Межфакультетский учебный курс:
«Государственные технологии и искусственный интеллект»

Тема 6.

Комплексная система защиты информации Единой цифровой платформы «ГосТех»

Лектор:
Мускатиньев Андрей Юрьевич
Начальник управления информационной безопасности ЕЦП ГосТех
Федерального казенного учреждения (ФКУ)
«Государственные технологии» («ГосТех»)

Лектор:
Назаренко Сергей Владимирович
кандидат социологических наук, доцент,
доцент Высшей школы государственного администрирования
МГУ имени М.В.Ломоносова

Высшая Школа Государственного Администрирования
МГУ имени М.В. Ломоносова

Модели представления облачных вычислений

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

Цели и задачи:

Факторы влияния:

- Сокращение времени на выпуск новых приложений
- Усложнение логики и архитектуры приложений
- Массовое переиспользование кода
- Активное использование заимствованных компонентов
- Активный цикл обновления версий
- Атаки на цепочки поставок

Цель: повышение общего уровня безопасности ПО в составе ГИС, создаваемых на Платформе «ГосТех»

Критерий: Систематическое снижение количества уязвимостей ПО

ГОСТЕХ

Постановление Правительства РФ от 06.07.2015 N 676

Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

Базовые принципы обеспечения ИБ в «ГосТех»

Комплексная система защиты информации

- Обеспечение взаимной совместимости СЗИ
- Интеграция и управление СЗИ в рамках мультитенантной архитектуры
- Соответствие требованиям регуляторов, применение «best practice» и т.д.

Технологическая независимость

- применяемые СЗИ, ПАК, серверные решения и т.д. должны соответствовать требованиям законодательства Российской Федерации в области импортозамещения

Разработка безопасного ПО на платформе «ГосТех» (DevSecOps)

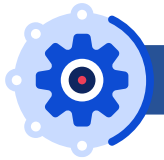
- обеспечение требуемого уровня доверия к прикладному ПО в составе ГИС
- обеспечение доверия при использовании Open Source библиотек
- Оперативное устранение уязвимостей в ППО

Обеспечение мероприятий по обнаружению компьютерных атак и реагированию на компьютерные инциденты

- создание и внедрение на различных технологических уровнях SOC
- Координация деятельности по реагированию на инциденты компьютерной безопасности

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

Обеспечение безопасности приложений на платформе «ГосТех»



Этап разработки

1. Защищенная архитектура
2 Статический анализ
3 Анализ open source компонентов
4 Динамический анализ
5 Безопасность публикации приложений
6 Ручной анализ защищенности (лучше на этом этапе)
7 Фаззинг-тестирование

Этап публикации

8 Анализ open source компонентов (Обратите внимание!)
9. Контроль целостности
10. Анализ конфигураций
11. Безопасность данных (Обезличивание и т.п.)
12. Ручной внешний анализ защищенности (лучше на этом этапе)

Этап эксплуатации

13. Межсетевой экран уровня приложений и защита от атак в обслуживании
14. Мониторинг и реагирование на инциденты
15.Тестирование на проникновение
16. Анализ уязвимостей заимствованных компонент

Ключевые вопросы

- Формирование требований ИБ
- Проектирование защищенной архитектуры
- Анализ рисков и принятие решений по выявленным недостаткам
- Обучение и вовлечение участников в процесс
- Управление процессом (Документация, Показатели эффективности)

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

Нормативно-правовые акты по ИБ в «ГосТех»

- [x] **Единая концепция обнаружения, предупреждения, ликвидации последствий компьютерных атак**, а также реагирования на компьютерные инциденты, связанные с информационными ресурсами платформы «ГосТех»
  Утверждена протоколом Президиума Правкомиссии от 07.07.2022 №25
- [x] **Концепция обеспечения информационной безопасности ЕЦП «ГосТех»**
  Утверждена приказом Минцифры России от 12.01.2023 № 7
- [x] **Политика информационной безопасности платформы «ГосТех»**
  Утверждена протоколом Президиума Правкомиссии от 07.07.2022 №25
- [x] **Методические рекомендации по обеспечению безопасности при разработке программного обеспечения** с использованием компонентов единой цифровой платформы Российской Федерации «ГосТех»
  Утверждена протоколом Президиума Правкомиссии от 08.12.2022 №54
- [x] **Методические рекомендации по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ**
  Утверждена протоколом Президиума Правкомиссии от 27.12.2022 №59
- [x] **Типовая модель угроз и нарушителя безопасности информации для ГИС при развертывании на ЕЦП «ГосТех»**
  Утверждена протоколом Президиума Правкомиссии от 27.12.2022 №59

- [ ] **Концепция разработки безопасного программного обеспечения на ЕЦП «ГосТех»**
- [ ] **Актуализация политики информационной безопасности ЕЦП «ГосТех»**
- [ ] **Актуализация единой концепции обнаружения, предупреждения, ликвидации последствий компьютерных атак,** а также реагирования на компьютерные инциденты, связанные с информационными ресурсами платформы «ГосТех»
- [ ] **Методические рекомендации по разграничению зон ответственности между участниками отношений,** возникающих в связи с созданием и функционированием платформы «ГосТех» в части информационной безопасности

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ МГУ имени М.В.Ломоносова

Общая архитектура платформы ГосТех

1 **Каналы** — Каналы, обеспечивающие взаимодействие с клиентами (ЕПГУ, МФЦ, инфраструктура банков и других организаций)

2 **Государственные сервисы** — Приложения, реализующие продукты и услуги для потребителей, ГИС

3 **Типовые решения** — Типовые облачные решения (ПГС, витрины данных НСУД, платежный шлюз)

4 **Базовые сервисы платформы** — Технологические сервисы платформы

5 **Фабрика данных** — Хранение и аналитика данных

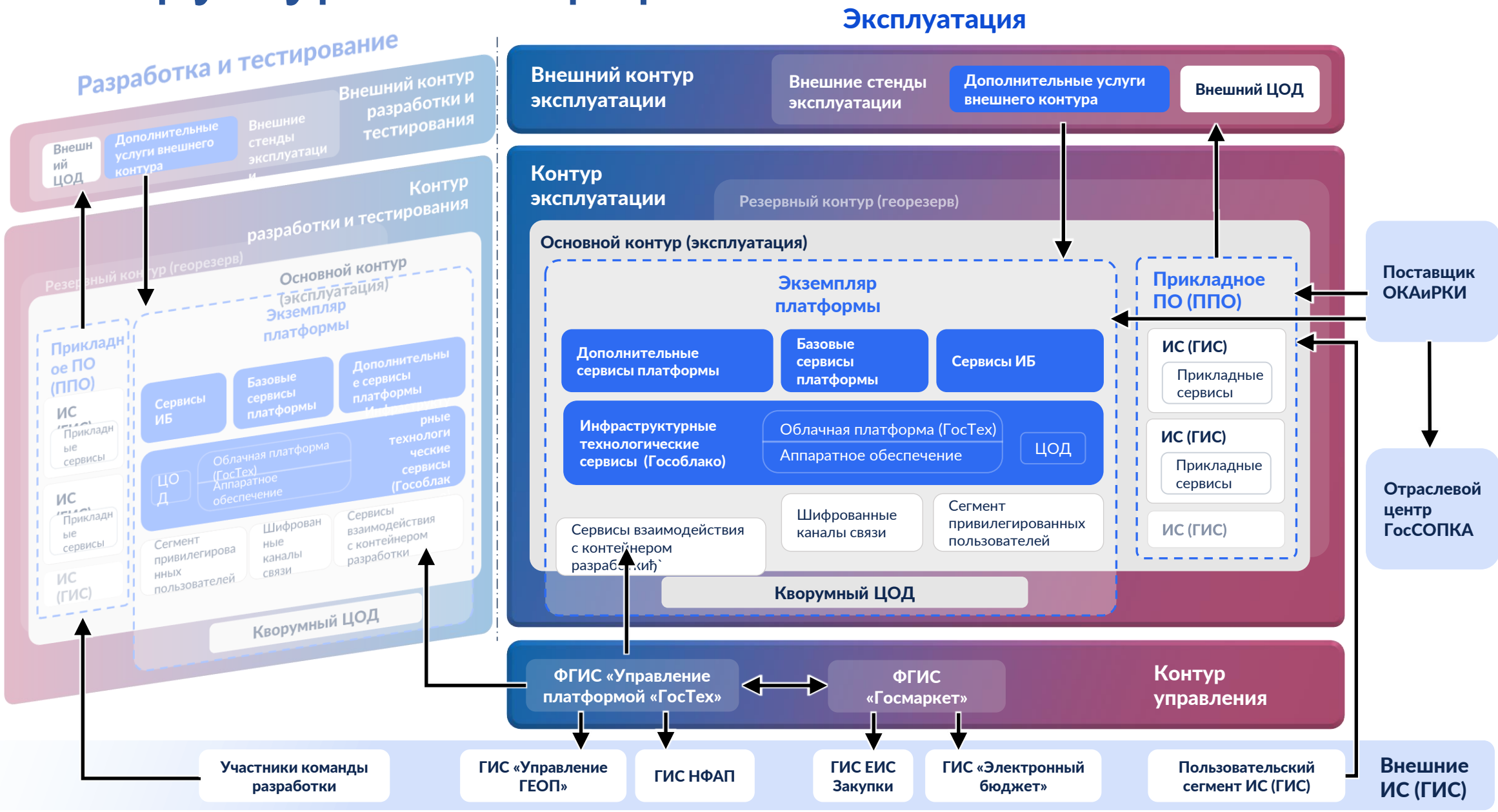
6 **Гособлако** — Управление вычислительной инфраструктурой в облаке

7 **Информационная безопасность**

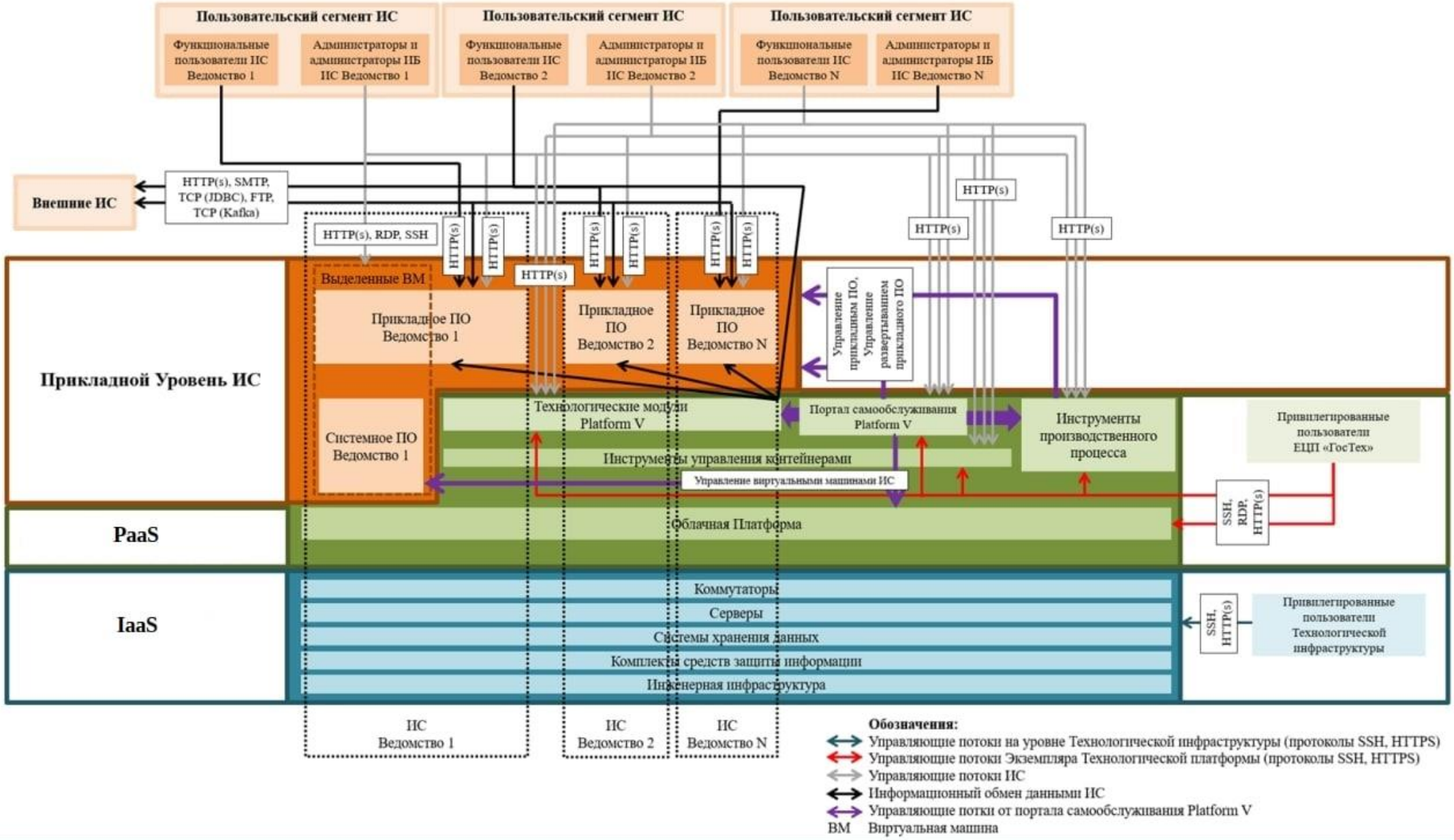
8 **Производственный процесс**

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ МГУ имени М.В.Ломоносова

Структура платформы «ГосТех»



Обобщенная схема экземпляра



Сертификация по требованиям безопасности

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4464

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
1 ноября 2021 г.

Выдан: 1 ноября 2021 г. Переоформлен: 5 декабря 2022 г.
Действителен до: 1 ноября 2026 г.

Настоящий сертификат удостоверяет, что **прикладное программное обеспечение «Облачная платформа Сбербанка»**, разработанное ПАО «Сбербанк России» и производимое АО «СБЕРБАНК-ТЕХНОЛОГИИ», является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции управления доступом, регистрации событий безопасности и обеспечения целостности, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и технических условиях RU.92573301.10004-01 ТУ 01 при выполнении указаний по эксплуатации, приведенных в формуляре RU.92573301.10004-01 30 01.

Сертификат выдан на основании технического заключения от 12.07.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ RU.0001.01БИ00.Б010), экспертного заключения от 16.09.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технического заключения от 20.04.2022, оформленного испытательной лабораторией ООО «КБ-Лаб», и технического заключения от 21.11.2022, оформленного испытательной лабораторией АО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

Заявитель: АО «СБЕРБАНК-ТЕХНОЛОГИИ»
Адрес: 117105, г. Москва, Новоданиловская набережная, д. 10
Телефон: (495) 669-0808

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

ВЫСШАЯ ШКОЛА
ГОСУДАРСТВЕННОГО
АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

Особый порядок аттестации ГИС на ЕЦП «ГосТех»

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ МГУ имени М.В.Ломоносова

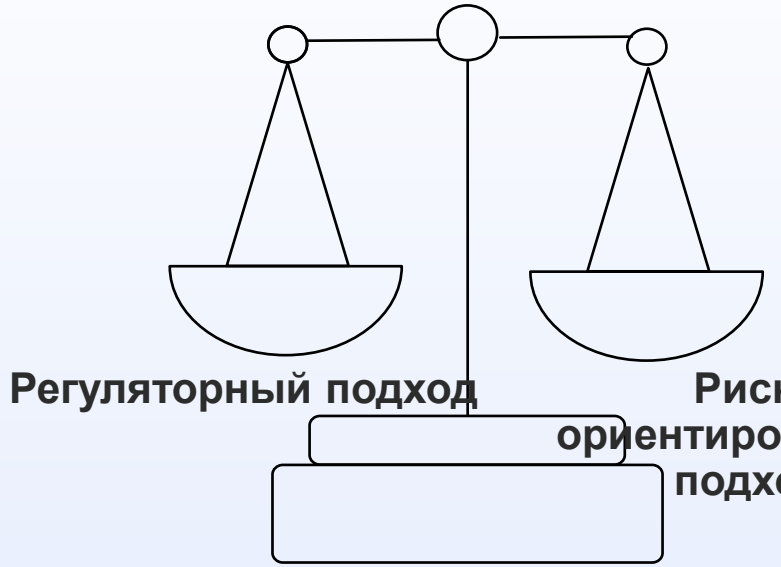
Комплексная система защиты информации

- A **Мониторинг и реагирование на инциденты ИБ**
- B **Защита от атак на веб-приложение**
- C **Защита от DDoS-атак**
- D **Защита DNS трафика**
- E **Межсетевое экранирование и обнаружение вторжений**
- F **Защищенный канал связи**
- G **Антивирусная защита**
- H **Защита от несанкционированного доступа**
- I **Анализ защищенности**
- J **Контроль действий привилегированных пользователей**

J Средство ЗИ J Услуга ИБ J Обязательная мера

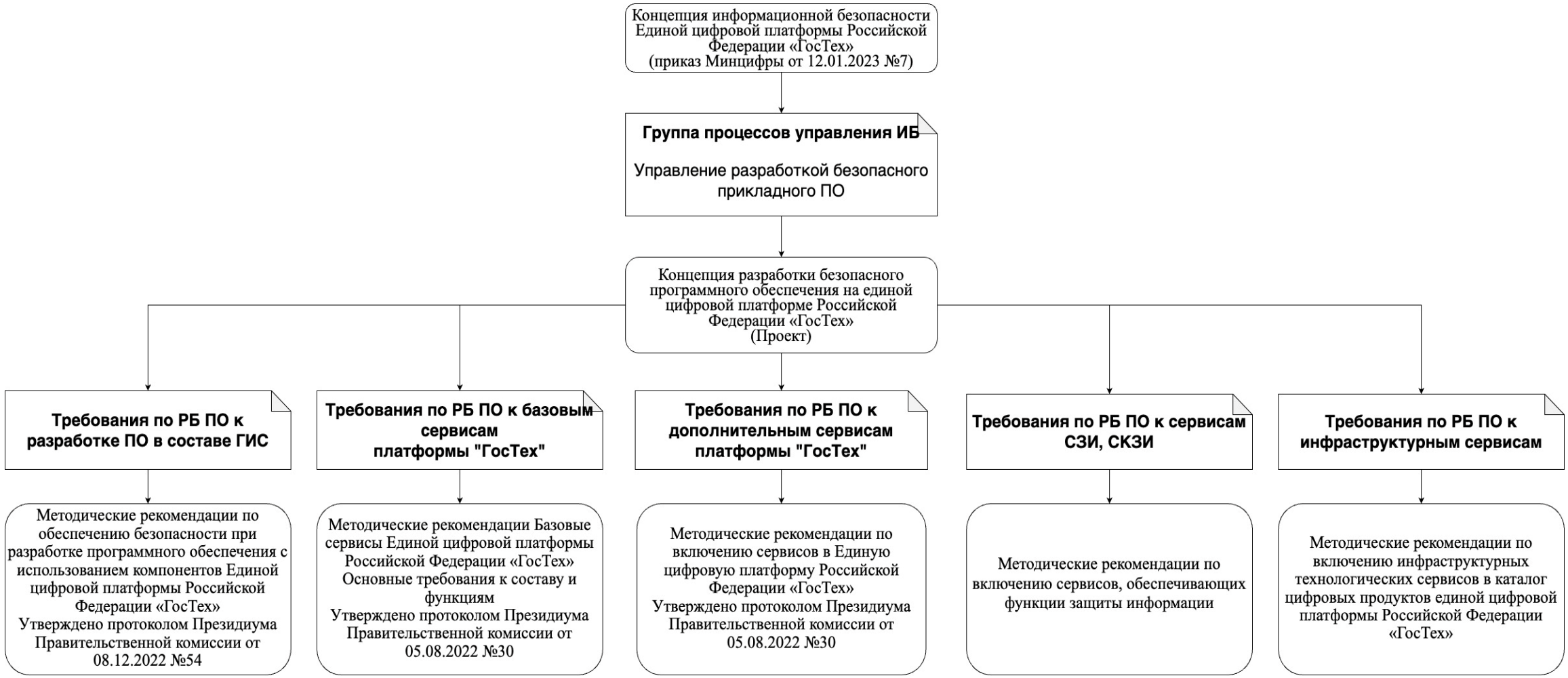
ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ МГУ имени М.В.Ломоносова

Система управления в ИБ



Модель мониторинга

Структура методических документов по РБПО



Процесс разработки безопасного ПО на «ГосТех»

в соответствии с рекомендациями ГОСТ 56939-2016

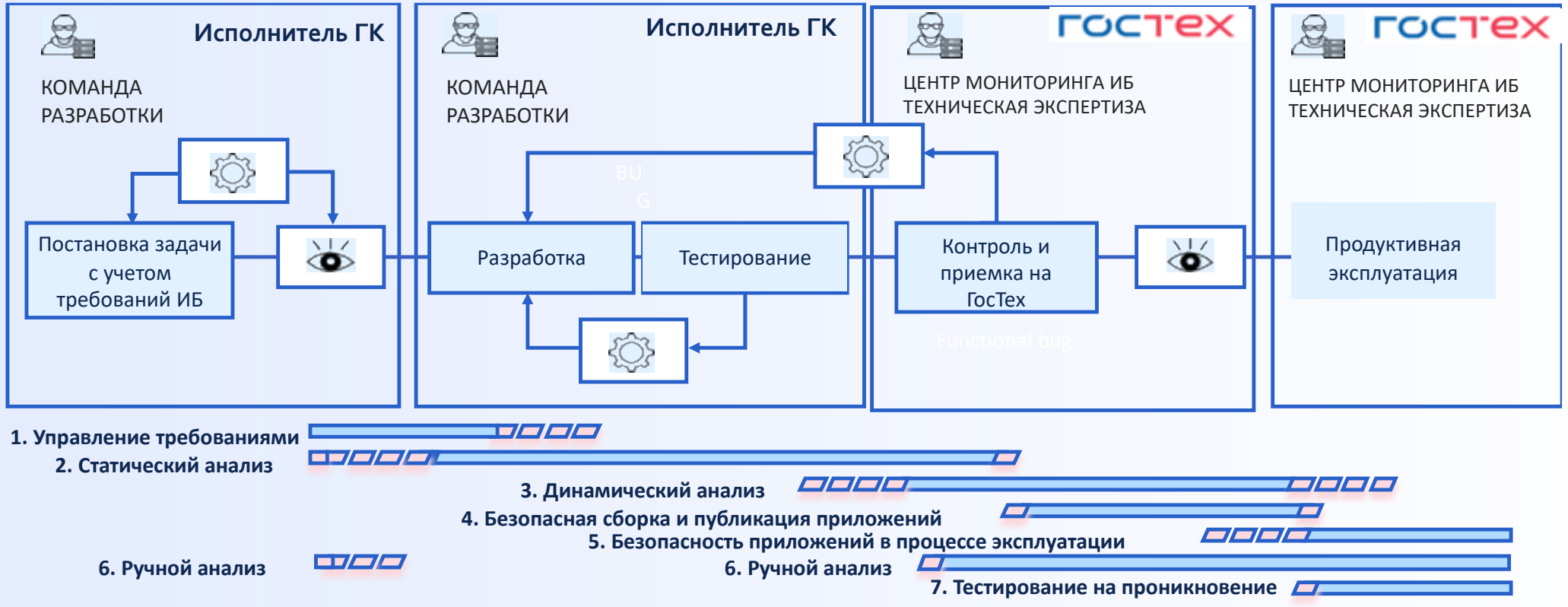


СХЕМА РАБОТАЕТ:

- ЕСЛИ РАЗРАБОТЧИКИ ВОВЛЕЧЕНЫ В ПРОЦЕСС
- ПРИ НАЛИЧИИ У РАЗРАБОТЧИКОВ СООТВЕТСТВУЮЩИХ ЗНАНИЙ
- ПРИ МИНИМАЛЬНОМ ВЛИЯНИИ НА ПРИВЫЧНЫЙ ПРОЦЕСС НЕПРЕРЫВНОЙ РАЗРАБОТКИ
- РУЧНОЙ АНАЛИЗ

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

Конвейер безопасной разработки

ВЫСШАЯ ШКОЛА
ГОСУДАРСТВЕННОГО
АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

Участники безопасной разработки

ГосТех — центр контроля ГИС

Аудит безопасности разрабатываемого на ЕЦП ГосТех ПО для всех типов ГИС (веб-сервисы, ИС, мобильное ПО)

ГосТех

а

Унифицированная среда разработки безопасного отечественного ПО

ФСТЭК России

Контроль безопасности ПО для всех организаций, представленных в системе сертификации ФСТЭК

б

Государственный центр проверки мобильных и веб-приложений

НИИ ВОСХОД системные инновации ФГАУ НИИ ВОСХОД

Анализ уязвимостей ПО, мобильных и веб-приложений, в т.ч. для всех типов ГИС

в

Единый репозиторий компонентов ПО

минцифры_

Единый репозиторий компонентов ПО

На сегодня все!

Вопросы?

ВЫСШАЯ ШКОЛА
ГОСУДАРСТВЕННОГО
АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова

ГОСТЕХ

Межфакультетский учебный курс:
«Государственные технологии и искусственный интеллект»

Тема 6.

Комплексная система защиты информации Единой цифровой платформы «ГосТех»

Лектор:
Мускатиньев Андрей Юрьевич
Начальник управления информационной безопасности ЕЦП ГосТех
Федерального казенного учреждения (ФКУ)
«Государственные технологии» («ГосТех»)

Лектор:
Назаренко Сергей Владимирович
кандидат социологических наук, доцент,
доцент Высшей школы государственного администрирования
МГУ имени М.В.Ломоносова

ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АДМИНИСТРИРОВАНИЯ
МГУ имени М.В.Ломоносова