Действующее нормативное регулирование, касающееся разработки безопасного ПО в РФ (относительно направлений регулирования)

КИИ

- **ФЗ № 187-ФЗ**
  - О чем - закон регулирует отношения в области безопасности критической информ.инфраструктуры (КИИ)

    Для кого - субъекты КИИ (здравоохранение, наука, транспорт, связь, энергетика, финансовые организации, ТЭК, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности, регистрация недвижимости) и обеспечивающие их организации
- **Приказ № 31**
  - О чем - приказ устанавливает требования по безопасности АСУ ТП в КИИ

    Для кого - субъекты КИИ (здравоохранение, наука, транспорт, связь, энергетика, финансовые организации, ТЭК, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности, регистрация недвижимости) и обеспечивающие их организации
- **Приказ № 239**
  - О чем - приказ устанавливает требования по безопасности значимых объектов КИИ

    Для кого - субъекты КИИ (здравоохранение, наука, транспорт, связь, энергетика, финансовые организации, ТЭК, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности, регистрация недвижимости) и обеспечивающие их организации

Условные обозначения отраслей

- КИИ
- Финансовая отрасль
- Иное:
  или ГИС
  или общие требования;
  или отраслевые требования
- ПДн

Материал Swordfish Security v9.2025.04

ПДн

- **ФЗ № 152-ФЗ**
  - О чем - закон регулирует отношения, связанные с обработкой персональных данных (ПДн)

    Для кого - все ФЛ (ИП), ЮЛ РФ, обрабатывающие ПДн
- **Приказ № 21**
  - О чем - приказ определяет меры по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах

    Для кого - все ФЛ (ИП), ЮЛ РФ, обрабатывающие ПДн

Иное: или ГИС или общие требования; или отраслевые требования

- **ФЗ № 149-ФЗ**
  - О чем - закон регулирует отношения, возникающие при работе с информацией, использовании ИТ и обеспечении защиты информации

    Для кого - все ФЛ и ЮЛ РФ
- **Приказ № 17**
  - О чем - приказ определяет требования по защите информации в гос.системах

    Для кого - владельцы (операторы) и пользователи гос.систем
- **Приказ № 55**
  - О чем - приказ определяет порядок сертификации средств защиты информации

    Для кого - компании, являющиеся разработчиком средств защиты информации
- **Приказ № 76**
  - О чем - приказ определяет требования по безопасности информации, устанавливающие уровни доверия к средствам защиты информации

    Для кого - компании, являющиеся разработчиком средств защиты информации
- **Приказ № 240**
  - О чем - приказ определяет порядок сертификации процессов разработки ПО, выполняющего функции средства защиты информации

    Для кого - компании, являющиеся разработчиком средств защиты информации
- **Приказ № 1215**
  - О чем - приказ определяет дополнительные требования по безопасности для объектов электроэнергетики при дистанционном управлении их технологическими режимами работы

    Для кого - компании, имеющие значимые объекты критической информационной инфраструктуры в сфере электроэнергетики
- **ГОСТ Р 58412**
  - О чем - ГОСТ устанавливает перечень и описание угроз безопасности информации при разработке ПО

    Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативном документе
- **ГОСТ Р 71207-2024**
  - О чем - ГОСТ устанавливает общие требования к внедрению и выполнению статического анализа ПО

    Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе
- **ГОСТ Р 56939-2024**
  - О чем - новый подход к процессу разработки безопасного ПО, введение новых требований к безопасной разработке (25 новых мер вместо 9 мер действующей версии ГОСТ).

    Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе
- **Методические рекомендации по обеспечению безопасности при разработке программного обеспечения на ЕЦП "ГосТех"**
  - О чем - рекомендации по мерам безопасности при разработкие ПО на платформе ГосТех

    Для кого - владельцы ИС, размещающие ИС на платформе ГосТех
- **Концепция разработки безопасного ПО на платформе ГосТех**
  - О чем - концепция определяет основные подходы и перечень мер по разработке безопасного ПО на платформе ГосТех

    Для кого - компании, размещающие ИС на платформе ГосТех (разработчики ПО, поставщики сервисов платформы ГосТех)

Финансовая отрасль

- **Положение № 716-П**
  - О чем - положение устанавливает требования к системе управления операционным риском в кредитной организации и банковской группе

    Для кого - кредитные организации
- **Положение № 757-П**
  - О чем - положение устанавливает требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций

    Для кого - некредитные финансовые организации
- **Положение № 779-П**
  - О чем - положение устанавливает требования к операционной надежности в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)

    Для кого - некредитные финансовые организации
- **Методический документ Профиль защиты**
  - О чем - устанавливает требования к оценке уязвимостей ПО и к безопасному жизненному циклу ПО

    Для кого - кредитные и некредитные финансовые организации, но только не для объектов КИИ
- **Положение № 802-П**
  - О чем - положение устанавливает требования к защите информации в платежной системе Банка России

    Для кого - кредитные организации
- **Положение № 808-П**
  - О чем - положение устанавливает требования к защите информации бюро кредитных историй и к лицам, оказывающим проф. услуги на фин.рынке

    Для кого - бюро кредитных историй; лица, оказывающие проф.услуги на фин.рынке
- **Положение № 820-П**
  - О чем - положение устанавливает требования к участникам платформы Цифрового рубля (ЦР)

    Для кого - кредитные организации, подключающиеся к платформе ЦР
- **Положение № 821-П**
  - О чем - положение устанавливает требования к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

    Для кого - кредитные организации
- **Положение № 833-П**
  - О чем - положение устанавливает требования к обеспечению защиты информации для участников платформы Цифрового рубля (ЦР)

    Для кого - кредитные организации, подключающиеся к платформе ЦР
- **Методические рекомендации от 30.09.2024 № 16-МР**
  - О чем - установление единых требований и подходов к организации взаимодействия информационных систем финансовых организаций с инфраструктурой Госуслугами

    Для кого - кредитные и некредитные финансовые организации
- **Стандарт Банка России СТО БР ФАПИ.СЕК-1.6-2024**
  - О чем - установление порядка использования модели API со структурированными данными и модели токена для повышения безопасности финансовых технологий

    Для кого - кредитные и некредитные финансовые организации
- **Стандарт Банка России СТО БР ФАПИ.ПАОК-1.0-2024**
  - О чем - установление порядка использования модели API со структурированными данными и модели токена для повышения безопасности финансовых технологий в случае инициирования OpenID Connect клиентом потока аутентификации по отдельному каналу

    Для кого - кредитные и некредитные финансовые организации
- **Методические рекомендации от 22.01.2025 № 2-МР**
  - О чем - установление единые подходы к проведению тестирования на проникновение и анализу уязвимостей информационной безопасности объектов финансового рынка

    Для кого - кредитные и некредитные финансовые организации
- **Положение № 850-П от 13.01.2025 (взамен 787-П)**
  - **О чем** - положение устанавливает требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг.
    Полный пересмотр 787-П, но при этом сохраняются ранее действовавшие требования к практикам безопасной разработки

    Для кого - кредитные финансовые организации
- **Положение № 851-П от 30.01.2025 (взамен 683-П)**
  - О чем - полный пересмотр 683-П, но при этом сохраняются ранее действовавшие требования к практикам безопасной разработки

    Для кого - кредитные финансовые организации

Presented with xmind