Материал
Swordfish Security
v9.2025.04

Условные обозначения
- Иные НПА
- ГОСТ
- ФЗ
- ФСТЭК
- Минцифры РФ
- Банк России

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

Действующее нормативное регулирование, касающееся разработки безопасного ПО в РФ (относительно даты издания)

2006

- ФЗ
  - 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
  - ФЗ № 152-ФЗ — О чем - закон регулирует отношения, связанные с обработкой персональных данных (ПДн). Для кого - все ФЛ (ИП), ЮЛ РФ, обрабатывающие ПДн

2013

- ФСТЭК
  - Приказ № 17 — О чем - приказ определяет требования по защите информации в гос.системах. Для кого - владельцы (операторы) и пользователи гос.систем
  - 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
- ГОСТ
  - ГОСТ Р 15408 - ОУД4 — О чем - ГОСТ устанавливает требования и уровни доверия к объектам оценки. Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативном документе

2014

- ФСТЭК
  - 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 химичечская промышленности, регистрация недвижимости) и обеспечивающие их организации

2017

- ГОСТ
  - ГОСТ Р 57580.1 — О чем - ГОСТ устанавливает требования к созданию безопасного ПО и устранению ошибок и уязвимостей ПО. Для кого - любая *финансовая* организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе
- ФЗ
  - 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 химичечская промышленности, регистрация недвижимости) и обеспечивающие их организации
- ФСТЭК
  - 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 химичечская промышленности, регистрация недвижимости) и обеспечивающие их организации

2018

- ФСТЭК
  - Приказ № 55 — О чем - приказ определяет порядок сертификации средств защиты информации. Для кого - компании, являющиеся разработчиком средств защиты информации

2019

- ГОСТ
  - 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

2020

- ФСТЭК
  - 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
- Банк России
  - Положение № 716-П — О чем - положение устанавливает требования к системе управления операционным риском в кредитной организации и банковской группе. Для кого - кредитные организации

2021

- Банк России
  - 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

2022

- Минцифры РФ
  - Методические рекомендации по обеспечению безопасности при разработке программного обеспечения на ЕЦП "ГосТех" — О чем - рекомендации по мерам безопасности при разработке ПО на платформе ГосТех. Для кого - владельцы ИС, размещающие ИС на платформе ГосТех
- Банк России
  - Положение № 787-П — О чем - положение устанавливает требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг. Для кого - кредитные организации
  - 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

2023

- Банк России
  - 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
- ФСТЭК
  - Приказ № 240 — О чем - приказ определяет порядок сертификации процессов разработки ПО, выполняющего функции средства защиты информации. Для кого - компании, являющиеся разработчиком средств защиты информации
- Минэнерго РФ
  - 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
- Минцифры РФ
  - 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)

2024

- ГОСТ
  - 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
- Банк России
  - 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

2025

- Банк России
  - 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 - положение устанавливает требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента. Полный пересмотр 683-П, но при этом сохраняются ранее действовавшие требования к практикам безопасной разработки. Для кого - кредитные финансовые организации
  - Актуализация Положения № 757-П — Какие изменения - в части разработки безопасного ПО вводится возможности верификации процесса разработки вместо сертификации ПО
  - Актуализация Положения № 821-П — Какие изменения - в части разработки безопасного ПО вводится возможности верификации процесса разработки вместо сертификации ПО
- ФСТЭК
  - Обновление Приказа № 17 — **Какие изменения -** полный пересмотр мер защиты информации, обрабатываемых в ГИС. Дополнительно проект приказа содержит отдельный набор мер по разработке безопасного ПО (утвержден во ФСТЭК от 11 апреля 2025 г. № 117 (находится на регистрации в Минюсте России))
- ГОСТ
  - Разработка ГОСТ - Композиционный анализ ПО — О чем - ГОСТ устанавливает требования к порядку и процессам композиционного анализа ПО. Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе. ГОСТ на данный момент не утвержден
  - Разработка ГОСТ - Secure-by-Design — О чем - ГОСТ устанавливает требования к мерам безопасности программного обеспечения с начала его разработки. Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе. ГОСТ на данный момент не утвержден
  - Разработка ГОСТ - Доверенная среда исполнения — О чем - ГОСТ устанавливает требования к мерам безопасности среды исполнения ПО с целью уменьшения поверхности атаки. Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе. ГОСТ на данный момент не утвержден
  - Разработка ГОСТ - Динамический анализ ПО — О чем - ГОСТ устанавливает требования к мерам безопасности программного обеспечения с начала его разработки. Для кого - любая организация на добровольной основе или в обязательном порядке, если ГОСТ упоминается в нормативной документе. ГОСТ на данный момент не утвержден
  - Разработка ГОСТ - Методики оценки реализации процессов разработки безопасного ПО — О чем - методика определяет порядок оценки реализации ГОСТ Р 56939. Для кого - любые организации, выполняющие ГОСТ Р 56939
  - Разработка ГОСТ - Руководство по внедрению процессов разработки безопасного ПО — О чем - руководство определяет порядок внедрения требований ГОСТ Р 56939. Для кого - любым организациям, выполняющие ГОСТ Р 56939

Presented with xmind