Защита информационных ресурсов государственных органов и организаций в условий масштабных информационных угроз

Заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Доктрина информационной безопасности Российской Федерации

(утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)

Стратегия национальной безопасности Российской Федерации

(утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400)

повышение защищенности КИИ и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления

развитие отрасли информационных технологий, а также совершенствование деятельности по разработке, производству и эксплуатации средств защиты информации

развитие кадрового потенциала в области обеспечения информационной безопасности

Снижение до минимально возможного уровня утечек информации ограниченного доступа и персональных данных

ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Стратегия национальной безопасности Российской Федерации

(утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400)

Доктрина информационной безопасности Российской Федерации

(утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности КИИ»

Требования к порядку создания, развития и ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС и дальнейшего хранения содержащейся в их базах данных информации

Утверждены постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676

Требования к защите персональных данных при их обработке в информационных системах персональных данных

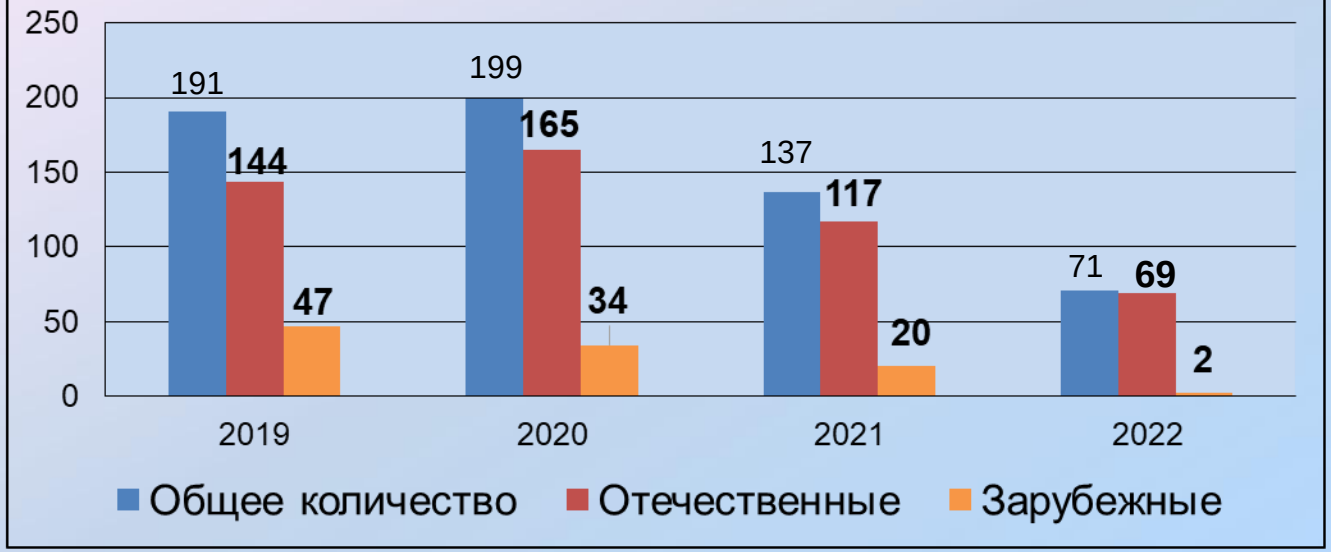
Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119

Нормативные правовые акты и методические документы ФСТЭК России

- Модель иностранных технических разведок на период до 2025 года
- Требования по технической защите информации, содержащей сведения, составляющие государственную тайну
- Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, содержащей сведения, составляющие государственную тайну
- Методика оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах
- Меры защиты информации в государственных информационных системах
- ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»

СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Количество выданных сертификатов соответствия



Количество основных типов производимых СЗИ НСД

- Операционные системы (21 сертификат)
- Системы управления базами данных (9 сертификатов)
- Средства виртуализации (9 сертификатов)
- Средства доверенной загрузки (11 сертификатов)
- Средства контроля и анализа защищенности (12 сертификатов)
- Средства антивирусной защиты (21 сертификат)
- Системы обнаружения вторжений (29 сертификатов)
- Межсетевые экраны (53 сертификата)
- Средства контроля съемных машинных носителей информации (4 сертификата)
- DLP – системы (5 сертификатов)
- Средства защиты от DOS-атак (3 сертификата)
- Системы управления событиями безопасности (13 сертификатов)

Проблемные вопросы:

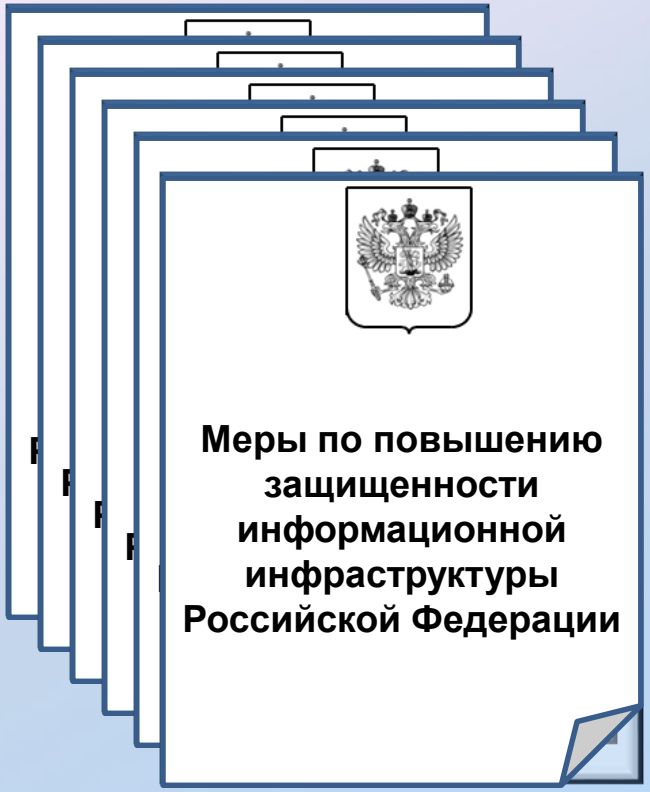
применение в ИС уязвимого свободнораспространяемого ПО;
применение в качестве среды функционирования несертифицированных ОС и СУБД;
использование несертифицированных средств сетевой безопасности;
несвоевременное обновление ПО СЗИ;
несоответствие настроек СЗИ эксплуатационной документации;

Требования по безопасности информации к средствам контейнеризации
утверждены приказом ФСТЭК России от 4 июля 2022 г. № 118

Требования по безопасности информации к средствам виртуализации
Проект

В настоящее время производится более 300 типов сертифицированных СЗИ
из них **99 %** отечественного производства

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ФЕДЕРАЛЬНЫХ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ



В ПЕРИОД С ФЕВРАЛЯ 2022 г. ПОДГОТОВЛЕНО 59 РЕКОМЕНДАЦИЙ

- Меры по повышению защищенности официальных сайтов органов государственной власти и организаций
- Меры по предотвращению несанкционированного распространения уволенными администраторами систем защищаемой информации
- Меры по предотвращению реализации угроз безопасности информации, связанных с утечкой защищаемой информации
- Меры по предотвращению реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков
- Меры по предотвращению реализации угроз безопасности информации, связанных с фишингом
- Меры по предотвращению реализации угроз безопасности информации, направленных на отказ в обслуживании
- Меры по обновлению применяемого в информационных системах иностранного программного обеспечения и средств

ПЕРВООЧЕРЕДНЫЕ РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Рекомендации по повышению защищенности информационной инфраструктуры Российской Федерации, содержащие дополнительные меры по информационной безопасности, направленные на противодействие компьютерным атакам на информационную инфраструктуру Российской Федерации

Исх. № 240/22/953
от 28 февраля 2022 г.

Блокировка доступа пользователей к информационным ресурсам

Провести инвентаризацию служб и веб-сервисов

Отключить неиспользуемые службы и веб-сервисы

Усилить требования к парольной политике администраторов и пользователей сайтов органов государственной власти

Исключить применение на сайтах органов государственной власти сервисов подсчета и сбора данных о посетителях, сервисов предоставления информации о местоположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, Google Analytics, Google Maps, Google Analytics)

Исключить возможность использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы

Блокировать входящий трафик, поступающий с зарубежных IP-адресов и иностранных доменных имен

СТАТИСТИКА ПО КОЛИЧЕСТВУ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ТЕХНИЧСЕКИХ ЗАДАНИЙ НА СОЗДАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к порядку создания, развития и ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС и дальнейшего хранения содержащейся в их базах данных информации

утверждены постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676

В 2022 ГОДУ ФСТЭК РОССИИ РАССМОТРЕНО – 1014

- Оценка негативных последствия проведена без учета специфики функции информационной системы и обрабатываемой в ней информации
- Занижение возможностей (потенциала) нарушителей безопасности информации
- Применение организационных и технических мер защиты при оценке возможностей нарушителей
- Не в полном объеме представлено описание сценариев реализации угроз безопасности информации
- Не проведена оценка угроз безопасности информации, связанных с применением технологий контейнеризации, представленными ФСТЭК России способами
- Отсутствие актуального способа реализации угроз безопасности информации

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к порядку создания, развития и ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС и дальнейшего хранения содержащейся в их базах данных информации

утверждены постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17

Основные замечания по рассмотрению технических заданий

- Занижается класс защищенности информационной системы
- Применяются не сертифицированные операционные системы и системы управления базами данных
- Не определяются требования к квалификации, знаниям и умениям специалистов, эксплуатирующих системы защиты информации
- Не определены требования к мерам и средствам защиты информации, применяемым в информационной системе

В 2022 году рассмотрено 192 технических задания

32 % документов возвращаются на доработку

Операционные системы	**Системы управления базами данных**
Реализация функций безопасности невозможна без применения функций безопасности операционной системы / системы управления базами данных	
Составляют поверхность атаки	

Требования доверия	**Требования к операционным системам**
(приказ ФСТЭК России от 2 июня 2020 г. № 76)	(приказ ФСТЭК России от 19 августа 2016 г. № 119)

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, содержащей сведения, составляющие государственную тайну

Приказ ФСТЭК России
от 28 сентября 2020 г. № 110
(зарегистрирован Минюстом России
10 февраля 2021 г. № 62451)

По состоянию на 3 октября в реестр ФСТЭК России занесены данные по **72363** объектам информатизации

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

Приказ ФСТЭК России
от 29 апреля 2021 г. № 77
(зарегистрирован Минюстом России
10 августа 2021 г. № 64589)

По состоянию на 3 октября в реестр ФСТЭК России занесены данные по **5665 объектам информатизации**:

- ✓ **ГИС - 1554**
- ✓ ИСУП - 235
- ✓ Защищаемые помещения - 580
- ✓ КИИ - 38
- ✓ ИСПДн- 3244
- ✓ АСУ ТП - 14

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

УКАЗ
Президента
Российской Федерации
от 01.05.2022 г. № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

- **Возложить на руководителя органа персональную ответственность за обеспечение ИБ**
- **Возложить на заместителя руководителя органа полномочия по обеспечению ИБ**
- **Создать структурное подразделение по ИБ**
- **Принимать решения о необходимости привлечения организаций, имеющих лицензию на деятельность по ТЗКИ**
- **Обеспечивать незамедлительную организацию мер защиты информации, направляемых в государственные органы ФСБ России и ФСТЭК России**
- **С 1 января 2025 г. запрещается использовать СЗИ, странами происхождения которых являются, недружественные Российской Федерации иностранные государства**

ОСНОВНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

- Создание подразделений (назначение специалистов)
- Приведение в соответствие организационно-распорядительных документов
- Разработка планов по внедрению технических мер ОБ КИИ
- Проведение оценки эффективности системы ОБ КИИ

Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Реализация технических мер обеспечения безопасности

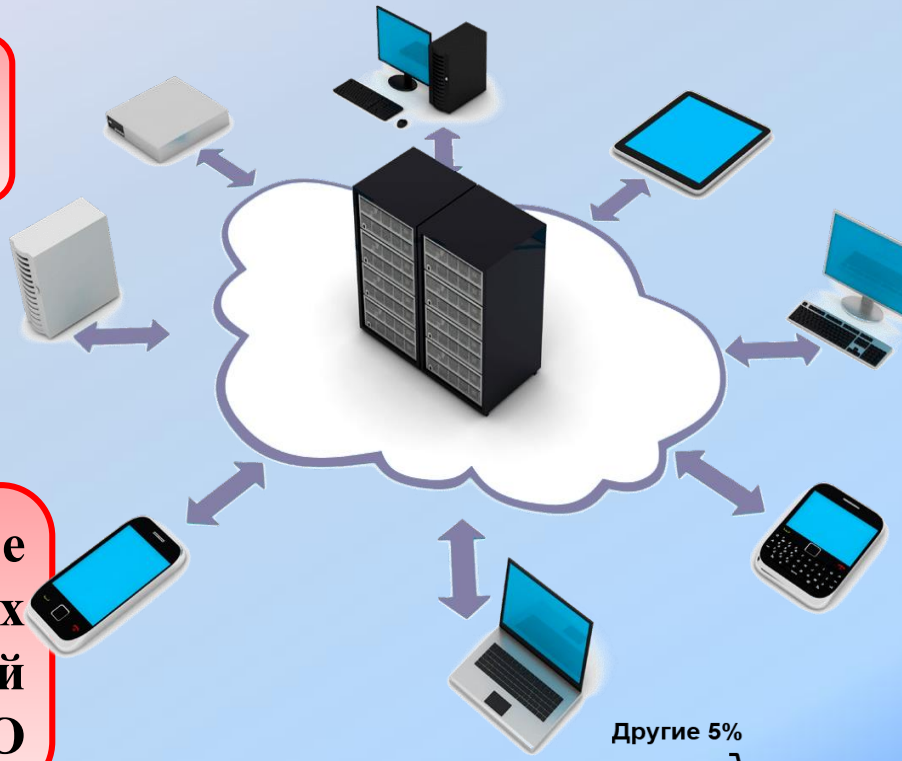
- Идентификация и аутентификация (ИАФ)
- Управление доступом (УПД)
- Аудит безопасности (АУД)
- Предотвращение вторжений (компьютерных атак) (СОВ)
- Антивирусная защита (АВЗ)
- Обеспечение целостности (ОЦЛ)
- Обеспечение доступности (ОДТ)
- Защита технических средств и систем (ЗТС)

УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В ХОДЕ ЭКСПЛУАТАЦИИ

40% — Использование уязвимого ПО

15% — Уязвимость к проведению SQL-инъекций

35% — Отсутствие актуальных обновлений антивирусного ПО



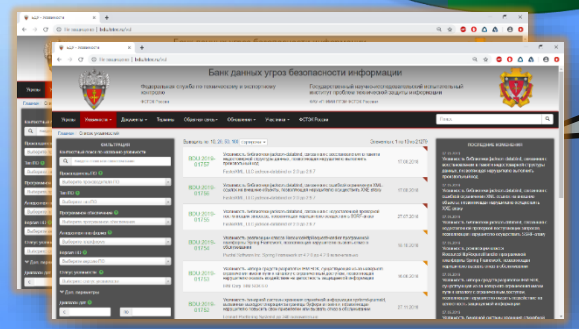
Несоответствие настроек средств защиты информации эксплуатационной документации — 30%

Использование «слабых паролей» — 65%

Использование «паролей по умолчанию» — 38%

80% проверенных информационных систем имеют уязвимости

20% выявляемых уязвимостей имеют высокий и критический уровни опасности



БДУ ФСТЭК России содержит сведения о:
222 угрозах безопасности информации;
более 42 800 уязвимостей ПО

Защита информационных ресурсов государственных органов и организаций в условий масштабных информационных угроз

Заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич