SWORDFISH
SECURITY

Разработка безопасного ПО для КИИ,

ИЛИ

что есть в регуляторике на эту тему

Альбина Аскерова

Руководитель направления
по взаимодействию с регуляторами

SWORDFISH SECURITY

- Родоначальники индустрии DevSecOps в России
- Высокий уровень навыков выстраивания процессов защищенного ПО
- Опыт адаптации процессов в компаниях от 100 разработчиков до 15 000+ разработчиков
- Высокий уровень навыков адаптации процессов безопасной разработки к требованиям внешних и внутренних регуляторов
- Экспертиза, компетенция и индустриальный вклад подтверждаются наличием собственной линейкой востребованных и коммерчески успешных продуктов международного уровня

Опыт внедрения процессов РБПО

Разработчики ПО: более 5 проектов

Промышленность: более 5 проектов

Телеком: более 5 проектов

Финансовая сфера: более 15 проектов

Всего – более 70 проектов

Вклад в индустрию

1. **Постоянный член ТК 362**
2. **Участники консорциума исследований безопасности технологий ИИ**
3. **Ассоциированный член Ассоциации ФинТех**
4. **Лидеры FinDevSecOps-сообщества**

SWORDFISH SECURITY

- Что такое разработка безопасного ПО?
- Кто регулирует?
- Кого регулирует?
- Как регулирует?
- Требования к КИИ (в промышленности)?
- Какая ответственность?
- Какие тренды в изменении регуляторики?
- Внедрение разработки безопасного ПО

Частые предпосылки для РБПО

SWORDFISH SECURITY

Бизнес

- Требования регуляторов выполняются частично / с нарушениями / несистемно
- Данные для принятия решений собираются и обрабатываются вручную
- Данные являются неактуальными на момент обработки

- Compliance формален
- Негативное влияние на скорость релизов
- Отчёты «ручные»

Безопасность

- Разработка не принимает во внимание вопросы безопасности
- Тесты безопасности проводятся в ручном режиме или не проводятся вообще

- Разработка игнорирует
- Безопасность «лоскутная»

Разработка

- Безопасность «тормозит» разработку
- Проблемы безопасности возвращаются после теста множественными табличными документами без учета ранее выставленных, принятых и/или отвергнутых комментариев и поправок

- ИБ «мешает»
- В отчёте — «уязвимости»
- «Костыльное» исправление уязвимостей, приводящее к деградации качества ПО

Разработка безопасного ПО

SWORDFISH SECURITY

OSA

Анализ библиотек с открытым исходным кодом

Open-Source Analysis

DAST

Динамический анализ

Dynamic Application Security Testing

SAST

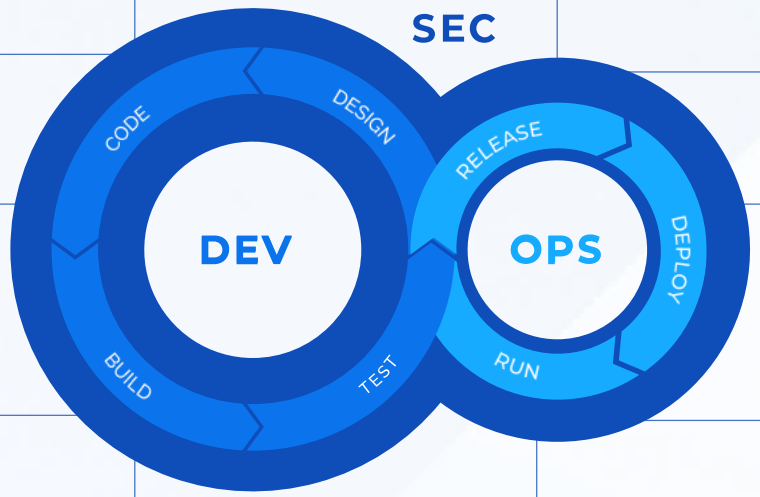
Статический анализ кода

Static Application Security Testing

MAST

Анализ защищенности мобильных приложений

Mobile Application Security Testing



SCM

Контроль исходного кода

Source Code Management

SBOM

Управление перечнем программных компонентов

Software Bill of Materials Management

SCA

Компонентный анализ ПО

Software Composition Analysis

CS

Анализ защищенности контейнеров

Container Security

API ST

Анализ программных интерфейсов

API Security Testing

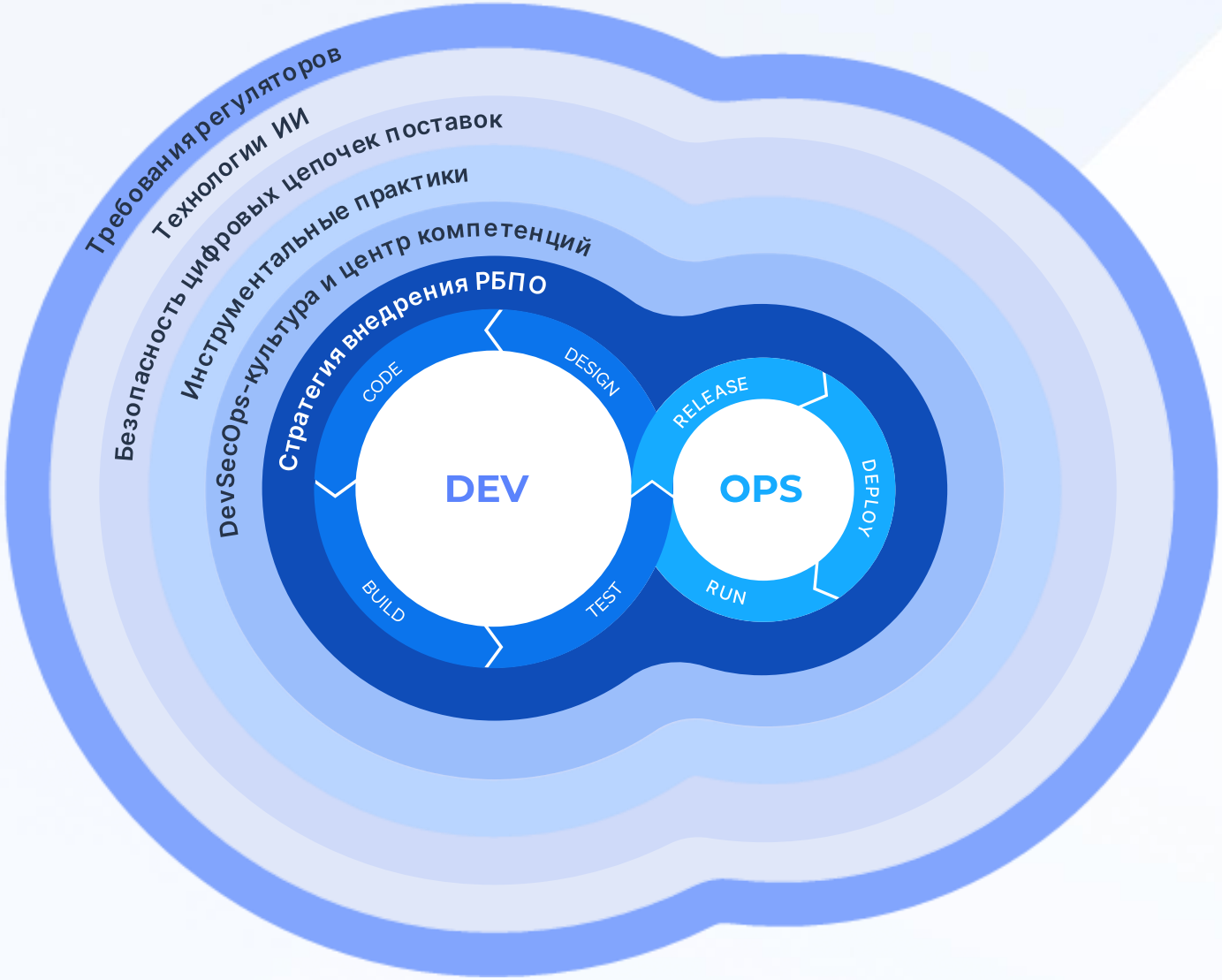
ASPM

Управление практиками анализа защищенного ПО

Application Security Posture Management

Разработка безопасного ПО

SWORDFISH SECURITY



Кто регулирует?

SWORDFISH SECURITY

Президент

Обязательное к исполнению |
Федеральные законы; Указы

Правительство РФ

Обязательное к исполнению |
постановления Правительства

Регуляторы (общие и отраслевые)

Общие — ФСТЭК России, ФСБ России
Отраслевые — Банк России, Минэнерго России

Обязательное к исполнению |
приказы, распоряжения, положения

Опциональное исполнение |
методические документы

Росстандарт

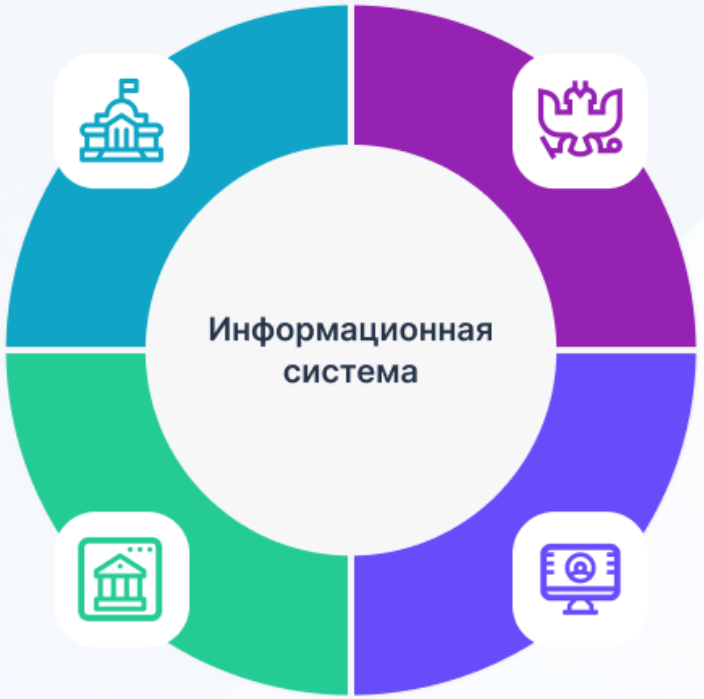
Применение на добровольной основе или обязательно, если упоминается в нормативном документе |
ГОСТ

Кого регулирует?

SWORDFISH SECURITY

КИИ
Объекты критической информационной инфраструктуры

Финтех
Финансовые кредитные и некредитные организации



ГИС
Государственные информационные системы

ИСПДн
Информационные системы персональных данных

Кого регулирует?

SWORDFISH SECURITY

По отрасли

Финансовая отрасль
(№ 86–ФЗ; № 395-1)

Кредитные организации
(если организация осуществляет банковские операции – банки)

Некредитные организации
1) профессиональные участники рынка ценных бумаг;
2) управляющие компании инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда;
3) специализированные депозитарии инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда;
4) акционерные инвестиционные фонды;
5) клиринговая деятельность;
6) деятельность по осуществлению функций центрального контрагента;
7) деятельность организатора торговли;
8) деятельность центрального депозитария;
9) репозитарная деятельность;
10) деятельность субъектов страхового дела;
11) негосударственные пенсионные фонды;
12) микрофинансовые организации;
13) кредитные потребительские кооперативы;
14) жилищные накопительные кооперативы;
15) сельскохозяйственные кредитные потребительские кооперативы;
16) деятельность оператора инвестиционной платформы;
17) ломбарды;
18) оператор финансовой платформы;
19) оператор информационных систем, в которых осуществляется выпуск цифровых финансовых активов;
20) операторов обмена цифровых финансовых активов

Критическая информационная инфраструктура
(№ 187–ФЗ)

здравоохранение,
наука,
транспорт,
связь,
энергетика,
государственная регистрация прав на недвижимое имущество и сделок с ним,
банковская сфера и иные сферы финансового рынка,
ТЭК
атомная энергия,
оборонная,
ракетно-космическая,
горнодобывающая,
металлургическая
и химическая промышленности

По целевому назначению системы

Государственная информационная система
(№ 149-ФЗ)

системы, которые создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях

Информационная система персональных данных
(№ 152–ФЗ)

совокупность содержащихся в базах данных персональных данных
и обеспечивающих их обработку информационных технологий
и технических средств.

АСУ ТП
(Приказ ФСТЭК России № 31)

автоматизированные системы управления производственными и технологическими процессами на критически важных объектах

Как регулирует?

КИИ по отрасли

• **Общее для КИИ**

Приказ ФСТЭК России от 14.03.2014 № 31

Федеральный закон от 26.07.2017 № 187-ФЗ

Приказ ФСТЭК России от 21.12.2017 № 235

Приказ ФСТЭК России от 25.12.2017 № 239

• **Кредитные финансовые организации:**

Положение Банка России от 17.04.2019 № 683-П

Положение Банка России от 08.04.2020 N 716-П

Положение Банка России от 12.01.2022 N 787-П

Положение Банка России от 25.07.2022 N 802-П

Положение Банка России от 03.08.2023 № 820-П (Цифровой рубль)

Положение Банка России от 17.08.2023 № 821-П

Положение Банка России от 07.12.2023 № 833-П (Цифровой рубль)

Положение Банка России от 17.10.2022 N 808-П

Методические рекомендации Банка России от 30.09.2024 № 16-МР

• **Некредитные финансовые организации:**

Положение Банка России от 20.04.2021 № 757-П

Положение Банка России от 15.11.2021 N 779-П

Положение Банка России от 17.10.2022 N 808-П

Методические рекомендации Банка России от 30.09.2024 № 16-МР

• **Энергетика:**

Приказ Минэнерго России от 26.12.2023 № 1215

Не КИИ, но

• Приказ ФСТЭК России от 11.02.2013 № 17 (ГИС)

• Приказ ФСТЭК России от 03.04.2018 № 55 (Производители СрЗИ)

• Положение Банка России от 17.10.2022 № 808-П (Бюро кредитных историй и другие организации в сфере фин.услуг)

• Методический документ Банка России от 2021 года Профиль защиты (Общий документ для кредитных и не кредитных организаций, но только для ПО, не являющегося объектом КИИ)

Общее

• Указ от 01.05.2022 № 250 (госкомпании, КИИ, стратегические и системообразующие компании)

• Федеральный закон от 27.07.2006 № 152-ФЗ (операторы ПДн)

• Приказ ФСТЭК России от 18.02.2013 № 21 (операторы ПДн)

• Приказ ФСТЭК России от 02.06.2020 № 76 (требования к уровням доверия)

• Приказ ФСТЭК России от 01.12.2023 № 240 (Сертификация процессов безопасной разработки)

• Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы «ГосТех» (ИС, размещаемые на ГосТех)

• Концепция разработки безопасного ПО на платформе ГосТех (ИС, размещаемые на ГосТех)

Требования к КИИ (в промышленности)

SWORDFISH SECURITY

Приказ ФСТЭК № 31

- Выявление источников угроз
- Анализ возможных уязвимостей
- Периодический анализ уязвимостей
- Обеспечение целостности

ФЗ № 187-ФЗ

- Принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры

Приказ ФСТЭК № 235

- Анализ угроз безопасности информации

Приказ ФСТЭК № 239

- Управление обновлениями
- Наличие руководства по безопасной разработке
- Проведение статического анализа
- Проведение фаззинг-тестирования
- Проведение динамического анализа

Приказ Минэнерго № 1215

- Наличие процедур отслеживания, исправления обнаруженных ошибок и уязвимостей программного обеспечения

Какая ответственность?

SWORDFISH SECURITY

Административная

Критическая информационная инфраструктура

ст. 13.12.1 (ч.1) КоАП РФ (выдержка):

Нарушение требований к созданию систем безопасности значимых объектов КИИ значимых объектов КИИ … влечет наложение административного штрафа на … юридических лиц – от 50 000 до 100 000 рублей

Общая ответственность

ст. 13.12 (ч.6) КоАП РФ (выдержка):

Нарушение требований о защите информации … влечет наложение административного штрафа на юридических лиц — от 10 000 до 15 000 рублей
(планируется изменение «от 50 000 до 100 000 рублей)

Уголовная

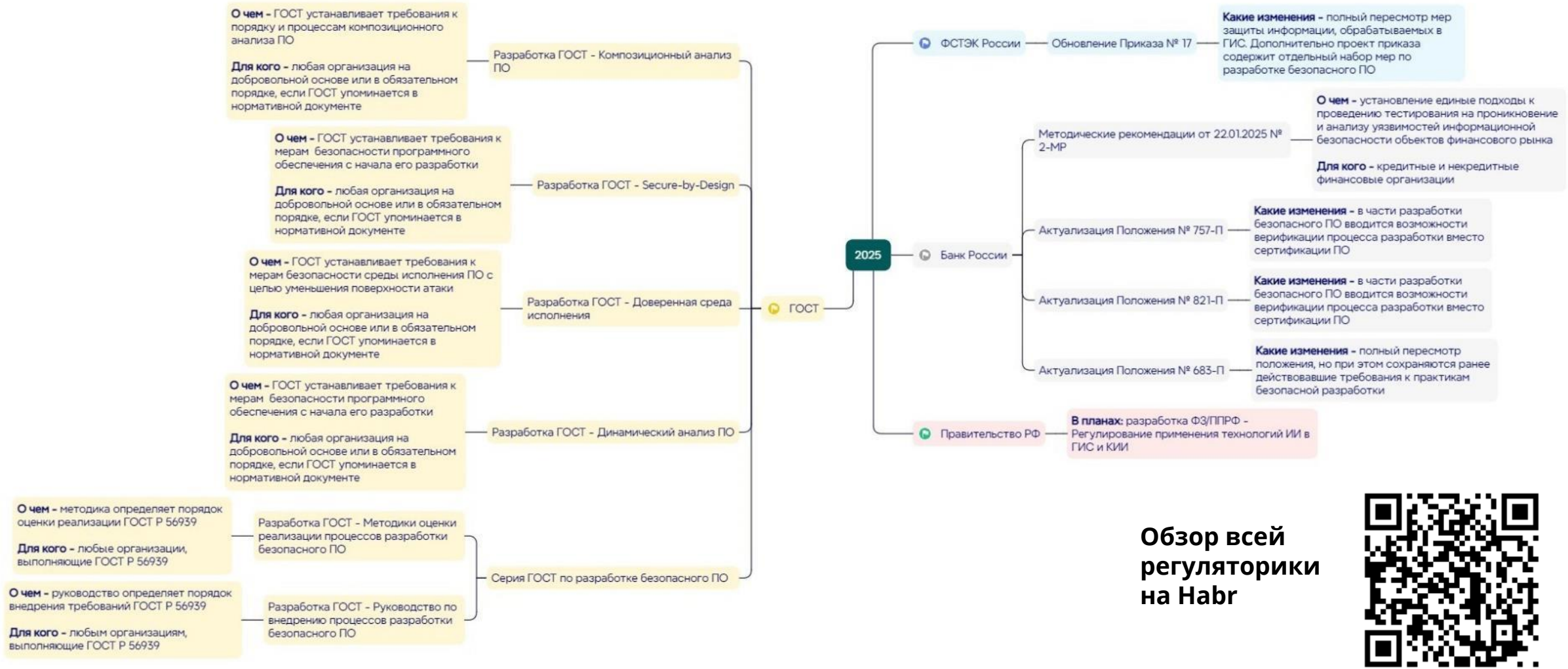
Критическая информационная инфраструктура

ст. 274.1 УК РФ (ч.3) (выдержка):

Нарушение правил эксплуатации … либо правил доступа, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации наказывается принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового

Какие тренды в изменении регуляторики?

SWORDFISH SECURITY



Обзор всей регуляторики на Habr

Внедрение разработки безопасного ПО

SWORDFISH SECURITY

Обследование и анализ текущего состояния процессов разработки безопасного ПО

Проведение обследования и анализа используемого технологического стека

Разработка документов: регламентов, политик, инструкций по итогам обследования

Проведение пилотных испытаний платформы ИБ и инструментальный анализ выбранной системы

Формирование стратегии внедрения практик разработки защищенного ПО

Проведение обучения специалистов ИБ

(Секьюрити Чемпионов?)

SWORDFISH SECURITY

Выстраивание процессов разработки ПО в соответствии с ГОСТ Р 56939-2024 подойдет, если:

1. Идет разработка средств защиты (или ПО, в котором реализуются функции безопасности) и есть желание/необходимость сертифицировать процесс разработки вместо сертификации каждой версии ПО
2. Ориентация на отечественное законодательство в разработке безопасного ПО
3. Продукт – объект КИИ (или разработан для субъектов КИИ)
4. Продукт – государственная система (ГИС) и/или система, в которой обрабатываются ПДн (ИСПДн)
5. Есть желание/необходимость повысить зрелость процессов разработки ПО
6. Есть желание/необходимость стандартизировать процессы разработки внутри компании

Задавайте вопросы ☺

SWORDFISH SECURITY

aaskerova@swordfishsecurity.ru

swordfish-security.ru

Наш telegram-канал

Обзор регуляторики на Habr