web Shell							
									Манипулирование хранимыми данными

Угроза модификации данных веб-приложения

Угроза несанкционированного доступа к системе управления базами данны

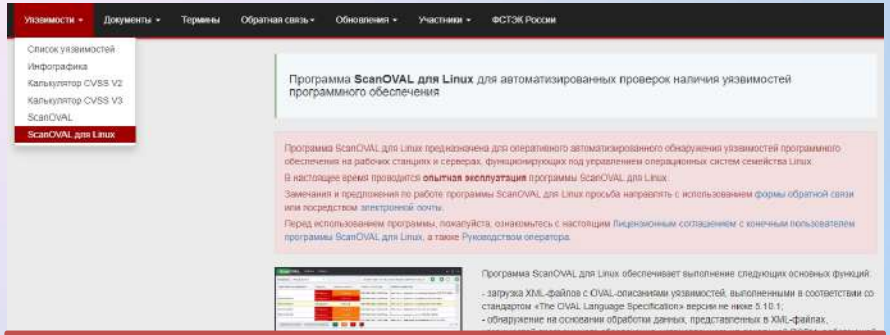
Сбор данных	Получение первоначального доступа	Закрепление	Исследование	Получение доступа к учетным записям	Повышение привилегий	Управление и контроль	Обход средств защиты	Вывод информации
Идентификация уязвимостей								
							Обфускация файлов или информации	
	Использование эксплойтов публичных приложений							
								Стандартные сетевые протоколы

Этап 2.1. Оценка уровня опасности и актуальности угроз безопасности информации

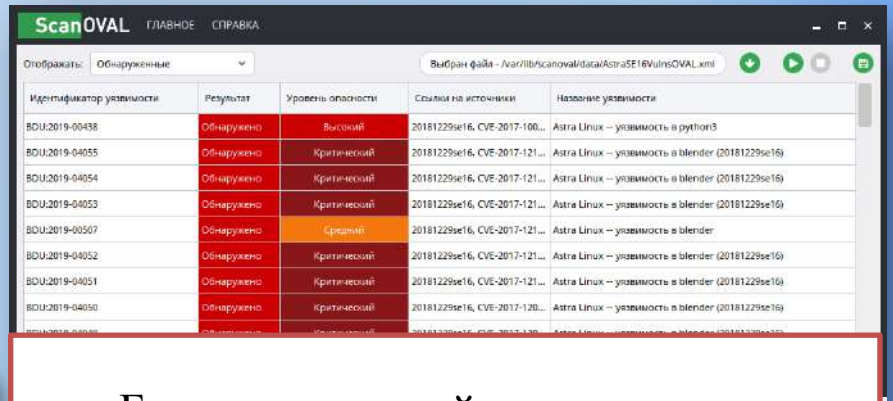
Показатель уровня опасности	Значения показателей уровня опасности	
Тип доступа (d)	Физический	3
	Локальный	2
	Удаленный (сетевой)	1
Направленность реализации угрозы безопасности информации (p)	Реализация угрозы приводит к целевому воздействию	3
	Реализация угрозы позволяет реализовать целевое воздействие	1
Сложность реализации угрозы (f)	Практически не реализуемые	1
	Многофакторные	2
	Однофакторные	3
Затронутые компоненты (пользователи) (s)	Ни одного пользователя и ни одного компонента	0
	Один пользователь и один компонент	1
	Более одного пользователя и более одного компонента	2
	Все пользователи и все компоненты	3
Последствия от реализации угрозы (u)	Отсутствуют	0
	Незначительные	1
	Умеренные	2
	Значительные	3

Актуальность и уровень опасности		Значение
Неактуальная		$3 \leq w \leq 4$
Актуальная	Низкая	$5 \leq w \leq 7$
	Средняя	$8 \leq w \leq 11$
	Высокая	$12 \leq w \leq 15$

Средство автоматизации поиска уязвимостей программного обеспечения, работающего под управлением Astra Linux 1.6 SE



Автоматизированная проверка уязвимостей ПО, работающего под управлением ОС Astra Linux 1.6 SE



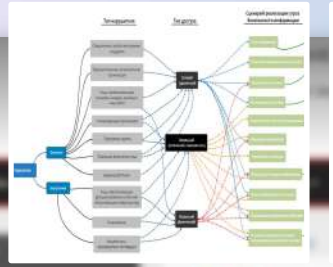
База уязвимостей, состоящая из **806** описаний на языке OVAL

Размещено на сайте банка данных 29 января 2020 г.

Более 500 загрузок

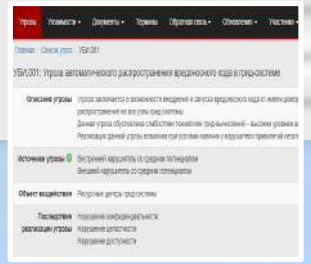
Формирование отчета по результатам анализа

Совершенствование банка данных угроз безопасности информации



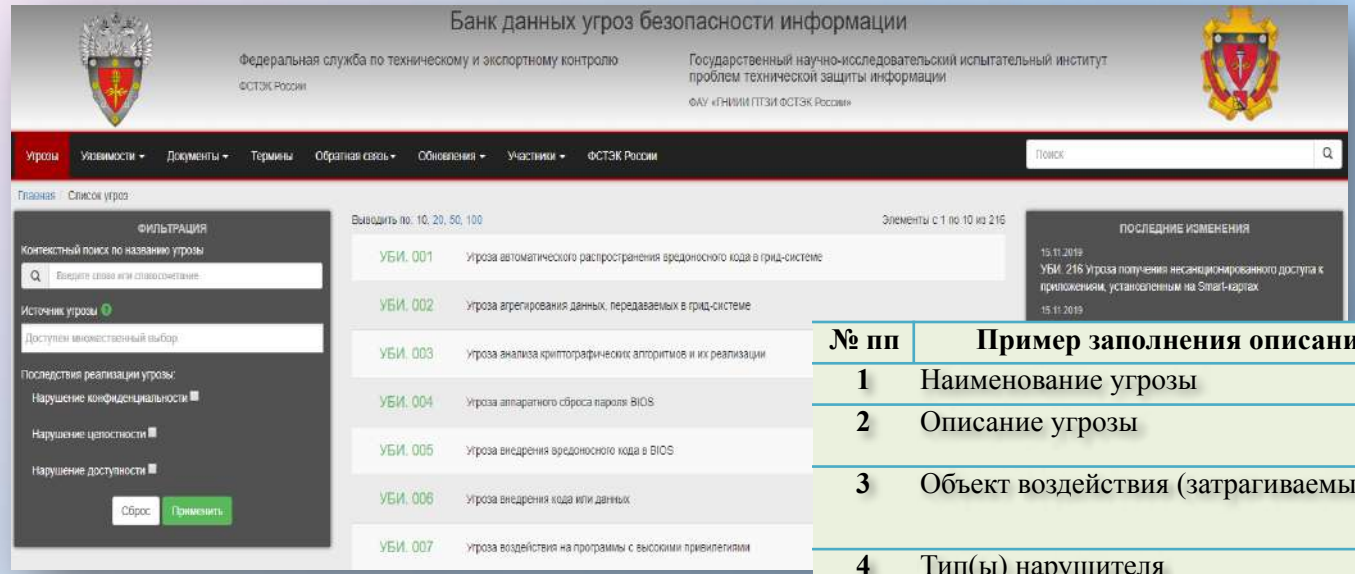
Разработка средства автоматизации моделирования угроз безопасности информации

Разработка механизмов оповещения органов власти и организаций об угрозах безопасности информации и уязвимостях программного обеспечения



Доработка базы угроз безопасности информации и описаний угроз безопасности информации

Новый подход к описанию угроз безопасности информации



№ пп	Пример заполнения описания угрозы безопасности	
1	Наименование угрозы	
2	Описание угрозы	
3	Объект воздействия (затрагиваемые компоненты)	
4	Тип(ы) нарушителя	
5	Потенциал нарушителя	
6	Тип(ы) доступа	
7	Действия и способы, за счет которых может быть реализована УБИ	
8	Индикаторы компрометации	
9	Возможные последствия	
10	**Рекомендации по защите**	

Проект методического документа ФСТЭК России «Методика моделирования угроз безопасности информации»

Начальник отдела управления
ФСТЭК России Гефнер Ирина Сергеевна