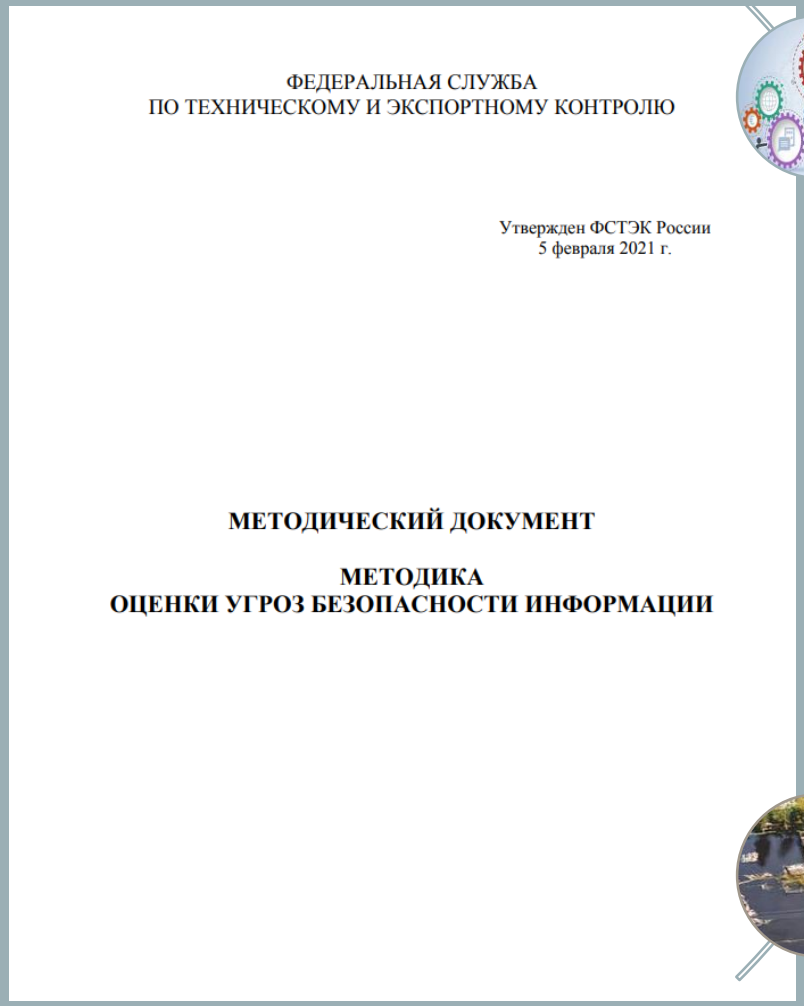
ПРАКТИКА РЕАЛИЗАЦИИ МЕТОДИКИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Начальник отдела управления ФСТЭК России

Гефнер Ирина Сергеевна

ВЫБОР МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ДЛЯ РАЗРАБОТКИ МОДЕЛЕЙ УГРОЗ



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Применяется для КИИ, ГИС, ИСПДн

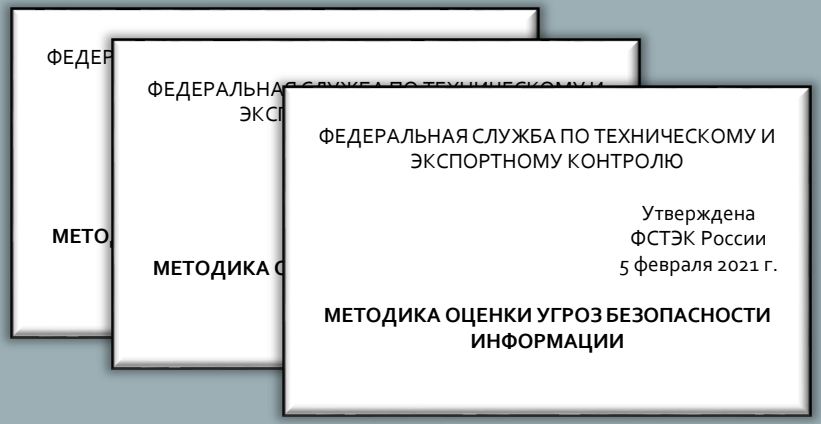
Вступил в действие с 5 февраля 2021 г.

Отмена Методика определения угроз для ИСПДн 2008 года

Не рассматриваются угрозы утечки по техническим каналам

Не является предметом моделирования техногенных угроз

СТАТИСТИКА ПО КОЛИЧЕСТВУ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, КОТОРЫЕ ПОСТУПАЮТ НА СОГЛАСОВАНИЕ ВО ФСТЭК РОССИИ



Количество рассмотренных ФСТЭК России документов по защите информации государственных информационных систем за 2020 и 2021 года

498

2020 год

710

2021 год

15 - по Методике ИСПДн

695 - новой Методике 2021 года

Количество рассмотренных документов в 2021 году увеличилось в 1,5 раза

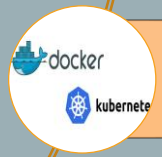
ТИПОВЫЕ ЗАМЕЧАНИЯ ПО РАССМОТРЕНИЮ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Не в полном объеме определены негативные последствия для видов (рисков) ущерба, а также объекты воздействия

Не оценены виды нарушителей, которые могут реализовывать угрозы безопасности информации

Внутренние пользователи не признаются актуальными нарушителями

Не в полном объеме представлено описание сценариев реализации угроз безопасности информации



Не оценены угрозы безопасности информации, связанные с технологией контейнеризации, представленными ФСТЭК России способами

Для информационно-телекоммуникационной инфраструктуры центра обработки данных, на которой размещается государственная информационная система не оценены угрозы безопасности информации

67 % документов возвращаются на доработку

ЭТАПЫ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Этап 1
Определение негативных последствий

Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации

Этап 2
Определение объектов воздействий

Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации

Этап 3
Оценка возможности реализации угроз и их актуальности

Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации

Оценка способов реализации (возникновения) угроз безопасности информации

Оценка сценариев реализации угроз безопасности информации в системах и сетях

ИСТОЧНИКИ ИСХОДНЫХ ДАННЫХ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

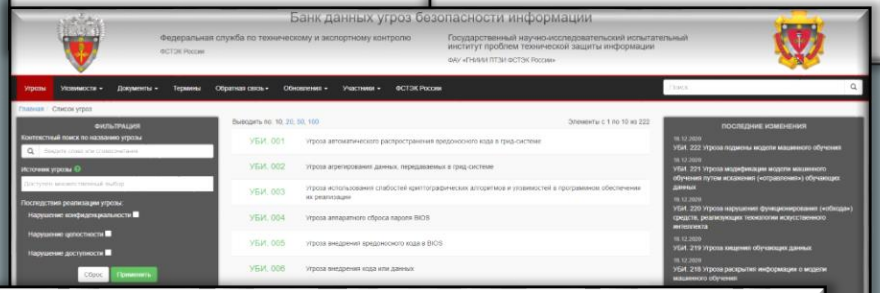
Утверж
ФСТЭК Р
15 феврал

**БАЗОВАЯ МОДЕЛЬ УГРО
БЕЗОПАСНОСТИ ПЕРСОНАЛ
ДАННЫХ ПРИ ИХ ОБРАБОТ
ИНФОРМАЦИОННЫХ СИСТЕ
ПЕРСОНАЛЬНЫХ ДАННЫ**

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утверждена
ФСТЭК
России
5 февраля
2021 г.

МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



Нормативные правовые акты Российской Федерации, в соответствии с которыми задаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим

Технические задания на создание систем и сетей, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация

Негативные последствия

Объекты воздействия угроз безопасности информации

Возможности нарушителей

Тактики и техники

Утверждена
_____ 202_ г.

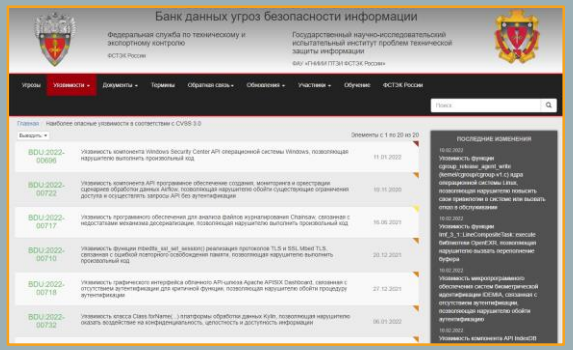
Модель угроз безопасности информации

Согласована
ФСБ России
_____ 202_ г.

Согласована
ФСТЭК России
_____ 202_ г.

ВЕДЕНИЕ МОДЕЛИ УГРОЗ В ЭЛЕКТРОННОМ ВИДЕ

Банк данных угроз безопасности



Новые угрозы безопасности информации

Удобство ведения Модели угроз безопасности информации в электронном виде в период эксплуатации систем и сетей

РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ ПРИ ОЦЕНКЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ МЕЖДУ ОПЕРАТОРОМ И ПОСТАВЩИКОМ УСЛУГ

1 Вариант. Включение в модель угроз системы или сети угроз, актуальных для инфраструктуры поставщика услуг

2 Вариант. Включение в модель угроз системы или сети ссылки на модель угроз безопасности информации инфраструктуры поставщика услуг

Оператор

Поставщик услуг

ОПРЕДЕЛЕНИЕ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ НА ПРИМЕРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНА ГОСУДАРСТВЕННОЙ ВЛАСТИ

1.Исходные данные

- **Положение об органе государственной власти**
- **Федеральный закон «Об информации, информационных технологиях и о защите информации»**
- **Федеральный закон «О персональных данных»**
- **Нормативный правовой акт о создании системы**
- **Концепция создания информационной системы**
- **Техническое задание на создание информационной системы**
- **Проектная документация**

2.Область деятельности

Цели:

- **Реализация полномочий ОГВ**
- **Повышение качества предоставления государственных услуг**

Задачи

- **Информирование граждан о деятельности органа власти**
- **Предоставление государственной услуги**
- **Прием обращений граждан**
- **Ведение реестра юридических лиц для осуществления для разрешительной деятельности**

3.Негативные последствия

- Отсутствие доступа к государственной услуге
- Финансовый, иной материальный ущерб физического лица
- Отсутствие возможности информирования граждан
- Неспособность выполнения договорных обязательств
- Увеличение количества жалоб в органы государственной власти или органы местного самоуправления

ПРОВЕДЕНИЕ ЭКСПЕРТНОЙ ОЦЕНКИ РИСКОВ (УЩЕРБА) В СООТВЕТСТВИИ С МЕТОДИКОЙ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Опросный метод

Параметры:

Негативные последствия от реализации угроз безопасности информации

Шкала измерений

Низкий
Средний
Высокий

Формирование результатов с занесением в таблицу

ЭКСПЕРТНАЯ ОЦЕНКА НЕГАТИВНЫХ ПОСЛЕДСТВИЙ НА ПРИМЕРЕ СИСТЕМЫ ОРГАНА ГОСУДАРСТВЕННОЙ ВЛАСТИ

Эксперты	Отсутствие доступа к государственной услуге	Финансовый, иной материальный ущерб физического лица	Отсутствие возможности информирования граждан	Увеличение количества жалоб в органы государственной власти или органы местного самоуправления	Неспособность выполнения договорных обязательств
Специалист по защите информации	низкий	высокий	высокий	высокий	высокий
Специалист финансово-экономического объекта	средний	низкий	высокий	высокий	высокий
Специалист ответственный за эксплуатацию сетей связи	высокий	средний	низкий	высокий	высокий
Специалист правового отдела	высокий	высокий	средний	низкий	высокий
Специалист ответственный за эксплуатацию АСУ ТП	высокий	высокий	высокий	средний	Низкий
Итоговое значение	высокий	высокий	высокий	высокий	высокий

ГРУППИРОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ И КОМПОНЕНТОВ НА ПРИМЕРЕ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРИ ОПРЕДЕЛЕНИИ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ

ВИДЫ ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ ГИС ОРГАНА ГОСУДАРСТВЕННОЙ ВЛАСТИ

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан	База данных	Утечка идентификационной информации граждан из базы данных
Отсутствие доступа к ГИС	Веб-приложение портала государственных услуг	Отказ в обслуживании веб-приложения
Не предоставление государственных услуг	Система управления содержимым веб-приложения (сайта) ГИС	Подмена информации на страницах портала на недостоверную
Не предоставление государственных услуг	Сервер баз данных ГИС	Отказ в обслуживании сервера управления базами данных
Не предоставление государственных услуг		Подмена информации в базах данных на недостоверную
Не предоставление государственных услуг		Утечка персональных данных граждан

ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ УГРОЗ

Специальные службы иностранных государств

Преступные группы (криминальные структуры)

Авторизованные пользователи

Цели нарушителей → **Перечень негативных последствий от реализации угроз безопасности информации**

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
1	Специальные службы иностранных государств	–	–	–	–
2	Террористические, экстремистские группировки	–	–	+ (дестабилизация деятельности органов государственной власти)	У3 (нарушение законодательства Российской Федерации)
3	Преступные группировки (криминальные структуры)	+ (получение финансовой выгоды за счет кражи и продажи ПДн)	+ (получение финансовой выгоды за счет кражи и продажи информации ограниченного доступа)	+ (получение финансовой выгоды за счет кражи и продажи информации ограниченного доступа)	У1 (Нарушение конфиденциальности (утечка) ПДн) У2 (невозможность заключения

Возможные цели нарушителей приведены в приложении № 6 к Методике

ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ УГРОЗ

Специальные службы иностранных государств

Преступные группы (криминальные структуры)

Авторизованные пользователи

Банк данных угроз безопасности информации

Потенциал нарушителей

Низкий

Средний

Высокий

Методика оценки угроз безопасности информации

Уровень возможностей нарушителей

Базовый

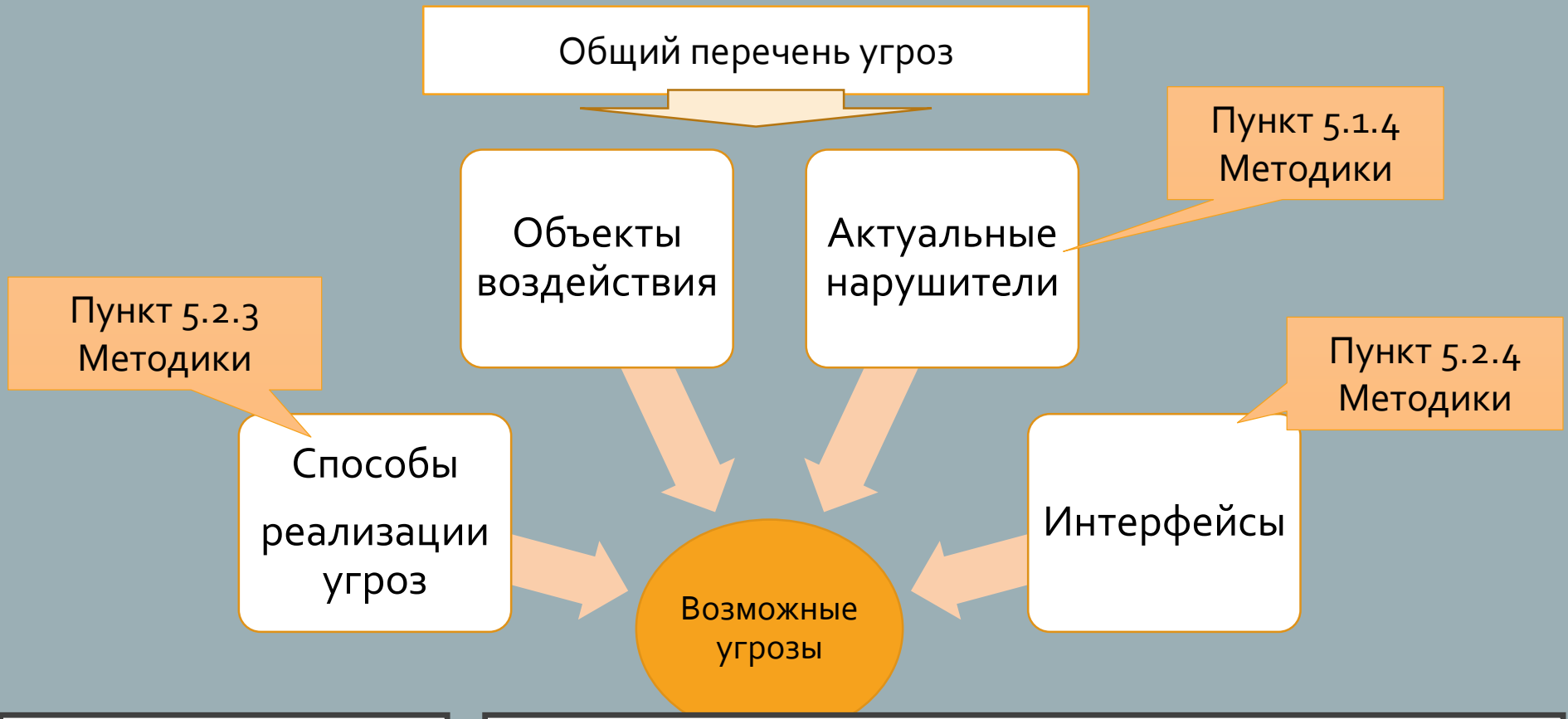
Базовый с повышенными возможностями

Средний

Высокий

№ п/п	Вид нару	Нанесение ущерба	юридическому лицу,	государству в области обеспече страны, госуд правопорядка, а также в соци эконом полит огической сфере деяте	возможным
1	Специальны службы ино государств	–	–	–	–
2	Террористические, экстремистские группировки	–	–	(дестабилизация деятельности органов государств	законодательства Российской
3	Преступны группировки (криминальные структуры)	+ (получение финансовой выгоды за счет кражи и продажи ПДн)	+ (получение финансовой выгоды за счет кражи и продажи информации ограниченного доступа)	+ (получение финансовой выгоды за счет кражи и продажи информации ограниченного доступа)	(нарушение конфиденциальности (утечка) ПДн) У2 (невозможность заключения

ОПРЕДЕЛЕНИЕ ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



Угрозы, содержащие в банке данных угроз (bdu.fstec.ru)

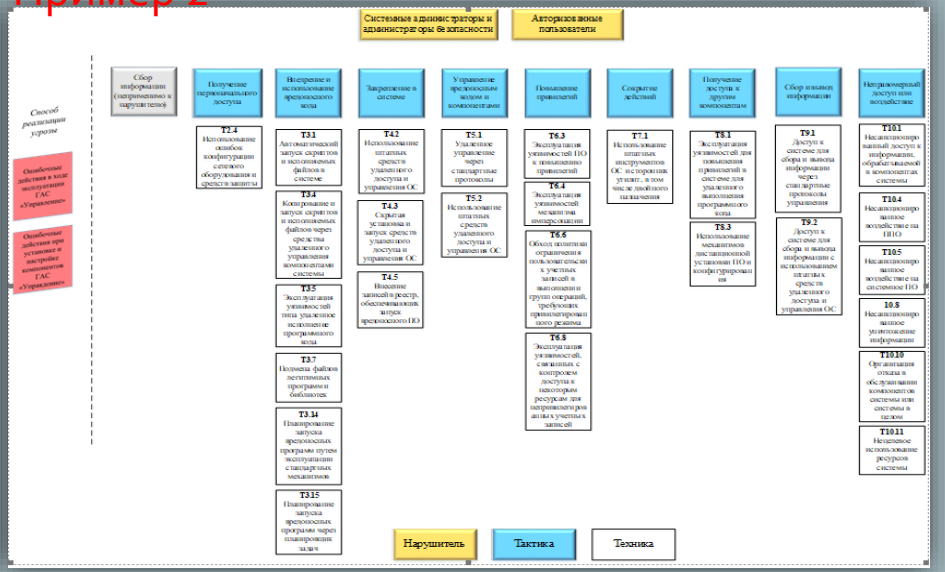
Пример описания угрозы безопасности информации:
УБИ.001 Угроза *несанкционированного доступа к* АРМ *пользователя путем внедрения вредосного кода*
УБИ.003 Угроза *отказа в обслуживании веб-портала путем эксплуатации уязвимостей*
УБИ.004 Угроза *подмены информации, содержащейся в базе данных, из-за ошибочных действий*

ПРИМЕРЫ ОПИСАНИЙ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Пример 1

Объекты воздействия	Тип доступного интерфейса	Вид воздействия	Способ реализации угрозы	Вероятные угрозы	Тактики/техники сценария реализации угроз
Средства обеспечения внутреннего и внешнего сетевого взаимодействия серверных компонент	Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет» (уровень 6)	Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности) Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности) Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации	Использование уязвимостей архитектуры	УБИ.14 Угроза длительного удержания вычислительных ресурсов пользователями	T1.2 T1.3 T1.4 T1.5 T1.6 T2.5 T2.13 T3.8 T5.1 T5.2 T5.3 T5.4 T5.6 T5.7 T5.8 T5.11 T5.12 T5.13 T6.1 T6.2 T7.17 T7.18 T7.19 T7.20 T7.23 T7.24 T7.25 T8.2 T8.3 T8.4 T8.6 T8.7 T8.8 T9.1 T9.2 T9.3 T9.4 T9.5 T9.6 T9.7 T9.8 T9.9 T9.13 T9.14 T10.3 T10.4 T10. 11
				УБИ.69 Угроза неправомерных действий в каналах связи	T1.2 T1.3 T1.4 T1.5 T1.6 T2.5 T2.13 T3.8 T5.1 T5.2 T5.3 T5.4 T5.6 T5.7 T5.8 T5.10 T5.11 T5.12 T5.13 T6.1 T6.2 T6.5 T7.18 T7.19 T7.20 T7.23 T7.24 T7.25 T8.2 T8.3 T8.4 T8.6 T8.7 T8.8 T9.1 T9.2 T9.3 T9.4 T9.5 T9.6 T9.7 T9.8 T9.9 T9.13 T9.14 T10.3 T10.4
				УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании»	T1.2 T1.3 T1.4 T1.5 T1.6 T2.5 T2.13 T3.8 T5.1 T5.2 T5.3 T5.4 T5.6 T5.7 T5.8 T5.11 T5.12 T5.13 T6.1 T6.2 T7.18 T7.19 T7.20 T7.23 T7.24 T7.25 T8.2 T8.3 T8.4 T8.6 T8.7 T8.8 T9.1 T9.2 T9.3 T9.4 T9.5 T9.6 T9.7 T9.8 T9.9 T9.13 T9.14

Пример 2



Пример 3

УБИ	Наименование УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Способ реализации угрозы	Объект воздействия	Сценарий	Актуальность
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель с низким потенциалом	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При	Аппаратное обеспечение, носители информации, объекты файловой системы	T1.3, T1.5, T1.8, T1.12, T1.13, T2.4, T2.10, T2.11, T2.8, T2.12, T3.14, T4.5	Актуальная

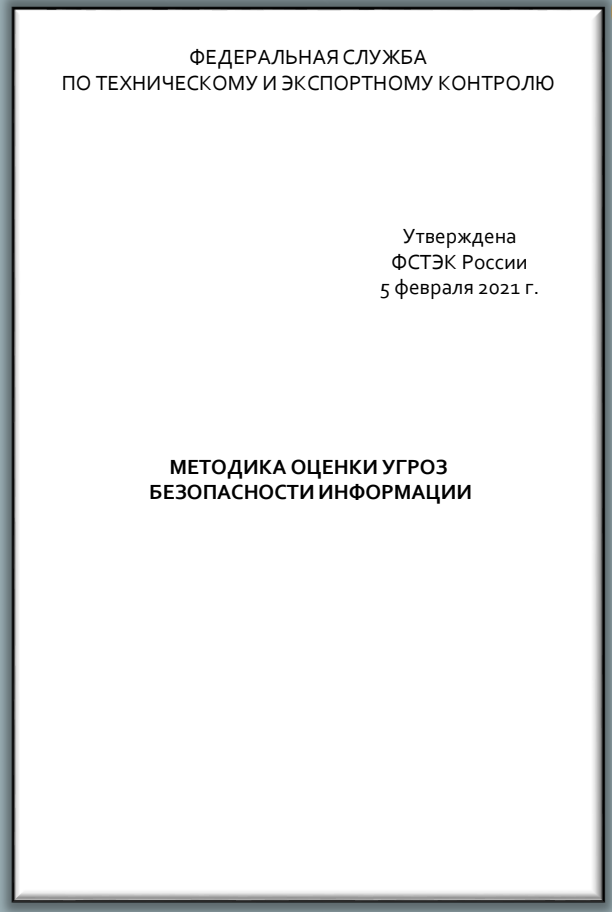
Пример 4

Идентификатор УБИ	Наименование УБИ	Источник угрозы	Способ реализации	Тактика 1	Тактика 2	Тактика 3	Тактика 4	Тактика 5	Тактика 6	Тактика 7	Тактика 8	Тактика 9	Тактика 10
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель Н4 с возможностью сговора с внутренним нарушителем (Внешний/внутренний Н4)	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных	T1.1, T1.2, T1.3, T1.4, T1.5, T1.6, T1.9, T1.11, T1.12, T1.14, T1.15, T1.16	T2.1, T2.2, T2.3, T2.4, T2.5, T2.7, T2.8, T2.9, T2.10, T2.11, T2.12, T2.13	T3.1, T3.3, T3.4, T3.5, T3.6, T3.7, T3.8, T3.9, T3.10, T3.14, T3.15, T3.16	T4.1, T4.2, T4.3, T4.4, T4.5, T4.7	T5.1, T5.2, T5.3, T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, T5.11, T5.12, T5.13	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8, T6.9	T7.1, T7.2, T7.3, T7.4, T7.6, T7.8, T7.10, T7.11, T7.12, T7.13, T7.15, T7.16, T7.17, T7.18, T7.19, T7.20, T7.21, T7.23, T7.24, T7.25, T7.26	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7, T8.8	T9.1, T9.2, T9.3, T9.5, T9.6, T9.7, T9.8, T9.9, T9.10, T9.11, T9.12, T9.13, T9.14	T10.1, T10.3, T10.4, T10.7, T10.8, T10.9
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель Н3 с возможностью сговора с внутренним нарушителем (Внешний/внутренний Н3)	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)	T1.1, T1.2, T1.3, T1.4, T1.5, T1.6, T1.9, T1.11, T1.12, T1.14, T1.15, T1.16	T2.1, T2.2, T2.3, T2.4, T2.5, T2.7, T2.8, T2.9, T2.10, T2.11, T2.12, T2.13	T3.1, T3.3, T3.4, T3.5, T3.6, T3.7, T3.8, T3.9, T3.10, T3.14, T3.15, T3.16	T4.1, T4.2, T4.3, T4.4, T4.5, T4.7	T5.1, T5.2, T5.3, T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, T5.11, T5.12, T5.13	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8, T6.9	T7.1, T7.2, T7.3, T7.4, T7.6, T7.8, T7.10, T7.11, T7.12, T7.13, T7.15, T7.16, T7.17, T7.18, T7.19, T7.20, T7.21, T7.23, T7.24, T7.25, T7.26	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7, T8.8	T9.1, T9.2, T9.3, T9.5, T9.6, T9.7, T9.8, T9.9, T9.10, T9.11, T9.12, T9.13, T9.14	T10.1, T10.3, T10.4, T10.7, T10.8, T10.9
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель Н3 с возможностью сговора с внутренним нарушителем (Внешний/внутренний Н3)	Внедрение вредоносного программного обеспечения	T1.1, T1.2, T1.3, T1.4, T1.5, T1.6, T1.9, T1.11, T1.12, T1.14, T1.15, T1.16	T2.1, T2.2, T2.3, T2.4, T2.5, T2.7, T2.8, T2.9, T2.10, T2.11, T2.12, T2.13	T3.1, T3.3, T3.4, T3.5, T3.6, T3.7, T3.8, T3.9, T3.10, T3.14, T3.15, T3.16	T4.1, T4.2, T4.3, T4.4, T4.5, T4.7	T5.1, T5.2, T5.3, T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, T5.11, T5.12, T5.13	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8, T6.9	T7.1, T7.2, T7.3, T7.4, T7.6, T7.8, T7.10, T7.11, T7.12, T7.13, T7.15, T7.16, T7.17, T7.18, T7.19, T7.20, T7.21, T7.23, T7.24, T7.25, T7.26	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7, T8.8	T9.1, T9.2, T9.3, T9.5, T9.6, T9.7, T9.8, T9.9, T9.10, T9.11, T9.12, T9.13, T9.14	T10.1, T10.3, T10.4, T10.7, T10.8, T10.9
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель Н3 с возможностью сговора с внутренним нарушителем (Внешний/внутренний Н3)	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных	T1.1, T1.2, T1.3, T1.4, T1.5, T1.6, T1.9, T1.11, T1.12, T1.14, T1.15, T1.16	T2.1, T2.2, T2.3, T2.4, T2.5, T2.7, T2.8, T2.9, T2.10, T2.11, T2.12, T2.13	T3.1, T3.3, T3.4, T3.5, T3.6, T3.7, T3.8, T3.9, T3.10, T3.14, T3.15, T3.16	T4.1, T4.2, T4.3, T4.4, T4.5, T4.7	T5.1, T5.2, T5.3, T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, T5.11, T5.12, T5.13	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8, T6.9	T7.1, T7.2, T7.3, T7.4, T7.6, T7.8, T7.10, T7.11, T7.12, T7.13, T7.15, T7.16, T7.17, T7.18, T7.19, T7.20, T7.21, T7.23, T7.24, T7.25, T7.26	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7, T8.8	T9.1, T9.2, T9.3, T9.5, T9.6, T9.7, T9.8, T9.9, T9.10, T9.11, T9.12, T9.13, T9.14	T10.1, T10.3, T10.4, T10.7, T10.8, T10.9

ОПРЕДЕЛЕНИЕ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. Выбирается некоторая начальная точка сценария
2. Проводится поиск последовательности тактик, которая потенциально может привести к получению нарушителем доступа в целевой сегмент
3. Определяются сценарии реализации угрозы безопасности информации на уровне тактик
4. Выбираются компоненты, за счет эксплуатации которых нарушителем может быть реализована каждая тактика
5. Производится поиск последовательности техник, которые позволят нарушителю создать условия, необходимые для получения доступа в следующий сегмент систем и сетей до целевого сегмента
6. Производится поиск последовательности техник в целевом сегменте

ИЗМЕНЕНИЯ В МЕТОДИКУ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ


ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утверждена
ФСТЭК России
5 февраля 2021 г.

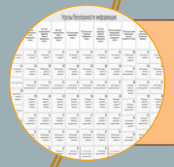
МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Изменение подхода к моделированию угроз систем и сетей в инфраструктуре поставщика услуг

Уточнение процедуры определения негативных последствий

Уточнение процедуры определения объектов воздействий

Изменение процедуры определения актуальных угроз безопасности информации



Доработка раздела угроз, содержащихся в банке данных

Автоматизация процесса формирования перечня возможных угроз

СПАСИБО ЗА ВНИМАНИЕ!

Начальник отдела управления ФСТЭК России

Гефнер Ирина Сергеевна