

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 3

Риски ИБ. Комплаенс

Спикер: Ануфриев Иван



ЗАНЯТИЕ 3.2

**Методики оценки рисков и моделирования угроз в контексте НПА РФ.
Особенности и практика применения методики ФСТЭК России**



УСЛОВНОЕ РАЗДЕЛЕНИЕ ИНФОРМАЦИИ. «МЕТКИ» НА СЛАЙДАХ

*

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.	«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
		

Рабочий «экспертный» инструментарий «Expert tools»	Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»	Метки по используемым инструментам и практикам
 (EXPERT TOOLS)	(BEST PRACTICE)	

Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
(INSIGHTS)	(COMPLIANCE) 	(BUSINESS CONTINUITY)	



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ПЕРВОЙ ЧАСТИ ЗАНЯТИЯ

(COMPLIANCE)



ВОПРОС 1.1

Исторический
трек развития
БДУ ФСТЭК

ВОПРОС 1.2

Методический
документ и
инструментарий

ВОПРОС 1.3

Для кого
обязательна
методика ФСТЭК
и кому она не
нужна

ВОПРОС 1.4

Другие методики,
методика ФСБ

ВОПРОС 1.5

Политика ЦБ в
сфере ИБ

ВОПРОС 1.6

Почему старые
модели нужно
менять

ВОПРОС 1.7

Юридический
аспект: разница
между перечнем
и моделью угроз

ВОПРОС 1.8

Чем регулируется
ответственность и
компетенции
ФСТЭК

ВОПРОС 1.9

Разбор классификации
угроз нарушения

ВОПРОС 1.10



Внутренний,
внешний
нарушители. Третьи
стороны тоже
«нарушители» ?



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ВТОРОЙ ЧАСТИ ЗАНЯТИЯ



ВОПРОС 2.1

«Helicopter view»
по треку новой
методики ФСТЭК

ВОПРОС 2.2

Пошаговый
алгоритм оценки
угроз

ВОПРОС 2.3

Схема по уровням
детализации при
составлении
модели угроз

ВОПРОС 2.4

(BEST PRACTICE)

Современные
тенденции развития
методик оценки
рисков и
моделирования
угроз

ВОПРОС 2.5

Конфликт методик
ФСБ и ФСТЭК и
необходимость
делать сразу две
модели

ВОПРОС 2.6

**(BUSINESS
CONTINUITY)**

Входные данные
для оценки угроз

ВОПРОС 2.7

**(BUSINESS
CONTINUITY)**

Системные циклы
и иные факторы
для обновления
модели угроз

ВОПРОС 2.7



БЛОК СЛАЙДОВ:
Средство
автоматизации
ФСТЭК РФ

ВОПРОС 2.8



Новый подход:
Матрица оценки
рисков и угроз



ИСТОРИЧЕСКИЙ ТРЕК РАЗВИТИЯ БДУ ФСТЭК



МЕТОДИЧЕСКИЙ ДОКУМЕНТ ФСТЭК И ДОП. ИНСТРУМЕНТАРИЙ В ПОДДЕРЖКУ



Связь угроз БДУ и мер приказов ФСТЭК 17
21.xlsx (документ в приложении)



Наименование УБИ	Описание	Источник угрозы (характеристика и потенциал нарушителя)
Объект	Последствия	Меры

2			Последствия	МЕРЫ:	ИАФ.1	ИАФ.2
4	Ид	Наименование УБИ	Описание	Ц	Д	
3		Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	1	0	
7		Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	1	0	
8			Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в			

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ
МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

МОСКВА
2021



МЕТОДИКА ОБЯЗАТЕЛЬНО РАСПРОСТРАНЯЕТСЯ НА:



Государственные и муниципальные информационные системы (ГИС и МИС)

17 приказ ФСТЭК



Информационная система персональных данных (ИСПДн)

21 приказ ФСТЭК



Значимые объекты критических субъектов информационной инфраструктуры РФ (ЗООКИИ)

239 приказ ФСТЭК



Информационная система управления производством (ИСУП), используемым организациями оборонно-промышленного комплекса

31 приказ ФСТЭК (2017)



Автоматизированные системы управления технологическим процессом (АСУ ТП)

31 приказ ФСТЭК (2014)



ОПТИМИЗИРУЕМ ЗАТРАТЫ:

В ЭТИХ СЛУЧАЯХ

ИСПОЛЬЗОВАНИЕ МЕТОДИКИ ЯВЛЯЕТСЯ ИЗЛИШНИМ:



Угрозы, связанные с шифровальными средствами



Угрозы, связанные с техническими каналами утечки информации (дсп)



Неантропогенные угрозы, вызванные не нарушителями (методика не покрывает всех антропогенных угроз)



На не системы и не сети (например в случае программного обеспечения)



ДРУГИЕ МЕТОДИКИ:

МЕТОДИКА ФСБ от 2015 года вместе с методикой ФСТЭК



**8 центр
ФСБ России
2015 г.**



**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по разработке нормативных правовых
актов, определяющих угрозы
безопасности персональных данных,
актуальные при обработке
персональных данных в
информационных системах
персональных данных,
эксплуатируемых при осуществлении
соответствующих видов
деятельности.pdf**
(документ в приложении)



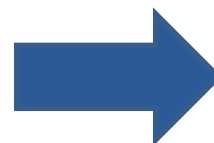
**МЕТОДИЧЕСКИЙ ДОКУМЕНТ
Методика оценки угроз
безопасности
информации.pdf**
(документ в приложении)



**ФСТЭК
России
2022 г.**



**«Для всех СКЗИ,
используемых в ГИС,
потребуется проводить
определение класса СКЗИ
по новым требованиям»**



**Памятка по согласованию моделей
угроз с ФСБ России.pdf**
(документ в приложении)



ПОЛИТИКА ЦБ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ. ДОКУМЕНТЫ БАНКА РОССИИ ПО МОДЕЛИРОВАНИЮ УГРОЗ



Банк России

Центральный банк Российской Федерации

- Контроль за соблюдение требований в части информации для участников кредитно финансовой, страховой сферы, национальной платежной системы
- Разработки основных направлений развития информационной безопасности кредитно-финансовой сферы

TADVISER:

«1 декабря 2022 года стало известно о решении [ЦБ РФ](#) регулировать наем [банками](#) ИТ-специалистов, работающих по схеме [аутсорсинга](#)»



BANKI.RU:

«ЦБ планирует в 2022 году продолжить проводить киберучения у финорганизаций»

Занятие

«Риски ИБ при выборе аутсорсинговой модели»



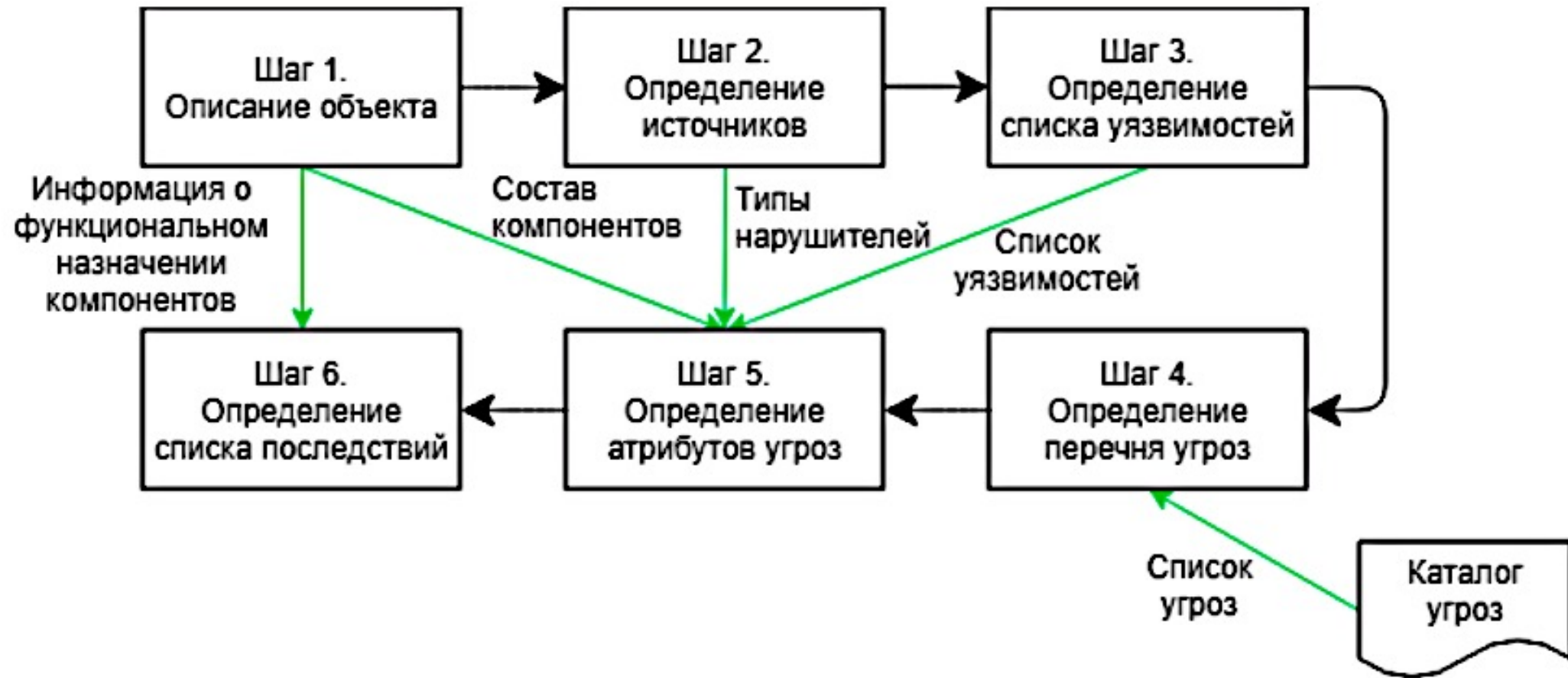
Указание Банка России 3889-У
Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных.pdf
(документ в приложении)



Указание Банка России от 16 декабря 2021 г. № 6017-У "О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой.pdf
(документ в приложении)

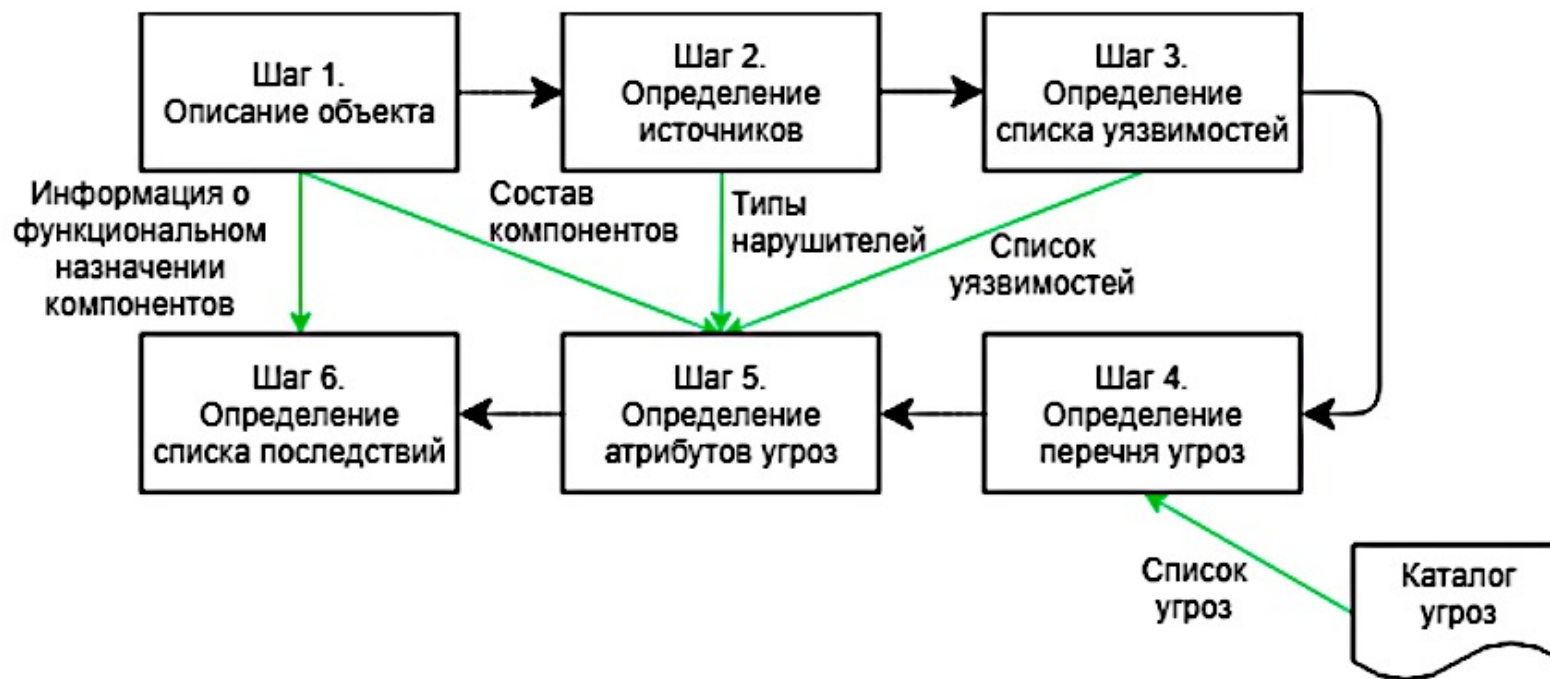


МОДЕЛИРОВАНИЕ УГРОЗ В УСЛОВИЯХ МЕТОДИЧЕСКОЙ НЕОПРЕДЕЛЕННОСТИ (СХЕМА ПРОЦЕССА – ЛАБОРАТОРИЯ КАСПЕРСКОГО).



СУЩЕСТВУЮЩИЕ МОДЕЛИ УГРОЗ «В КОРЗИНУ».

МОДЕЛИРОВАНИЕ УГРОЗ В УСЛОВИЯХ МЕТОДИЧЕСКОЙ НЕОПРЕДЕЛЕННОСТИ



*Вспомним первые занятия:
«при изменении структуры
бизнес-процессов зачастую
меняется и структура ИТ-
процессов, поэтому
меняется модель угроз»*



Модели угроз, разработанные и утвержденные до 5 февраля 2021 года продолжают действовать, подвергаются изменению лишь при изменении бизнес-процессов, но фактически – они устаревают...



ЮРИДИЧЕСКИЙ АСПЕКТ: В ЧЕМ РАЗНИЦА МЕЖДУ МОДЕЛЮ И ПЕРЕЧНЕМ УГРОЗ ?

МОДЕЛЬ УГРОЗ

VS

ПЕРЕЧЕНЬ УГРОЗ

*МОДЕЛЬ УГРОЗ ДОПОЛНИТЕЛЬНО
СОГЛАСОВЫВАТЬ НЕ НУЖНО
(ИСКЛЮЧАЯ ГОСОРГАНЫ)*

*ПЕРЕЧЕНЬ В ОТЛИЧИЕ ОТ МОДЕЛИ
НЕ ВКЛЮЧАЕТ ОБОСНОВАНИЕ
ВЫБОРА АКТУАЛЬНЫХ УГРОЗ*

- описание информационной системы
- структурно-функциональные характеристики
 - описание угроз безопасности
 - модель нарушителя
 - возможные уязвимости
 - способы реализации угроз
- последствия от нарушения свойств безопасности информации.

- Нежелательный контент.
Несанкционированный доступ. Утечки информации.
 - Потеря данных.
Мошенничество.
 - Кибервойны
 - Кибертерроризм.



РАЗБОР КЛАССИФИКАЦИИ УГРОЗ НАРУШЕНИЯ:

 КОНФИДЕНЦИАЛЬНОСТИ

 ЦЕЛОСТНОСТИ

 ДОСТУПНОСТИ

 АУТЕНТИЧНОСТИ

 НЕОТКАЗУЕМОСТИ

 ПОДОТЧЕТНОСТИ

 ДОСТОВЕРНОСТИ



ЧЕМ РЕГУЛИРУЕТСЯ ОТВЕТСТВЕННОСТЬ ФСТЭК



УКАЗ ПРЕЗИДЕНТА РФ №1085

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ВОПРОСЫ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Список изменяющих документов
(в ред. Указов Президента РФ от 22.03.2005 N 330,
от 20.07.2005 N 846, от 30.11.2006 N 1321,
от 23.10.2008 N 1517, от 17.11.2008 N 1625,
от 08.02.2012 N 146, от 29.06.2013 N 593,
от 21.12.2013 N 940, от 01.09.2014 N 606,
от 28.10.2014 N 689, от 20.01.2015 N 26,
от 31.12.2015 N 682, от 25.11.2017 N 569,
от 08.05.2018 N 207, от 13.06.2019 N 266)

(Выписка)

1. Утвердить прилагаемое Положение о Федеральной службе по техническому и экспортному контролю.



ПОЛОЖЕНИЕ О ФСТЭК

Москва, Кремль
16 августа 2004 года
N 1085

Президент
Российской Федерации
В.Путин

УТВЕРЖДЕНО
Указом Президента
Российской Федерации
от 16 августа 2004 года N 1085

ПОЛОЖЕНИЕ

о Федеральной службе по техническому и экспортному контролю

(с изменениями на 8 декабря 2021 года)

I. Общие положения

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

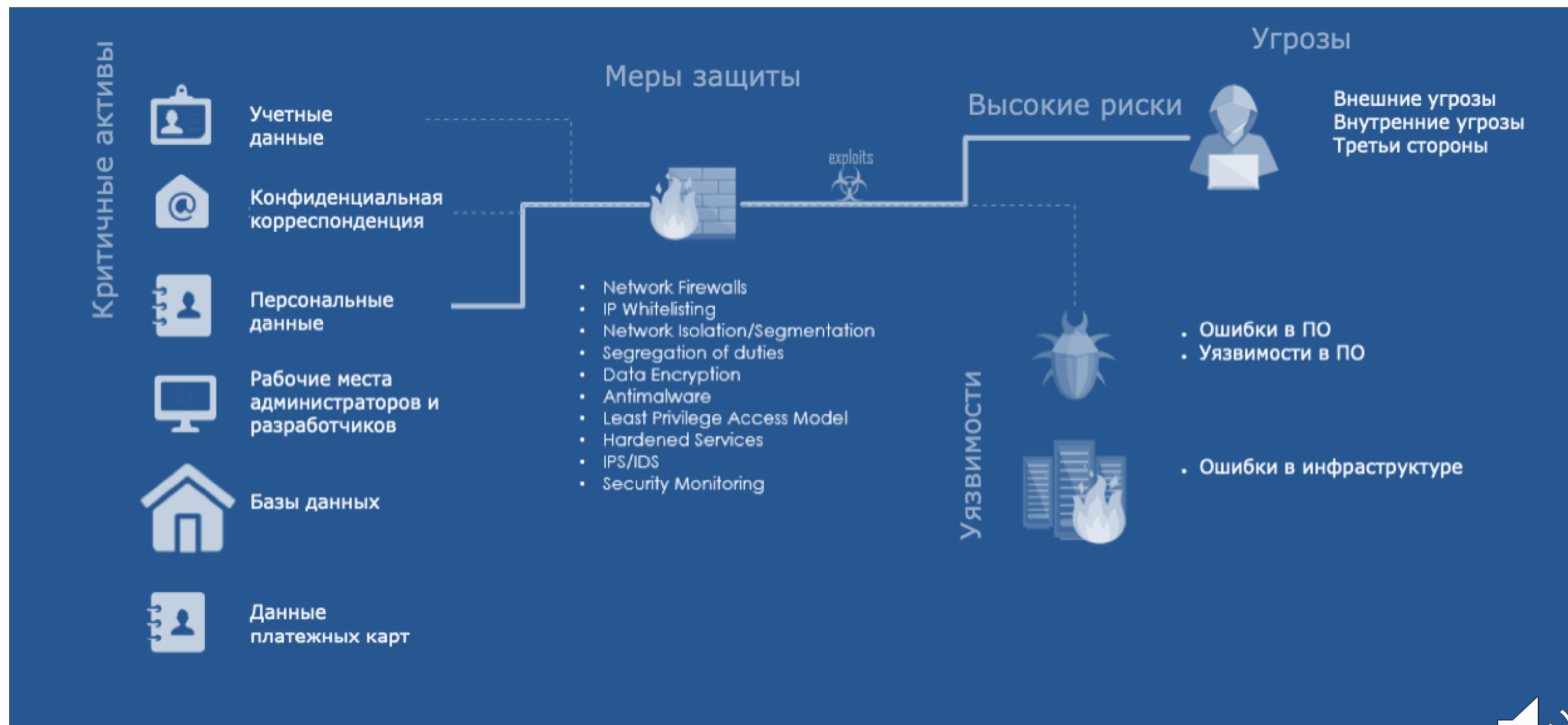
1) обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура);

(Подпункт в редакции, введенной в действие с 1 января 2018 года Указом Президента Российской Федерации от 25 ноября 2017 года N 569. - См. предыдущую редакцию)



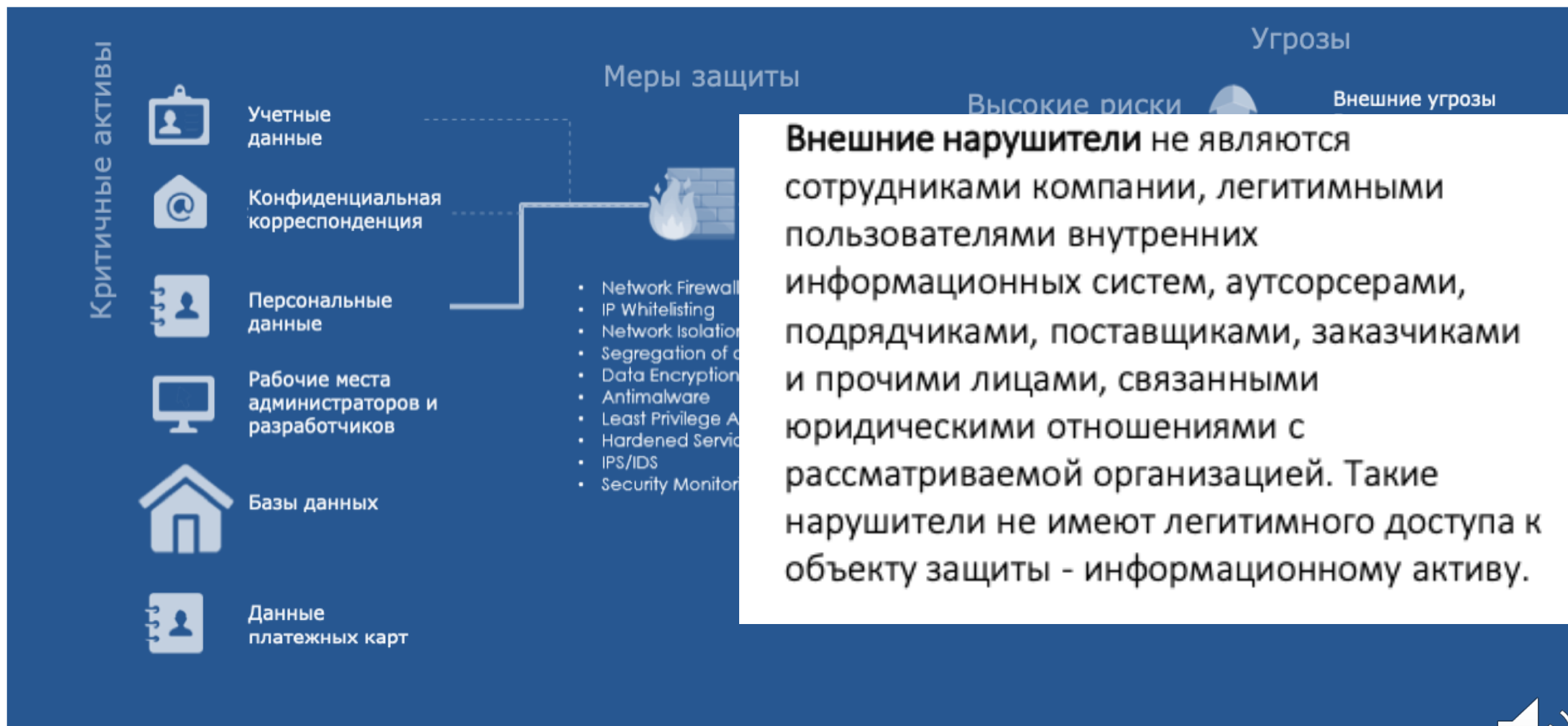


МОДЕЛЬ УПРАВЛЕНИЯ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



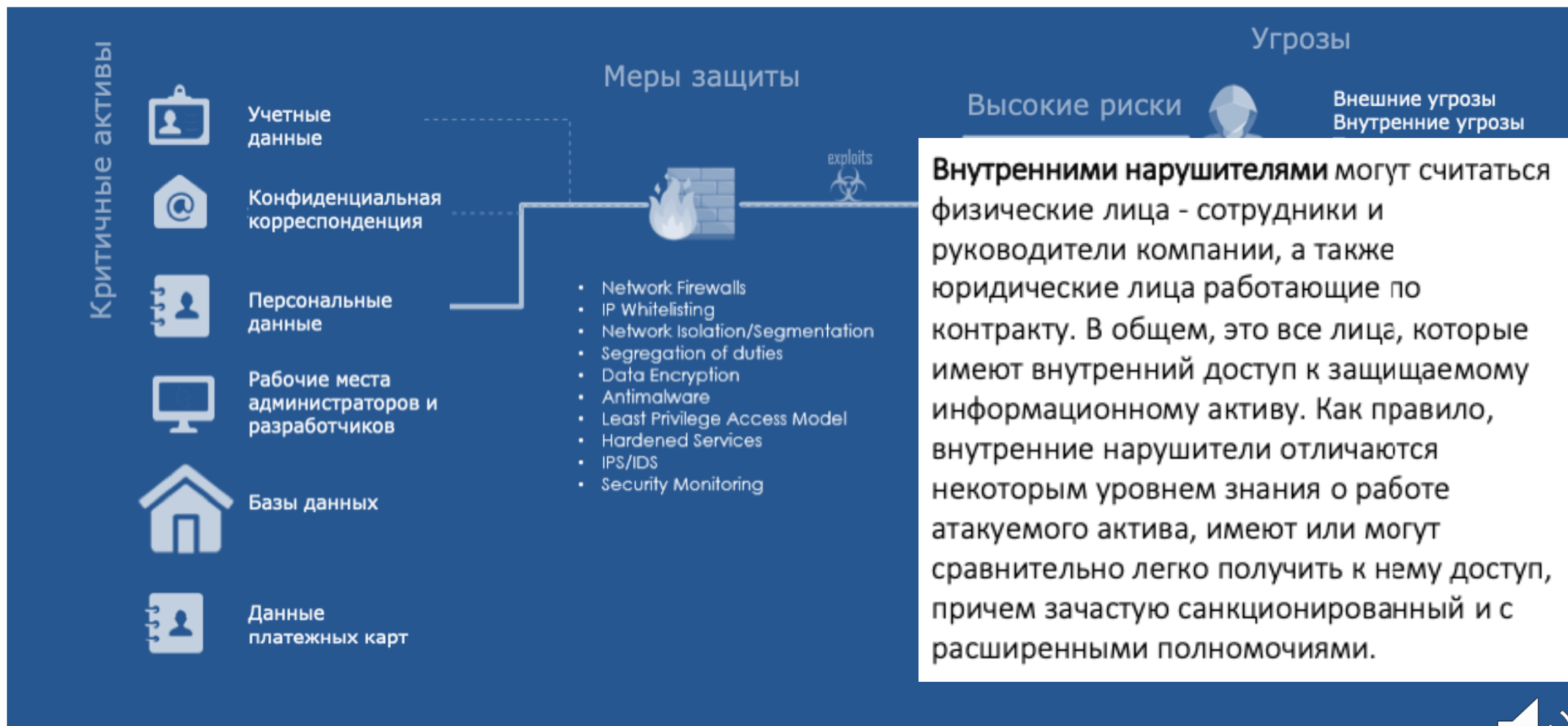


МОДЕЛЬ УПРАВЛЕНИЯ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



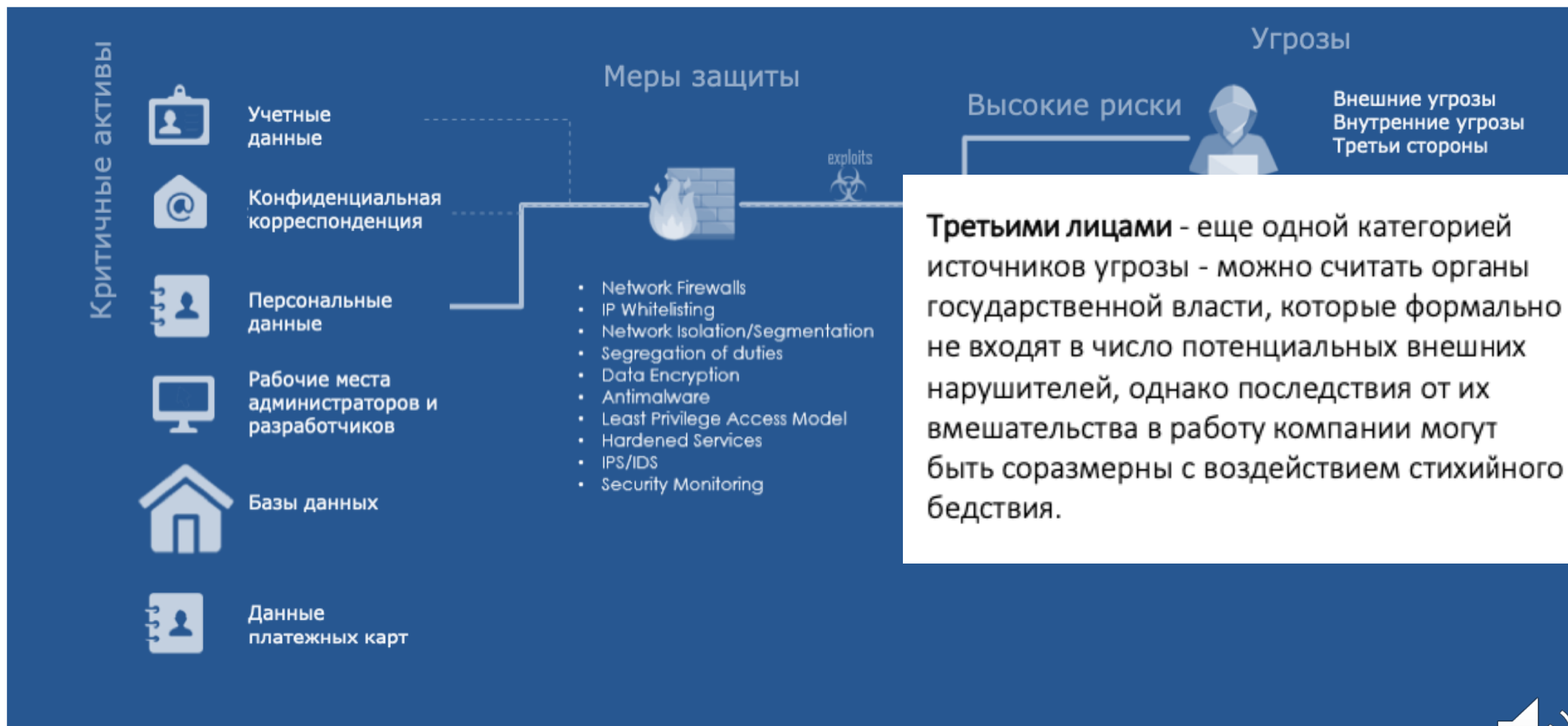


Модель управления угрозами информационной безопасности





С ПОЗИЦИИ БИЗНЕСА ТРЕТЬИ СТОРОНЫ – ЭТО ТОЖЕ УГРОЗА ?



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ВТОРОЙ ЧАСТИ ЗАНЯТИЯ

ВОПРОС 2.1

«Helicopter view»
по треку новой
методики ФСТЭК

ВОПРОС 2.2

Пошаговый
алгоритм оценки
угроз

ВОПРОС 2.3

Схема по уровням
детализации при
составлении
модели угроз

ВОПРОС 2.4

(BEST PRACTICE)

Современные
тенденции развития
методик оценки
рисков и
моделирования
угроз

ВОПРОС 2.5

Конфликт методик
ФСБ и ФСТЭК и
необходимость
делать сразу две
модели

ВОПРОС 2.6

**(BUSINESS
CONTINUITY)**

Входные данные
для оценки угроз

ВОПРОС 2.7

**(BUSINESS
CONTINUITY)**

Системные циклы
и иные факторы
для обновления
модели угроз



«HELICOPTER VIEW» ПО ТРЕКУ НОВОЙ МЕТОДИКИ ФСТЭК

В СЛУЧАЕ, ЕСЛИ ИСПОЛЬЗОВАНИЕ СРЕДСТВ АВТОМАТИЗАЦИИ НЕ ПРЕДУСМОТРЕНО

1 БЕРЕМ ВСЕ УГРОЗЫ

ИСКЛЮЧАЕМ угрозы которые:

- *Не приводят к негативным последствиям*
- *Не связаны с нарушителями нужного типа*
- *Не связаны с нашими активами*
- *Требует от нарушителей доступа, которого у них нет*

2 СМОТРИМ НА ОСТАВШЕЕСЯ УГРОЗЫ

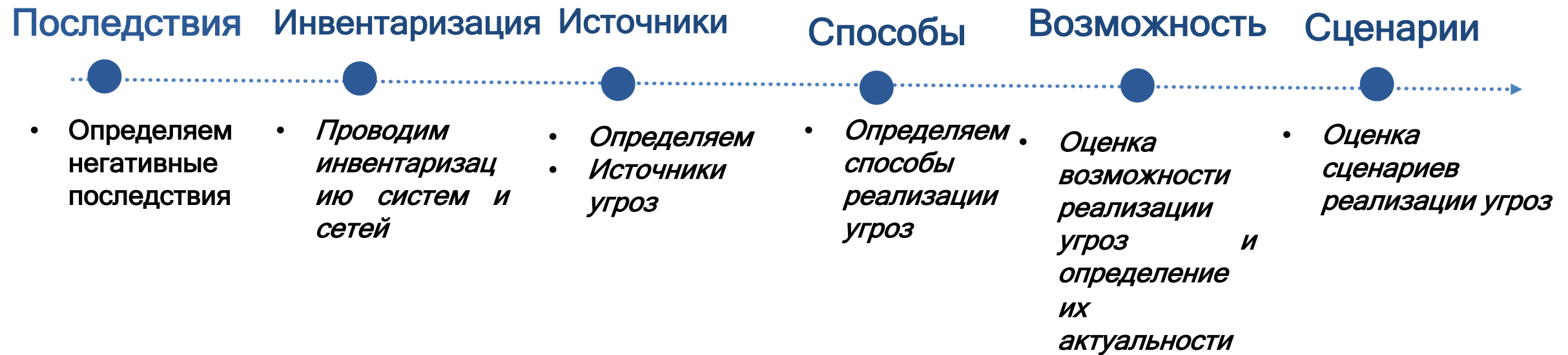
- *ПОДБИРАЕМ
ВСЕ
ВОЗМОЖНЫЕ
СЦЕНАРИИ
РЕАЛИЗАЦИИ
УГРОЗ (10 ТАКТИК
145 ТЕХНИК)*

3 РАНЖИРУЕМ УГРОЗЫ

- *ПРОВОДИМ ОЦЕНКУ
УГРОЗ ПО
ЗНАЧИМОСТИ ДЛЯ
НАС (ПЕРВИЧНАЯ
ОЦЕНКА РИСКОВ)*



ТЕПЕРЬ РАССМОТРИМ ПОШАГОВО ЭТАПЫ ОЦЕНКИ УГРОЗ



УРОВНИ ДЕТАЛИЗАЦИИ ПРИ СОСТАВЛЕНИИ МОДЕЛИ УГРОЗ



СОВРЕМЕННЫЕ МЕТОДИКИ ОЦЕНКИ УГРОЗ



Обзор современных тенденций развития методик оценки рисков и моделирования угроз



КОНФЛИКТ ПОДХОДОВ ФСБ И ФСТЭК ПРИ ОЦЕНКЕ УГРОЗ

Разные модели, разные подходы , разные миры....



ФСБ России

Моделирование угроз по методике ФСБ

В ЧЕМ ПРИНЦИПИАЛЬНАЯ ОСОБЕННОСТЬ ?

- КОНКРЕТНЫЕ ИНДИКАТОРЫ, КОТОРЫЕ РАССЫЛАЮТСЯ В БЮЛЛЕТЕНЯХ



ФСТЭК России

Моделирование угроз по методике ФСТЭК

В ЧЕМ СУТЬ ?

- МОДЕЛИРОВАНИЕ УГРОЗ ИСХОДЯ ИЗ ТЕХНИК И ТАКТИК

В госорганах где есть криптография, по факту нужно делать и согласовывать сразу 2 типа моделей по методике ФСТЭК и по методике ФСБ.

А моделей может быть много



ВХОДНЫЕ ДАННЫЕ ДЛЯ ОЦЕНКИ УГРОЗ. НЕПРЕРЫВНОСТЬ ОБНОВЛЕНИЯ



Перечень угроз

Угрозы берем из Банка данных угроз ФСТЭК

Описание векторов компьютерных атак или их типовых сценариев

CAPEC, ATT&CK, OWASP

Документация на системы и сети

239 приказ ФСТЭК

Риски

Результаты оценки рисков по существующим системам, которые мы определяем как критичные

Договора

Как пример – с сервис-провайдером

НПА

Все нормативно-правовые акты по создаваемым системам

Критичные процессы

Список критичных процессов как в корпоративном сегменте, так и в бизнес-сегменте



СИСТЕМНЫЕ ЦИКЛЫ И ИНЫЕ ФАКТОРЫ ПРИ КОТОРЫХ ВОЗНИКАЕТ НЕОБХОДИМОСТЬ В ПЕРЕОЦЕНКЕ УГРОЗ

**BUSINESS
CONTINUITY**



Создание



- На данном этапе учитывается большинство угроз и их нейтрализация может быть обеспечена при минимальных усилиях

Эксплуатация



- На данном этапе жизненного цикла в большинстве случаев оцениваются угрозы. Наиболее валидно для систем с длинным жизненным циклом оцениваются угрозы

Модернизация



- Любое изменение бизнес-процесса, приводящее к модернизации ИТ-систем, приводит к необходимости переоценки модели угроз

Изменение НПА,

Изменение архитектуры, условий функционирования систем и сетей, режима обработки информации

Выявление новых угроз или новых сценариев реализации угроз, обновление БДУ

ПОЛИТИКА НЕПРЕРЫВНОЙ ОЦЕНКИ УГРОЗ. Оценка угроз осуществляется:

По результатам инвентаризации информационных ресурсов

По результатам анализа уязвимостей

По результатам теста на проникновение

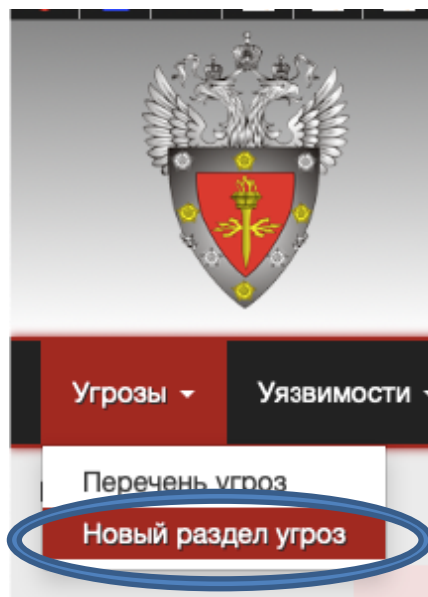


ВСПОМИНАЕМ СЛАЙДЫ «ИЗ ПРОШЛОГО»:

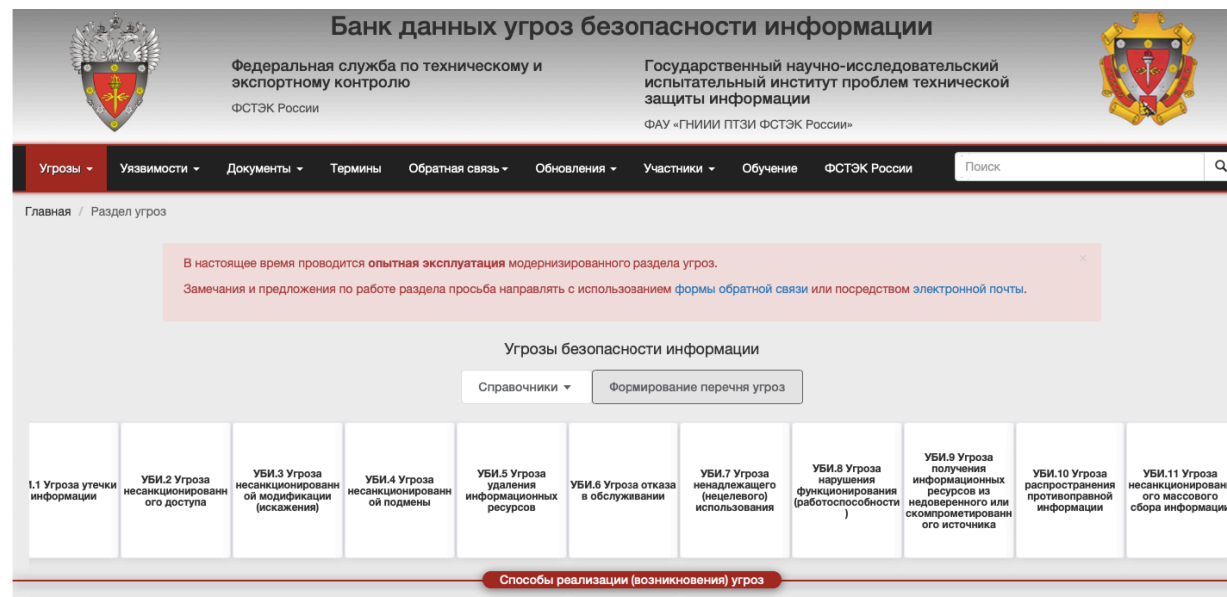
КАК МОДЕЛИРОВАТЬ КИБЕРАТАКИ, ОПИРАЯСЬ НА МЕТОДИКУ ФСТЭК ?



Банк данных угроз информационной безопасности



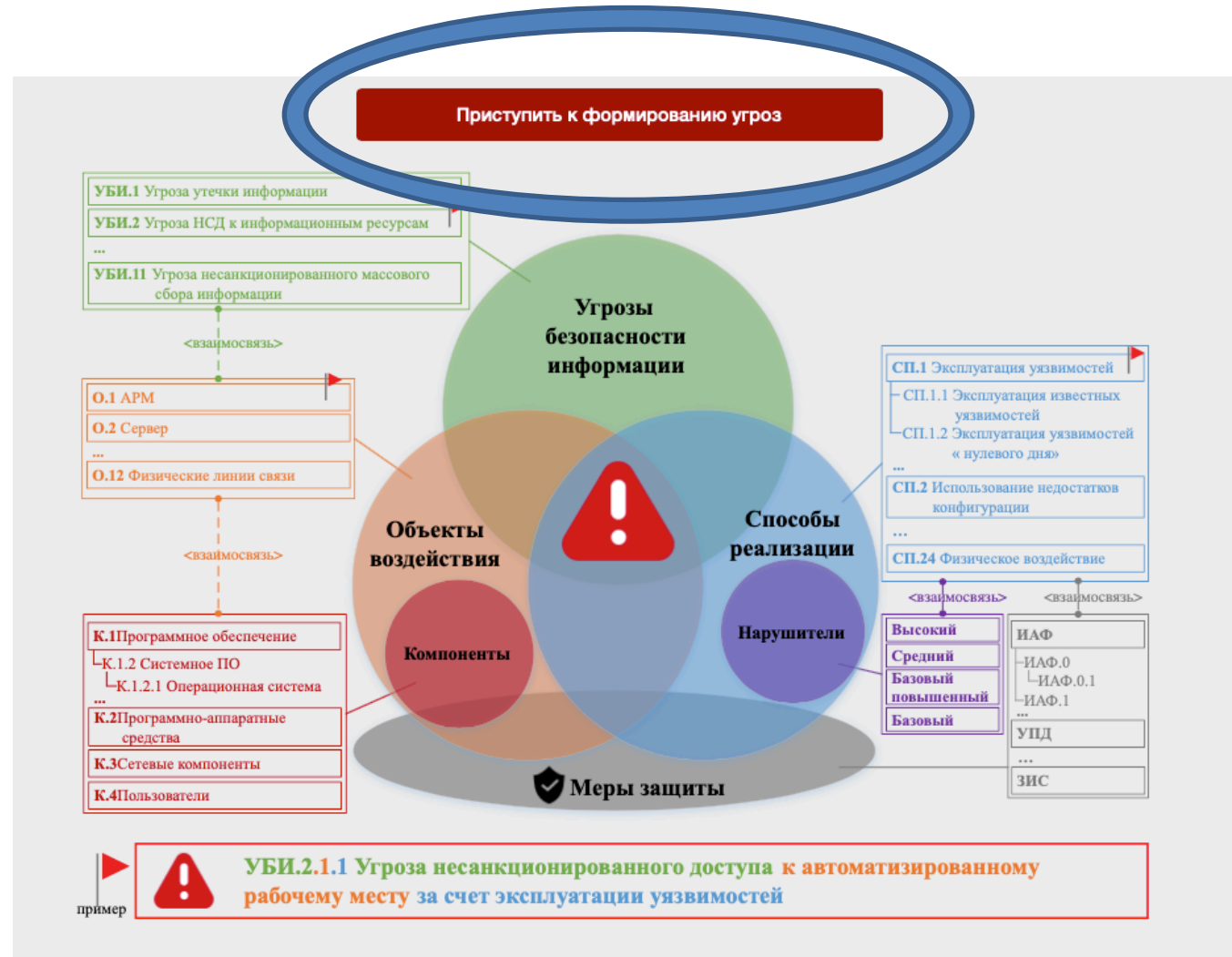
<https://bdu.fstec.ru>





Формирование перечня возможных УБИ

По модели ФСТЭК





Негативные последствия

Перечень

Справочники

Негативные последствия

Угрозы

Объекты

Компоненты

Способы реализации

Нарушители

Меры защиты

1 Начальная страница

2 Негативные последствия

3 Угрозы

4 Объекты воздействия

5 Компоненты

6 Нарушитель

7 Результат

←

Выберите негативные последствия

?

☒ Н.1 Угроза жизни или здоровью.

☒ Н.2 Нарушение неприкосновенности частной жизни.

☒ Н.3 Нарушение личной, семейной тайны, утрата чести и доброго имени.

☒ Н.4 Нарушение тайны переписки, телефонных переговоров, иных сообщений.

☒ Н.5 Нарушение иных прав и свобод гражданина, закрепленные в Конституции Российской Федерации и федеральных законах.

☒ Н.6 Финансовый, иной материальный ущерб физического лица.

☒ Н.7 Нарушение конфиденциальности (утечка) персональных данных.

☒ Н.8 Разглашение персональных данных граждан.

☒ Н.9 Нарушение законодательства Российской Федерации.

☒ Н.10 Потеря (хищение) денежных средств.

☒ Н.11 Недополучение ожидаемой (прогнозируемой) прибыли.

☒ Н.12 Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.





Угрозы безопасности информации

Раздел из справочника ФСТЭК

 | Выберите угрозы 

- ☒ УБИ.1 Угроза утечки информации
- ☒ УБИ.2 Угроза несанкционированного доступа
- ☒ УБИ.3 Угроза несанкционированной модификации (искажения)
- ☒ УБИ.4 Угроза несанкционированной подмены
- ☒ УБИ.5 Угроза удаления информационных ресурсов
- ☒ УБИ.6 Угроза отказа в обслуживании
- ☒ УБИ.7 Угроза ненадлежащего (нецелевого) использования
- ☒ УБИ.8 Угроза нарушения функционирования (работоспособности)
- ☒ УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника
- ☒ УБИ.10 Угроза распространения противоправной информации
- ☒ УБИ.11 Угроза несанкционированного массового сбора информации

Назад

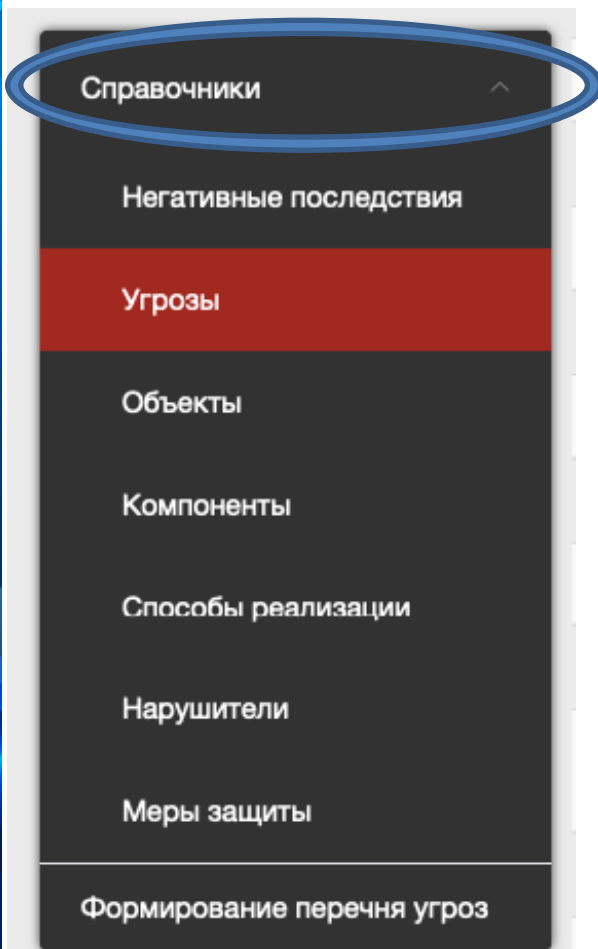
Далее





Угрозы безопасности информации

Раздел из справочника ФСТЭК



Перечень угроз безопасности информации	
УБИ.1	Угроза утечки информации ?
УБИ.2	Угроза несанкционированного доступа ?
УБИ.3	Угроза несанкционированной модификации (искажения) ?
УБИ.4	Угроза несанкционированной подмены ?
УБИ.5	Угроза удаления информационных ресурсов ?
УБИ.6	Угроза отказа в обслуживании ?
УБИ.7	Угроза ненадлежащего (нецелевого) использования ?
УБИ.8	Угроза нарушения функционирования (работоспособности) ?
УБИ.9	Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника ?
УБИ.10	Угроза распространения противоправной информации ?
УБИ.11	Угроза несанкционированного массового сбора информации ?



КАК МОДЕЛИРОВАТЬ КИБЕРАТАКИ, ОПИРАЯСЬ НА МЕТОДИКУ ФСТЭК ?



Угрозы

Справочники

Перечень возможных угроз безопасности информации

- УБИ.1** Угроза утечки информации
- УБИ.2** Угроза несанкционированного доступа
- УБИ.3** Угроза несанкционированной модификации (искажения)
- УБИ.4** Угроза несанкционированной подмены
- УБИ.5** Угроза удаления информационных ресурсов
- УБИ.6** Угроза отказа в обслуживании
- УБИ.7** Угроза ненадлежащего (нецелевого) использования
- УБИ.8** Угроза нарушения функционирования (работоспособности)
- УБИ.10** Угроза распространения противоправной информации
- УБИ.11** Угроза несанкционированного массового сбора информации



- УБИ.2.2.1** Угроза несанкционированного доступа к серверу за счет эксплуатации уязвимостей
- УБИ.2.2.2** Угроза несанкционированного доступа к серверу за счет использования недостатков конфигурации
- УБИ.2.2.3** Угроза несанкционированного доступа к серверу за счет использования недостатков архитектуры
- УБИ.2.2.4** Угроза несанкционированного доступа к серверу за счет внедрения вредоносного программного обеспечения
- УБИ.2.2.7** Угроза несанкционированного доступа к серверу за счет прослушивания (захвата) сетевого трафика
- УБИ.2.2.10** Угроза несанкционированного доступа к серверу за счет атаки типа "человек посередине"
- УБИ.2.2.13** Угроза несанкционированного доступа к серверу за счет реализации социальной инженерии
- УБИ.2.2.17** Угроза несанкционированного доступа к серверу за счет подбора (восстановления) аутентификационной информации
- УБИ.2.2.18** Угроза несанкционированного доступа к серверу за счет использования недостатков механизмов разграничения доступа

бросить результат





Объекты

Перечень объектов воздействия злоумышленника совершения

Перечень объектов воздействия	
Справочники	O.1 Автоматизированное рабочее место ?
Негативные последствия	O.2 Сервер ?
Угрозы	O.3 Периферийное оборудование ?
Объекты	O.4 Устройство хранения данных ?
Компоненты	O.5 Устройство интернета-вещей ?
Способы реализации	O.6 Активное сетевое оборудование ?
Нарушители	O.7 Обеспечивающие системы ?
Меры защиты	O.8 Телефония (VoIP, GSM) ?
Формирование перечня угроз	O.9 Средства защиты информации ?
	O.10 Мобильное устройство ?
	O.11 Информация (данные), содержащаяся в системах и сетях ?
	O.12 Физические линии связи ?





Компоненты

Перечень компонентов воздействия – справочники

Перечень компонентов объектов воздействия	
Q	Контекстный поиск
>	K.1 Программное обеспечение
>	K.2 Программно-аппаратные средства
>	K.3 Сетевые компоненты
>	K.4 Пользователи

K.1 Программное обеспечение	
▼	K.1.1 Микропрограммное обеспечение
	K.1.1.1 Прошивка (встроенная микропрограмма)
	K.1.1.2 UEFI/BIOS
▼	K.1.2 Системное программное обеспечение (ПО)
	K.1.2.1 Операционная система
	K.1.2.2 Мобильная операционная система
	K.1.2.3 Программная оболочка
	K.1.2.4 Драйвер
	K.1.2.5 Утилита
	K.1.2.6 Загрузчик операционной системы
	K.1.2.7 Гипервизор



КАК МОДЕЛИРОВАТЬ КИБЕРАТАКИ, ОПИРАЯСЬ НА МЕТОДИКУ ФСТЭК ?



Компоненты

Перечень компонентов воздействия

←

Выберите компоненты объектов воздействия

?

О.2 Сервер

Основные компоненты

☒ К.1.1.1 Прошивка (встроенная микропрограмма)

☒ К.1.1.2 UEFI/BIOS

☒ К.1.2.1 Операционная система

☒ К.1.2.3 Программная оболочка

☒ К.1.2.4 Драйвер

☒ К.1.2.6 Загрузчик операционной системы

☒ К.1.3.1 Системные и сетевые службы

☒ К.2.2.8 Сетевой интерфейс

☒ К.4.1.1 Администратор

Дополнительные компоненты

>

О.5 Устройство интернета-вещей

Основные компоненты

☒ К.1.1.1 Прошивка (встроенная микропрограмма)

Дополнительные компоненты

>

Назад

Далее





Нарушители

Внутренний и внешний нарушители – справочники

- > **V.1** Нарушитель, обладающий базовыми возможностями
- > **V.2** Нарушитель, обладающий базовыми повышенными возможностями
- > **V.3** Нарушитель, обладающий средними возможностями
- > **V.4** Нарушитель, обладающий высокими возможностями

> **V.1** Нарушитель, обладающий базовыми возможностями

< **V.2** Нарушитель, обладающий базовыми повышенными возможностями

Описание: Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами, однако хорошо владеют этими средствами и инструментами, понимают, как они работают и могут вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеют знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.

Типы нарушителей: Преступные группы (два лица и более, действующие по единому плану)
Конкурирующие организации
Поставщики вычислительных услуг, услуг связи
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ
Системные администраторы и администраторы безопасности

> **V.3** Нарушитель, обладающий средними возможностями

> **V.4** Нарушитель, обладающий высокими возможностями





Нарушители

Внутренний и внешний нарушители – выбираем нарушителей

Progress bar: 1. Начальная страница (✓) 2. Негативные последствия (✓) 3. Угрозы (✓) 4. Объекты воздействия (✓) 5. Компоненты (✓) 6. **Нарушитель** (6) 7. Результат (7)

← | Выберите уровень возможностей нарушителей

- ☒ В.1 Нарушитель, обладающий базовыми возможностями ?
- ☒ В.2 Нарушитель, обладающий базовыми повышенными возможностями ?
- ☒ В.3 Нарушитель, обладающий средними возможностями ?
- ☐ В.4 Нарушитель, обладающий высокими возможностями ?

Назад Далее





Способы реализации угроз

Перечень способов реализации угроз

6.2	УБИ.6.2.2 Угроза вызова отказа в обслуживании сервера за счет использования недостатков конфигурации
Описание	Угроза заключается в недоступности информационной системы или ее компонентов и (или) приостановлении оказания услуг или предоставления сервисов для авторизованных пользователей. Например, угроза отказ в доступе к Интернет-сайту авторизованным пользователям
Объект	О.2
Компоненты	К.1.1.1, К.1.1.2, К.1.2.1, К.1.2.2, К.1.2.3, К.1.2.4, К.1.2.5, К.1.2.6, К.1.2.7, К.1.3.1, К.1.3.2, К.1.3.3, К.1.3.4, К.1.3.5, К.1.3.6, К.1.3.7, К.1.3.8, К.1.3.9, К.1.3.10, К.1.4.1, К.1.4.2, К.1.5.1, К.1.5.2, К.1.5.3, К.1.5.4, К.1.5.5, К.1.5.6, К.1.5.7, К.1.5.8, К.1.5.9, К.1.5.10, К.1.5.11, К.1.5.12, К.1.5.13, К.1.5.14, К.1.5.15, К.1.5.16, К.1.6.1, К.1.6.2, К.1.6.3, К.1.6.4, К.1.6.5, К.1.6.6, К.1.6.7, К.1.7.1, К.1.7.2, К.1.7.3, К.1.7.4, К.2.5.1
Способы реализации угрозы	СП.2.1, СП.2.2, СП.2.3, СП.2.7, СП.2.8, СП.2.9, СП.2.10, СП.2.11
Потенциал нарушителя	В.1, В.2
Возможные меры защиты	АУД.1.3, ЗИС.2.2, ЗИС.26.1, ЗИС.26.2, ЗИС.27.1, ЗИС.28.1, ЗИС.28.3, ЗИС.29.1, ЗИС.29.3, ЗИС.31.1, ЗИС.32.1, ЗИС.32.2, ЗИС.32.3, ЗИС.35.1, ЗИС.35.2, ЗИС.35.5, ИАФ.4.2, ОЦЛ.3.1, ОЦЛ.4.2, УКФ.0.1, УКФ.1.1, УКФ.1.2, УКФ.2.2, УКФ.4.1, УПД.1.1, УПД.1.2, УПД.1.3, УПД.1.4, УПД.1.5, УПД.1.6, УПД.1.7, УПД.1.8, УПД.1.9, УПД.2.1, УПД.2.2, УПД.2.3, УПД.3.2, УПД.4.1, УПД.5.1, УПД.6.2, УПД.13.1, УПД.13.2, УПД.13.3, УПД.13.5, УПД.14.1, УПД.14.2



←	СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных	?
Группа способов:	СП.2 Использование недостатков конфигурации	
Способ реализации:	СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных	
Уровень возможностей нарушителя:	В.2	
Возможные реализуемые угрозы:	УБИ.1, УБИ.2, УБИ.3, УБИ.4, УБИ.5, УБИ.6, УБИ.7, УБИ.8, УБИ.9, УБИ.10, УБИ.11	
Компоненты объектов воздействия:	К.1.1.1, К.1.1.2, К.1.2.1, К.1.2.2, К.1.2.3, К.1.2.4, К.1.2.5, К.1.2.6, К.1.2.7, К.1.3.1, К.1.3.2, К.1.3.3, К.1.3.6, К.1.3.7, К.1.3.8, К.1.3.9, К.1.3.10, К.1.4.1, К.1.4.2, К.1.5.1, К.1.5.2, К.1.5.3, К.1.5.4, К.1.5.5, К.1.5.6, К.1.5.7, К.1.5.8, К.1.5.9, К.1.5.10, К.1.5.11, К.1.5.12, К.1.5.13, К.1.5.14, К.1.5.15, К.1.5.16, К.1.6.1, К.1.6.2, К.1.6.3, К.1.6.4, К.1.6.5, К.1.6.6, К.1.6.7, К.1.7.1, К.1.7.2, К.1.7.3, К.1.7.4, К.2.5.1	
Возможные меры защиты:	ОЦЛ.3.1, ОЦЛ.4.2, УКФ.2.2, УКФ.4.1	





Способы реализации угроз

Перечень способов реализации угроз - справочники

Справочники

Негативные последствия

Угрозы

Объекты

Компоненты

Способы реализации

Нарушители

Меры защиты

Формирование перечня угроз

Кontекстный поиск

СП.1 Эксплуатация уязвимостей

СП.1.1 Эксплуатация известных уязвимостей

СП.1.2 Эксплуатация уязвимостей "нулевого дня"

СП.2 Использование недостатков конфигурации

СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных

СП.2.2 Использование недостатков, связанных с управлением учетными данными

СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя

СП.2.4 Использование недостатков, связанных с хранением ключевой информации в программном коде (в оперативной памяти)

СП.2.5 Использование недостатков, связанных с передачей ключевой информации по системным шинам

СП.2.6 Использование недостатков, связанных с использованием нестойкой криптографии

СП.2.7 Использование недостатков, связанных с некорректной настройкой сетевого доступа





Меры защиты

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий – справочники

Группы мер защиты информации

Справочники

- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты**
- Формирование перечня угроз

Контекстный поиск

AB3 Антивирусная защита

- AB3.0 Регламентация правил и процедур антивирусной защиты
 - AB3.0.1 Разработка правил и процедур (политик) антивирусной защиты
- AB3.1 Реализация антивирусной защиты
 - AB3.1.1 Применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационной системе, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы)
 - AB3.1.2 Установка, конфигурирование и управление средствами антивирусной защиты
 - AB3.1.3 Предоставление доступа средствам антивирусной защиты к информационной системе, которые должны быть подвергнуты проверке средством антивирусной защиты
 - AB3.1.4 Проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на

- > AB3 Антивирусная защита
- > АУД Аудит безопасности
- > ДНС Обеспечение действий в нестандартных ситуациях
- > ЗИС Защита информационной (автоматизированной) системы и ее компонентов
- > ЗНИ Защита машинных носителей информации
- > ЗТС Защита технических средств и систем
- > ИАФ Идентификация и аутентификация
- > ИНЦ Реагирование на компьютерные инциденты
- > ИПО Информирование и обучение персонала
- > ОДТ Обеспечение доступности
- > ОПО Управление обновлениями программного обеспечения
- > ОПС Ограничение программной среды
- > ОЦЛ Обеспечение целостности
- > ПЛН Планирование мероприятий по обеспечению безопасности
- > СОВ Предотвращение вторжений (компьютерных атак)
- > УКФ Управление конфигурацией
- > УПД Управление доступом



ЗАЧЕМ ЭТО ? ПОКАЖЕМ НА СЛАЙДЕ«ИЗ БУДУЩЕГО»:
НА ОСНОВАНИИ ДАННЫХ ВЫБИРАЕМ МЕРЫ ЗАЩИТЫ. ЗАПОЛНЯЕМ МАТРИЦУ УГРОЗ И МЕР ЗАЩИТЫ



Унификация мер по одному стандарту для предприятия.
Унифицируем меры в таблица с перечнем конкретных мер и указанием, для каких типов систем эти меры должны применяться.

Направление Защиты	Группа мер	Мера защиты	Применимость согласно техническому стандарту ИБ					Группы угроз
			ИСПДн	АСУ ТП	ЗООКИИ	КТ	иные	
Идентификация								Угрозы УБИ-1
Защита								...
Обнаружение								УБИ-10
Реагирование								
Восстановление								

БДУ ФСТЭК

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

NISTIR 8183 «Cybersecurity Framework Manufacturing Profile»

**Благодарю
за внимание!**

