КОНЦЕПЦИЯ

разработки безопасного программного обеспечения

на единой цифровой платформе Российской Федерации «ГосТех»

Москва
2023

Содержание

1. Перечень терминов, сокращений и обозначений

В Концепции разработки безопасного программного обеспечения на единой цифровой платформе Российской Федерации «ГосТех» (далее – Концепция) используются следующие сокращения, термины и определения:

1.1 Сокращения

Сокращение	Определение
ГИС	Государственная информационная система
ГОСТ	Государственный стандарт
ИС	Информационная система
ПО	Программное обеспечение
ГЦА	Центр проверки мобильных и веб-приложений ФГАУ НИИ «Восход»
РБПО	Разработка безопасного программного обеспечения
ФСТЭК	Федеральная служба по техническому и экспортному контролю

1.2 Термины и определения

Термин	Определение
Базовые сервисы платформы «ГосТех»	Набор сервисов платформы «ГосТех», включающие в себя в том числе сервисы конфигурирования, аудита событий безопасности, журналирования, сбора метрик, управление учетными записями пользователей, управления базами данных различных типов, интеграционного взаимодействия и управления очередями сообщений, сервисы управления микросервисами и процессами, сервисы интеграции с инфраструктурой электронного правительства
Государственная информационная система	Федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях
ГИС на платформе	Государственные информационные системы, создаваемые, развиваемые, эксплуатируемые с

Термин	Определение
«ГосТех»	использованием программно-аппаратной среды, цифровых продуктов, включенных в каталог цифровых продуктов платформы «ГосТех», а также инструментов, информационных технологий платформы «ГосТех»
Жизненный цикл	Развитие системы, продукта, услуги, проекта или других изготовленных человеком объектов, начиная со стадии разработки концепции и заканчивая прекращением применения
Иностранный агент	Лицо (физическое или юридическое), которое, будучи резидентом одной страны, действует в интересах другой, обычно при отсутствии дипломатического иммунитета
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Инфраструктурные технологические сервисы	Инфраструктурные вычислительные ресурсы и сервисы, в том числе осуществляющие взаимодействие с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее - инфраструктура электронного правительства)
Дополнительные сервисы платформы «ГосТех»	Сервисы, реализующие дополнительные функциональные потребности, поставляемые в виде дистрибутивов программного обеспечения, в виде прикладных сервисов, работающих в инфраструктуре облачных вычислений, и в виде исходного кода, включенного в государственную библиотеку типовых программных компонентов информационных систем, предусмотренную постановлением Правительства Российской Федерации от 30 января 2013 г. № 62 «О национальном фонде алгоритмов и программ для электронных вычислительных машин»

Термин	Определение
Недостаток программы (сервиса)	Любая ошибка, допущенная в ходе проектирования или реализации программы, которая в случае ее не исправления может являться причиной уязвимости программы
Оператор ГИС	Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации государственной информационной системы, в том числе по обработке информации, содержащейся в ее базах данных
Оператор платформы «ГосТех»	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации или подведомственное ему казенное учреждение, которому переданы полномочия по осуществлению функций оператора Платформы «ГосТех»
Платформа «ГосТех»	Цифровая экосистема создания, развития и эксплуатации государственных информационных систем, включающих в себя единую программно-аппаратную среду, цифровые продукты, информацию, информационные технологии, государственные информационные системы, необходимые для реализации функций платформы «ГосТех», а также совокупность нормативных, правовых, организационных, методологических правил и процедур, обеспечивающих деятельность участников отношений, возникающих в связи с созданием и функционированием платформы «ГосТех»
Поставщики платформы «ГосТех»	Юридические или физические лица, в том числе зарегистрированные в качестве индивидуальных предпринимателей, предоставляющие сервисы на платформе «ГосТех»
Программное обеспечение	Совокупность программ для обработки информации и программных документов, необходимых для их эксплуатации
Разработчик ПО	Лицо, осуществляющее выполнение работ, оказание услуг по разработке ПО в составе ГИС на Платформе «ГосТех», в рамках заключенного государственного

Термин	Определение
	контракта (договора, соглашения) на создание, развитие, эксплуатацию ГИС на Платформе «ГосТех»;
Разработчик ГИС	Юридическое лицо или физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя, выполняющее функции по созданию или переработке (модернизации) ГИС на основании соответствующего договора
Сервис	Программное обеспечение, входящее в состав платформы «ГосТех» или ГИС на платформе «ГосТех» и реализующее дополнительные функциональные потребности, предназначенные для функционирования в отдельном процессе и взаимодействующие с другими сервисами и сторонними приложениями с использованием стандартизированных интерфейсов. Сервисы могут быть написаны на разных языках программирования и использовать разные технологии хранения данных
Сервисы защиты информации	Сервисы, обеспечивающие функции защиты информации, включающие в том числе программно-аппаратные комплексы и сервисы обнаружения и блокирования сетевых атак
Среда разработки	Среда, в которой осуществляется разработка программного обеспечения.
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
Уязвимость программы (сервиса)	Недостаток программы (сервиса), который может быть использован для реализации угроз безопасности информации
Экспертная организация по разработке безопасного ПО	Юридическое лицо, привлекающееся в соответствии с законодательством Российской Федерации к проведению испытаний ПО в составе ГИС и сервисов на платформе «ГосТех» на предмет выявления

Термин	Определение
	недостатков, уязвимостей и недекларированных возможностей.

2. Общие положения

Настоящая Концепция определяет основные подходы и перечень мер по разработке безопасного ПО необходимых для обеспечения и поддержания высокого уровня защищенности платформы «ГосТех» и ГИС на платформе «ГосТех».

Меры, предусмотренные настоящей концепцией, применяются к следующим субъектам и объектам платформы «ГосТех»:

Субъекты платформы «ГосТех»:

- разработчикам ПО в составе ГИС на платформе «ГосТех»;
- поставщикам сервисов платформы «ГосТех»;
- экспертным организациям в области разработки безопасного ПО;

Объекты платформы «ГосТех»:

- государственным информационным системам (ГИС);
- базовым сервисам платформы «ГосТех»;
- дополнительным сервисам платформы «ГосТех»;
- сервисам защиты информации;
- инфраструктурным технологическим сервисам.

Концепция представляет собой систематизированное изложение целей, и задач реализации организационных и технических мер по разработке безопасного ПО, необходимых к внедрению на платформе «ГосТех».

Организационно-распорядительные и иные нормативно-методические документы платформы «ГосТех», затрагивающие вопросы разработки безопасного ПО, должны разрабатываться и актуализироваться с учетом положений настоящей Концепции и не противоречить ей.

Положения Концепции являются основанием и методологической основой для:

а) формирования и внедрения единых требований и политики в области разработки безопасного ПО на платформе «ГосТех» для разработчиков ПО на платформе «ГосТех» и поставщиков сервисов на платформу «ГосТех»;

б) разработки и актуализации документов методического и организационного обеспечения в рамках процесса разработки безопасного ПО на платформе «ГосТех»;

в) разработки предложений по совершенствованию правового, методического, технического и организационного обеспечения процессов разработки безопасного ПО на платформе «ГосТех».

Положения Концепции определяют процессы, требования и меры по разработке безопасного ПО на платформе «ГосТех».

Детализация положений настоящей Концепции отражена в следующих методических документах платформы «ГосТех»:

1) Методические рекомендации «Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех». Основные требования к составу и функциям»;

2) Методические рекомендации по включению сервисов в Единую цифровую платформу Российской Федерации «ГосТех»;

3) Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы Российской Федерации «ГосТех».

Меры по разработке безопасного ПО на платформе «ГосТех» реализуются в рамках группы процессов управления разработкой безопасного ПО.

3. Правовая основа концепции

Настоящая Концепция разработана с учетом следующих нормативно-правовых актов и методических документов:

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

2) Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

3) Федеральный закон от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

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

5) Указ Президента РФ от 31.03.2023 № 231 «О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации «ГосТех»;

6) Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

7) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

8) Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

9) Методический документ «Меры защиты информации в государственных информационных системах» (ФСТЭК России, 2014 г);

10) Концепция информационной безопасности Единой цифровой платформы Российской Федерации «ГосТех»;

11) Политика информационной безопасности Единой цифровой платформы Российской Федерации «ГосТех»;

12) Положение о единой цифровой платформе Российской Федерации «ГосТех», утверждённое Постановлением Правительства Российской Федерации от 16.12.2022 № 2338;

13) ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

14) ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»;

15) ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

16) ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств».

4. Цели и задачи разработки безопасного программного обеспечения на платформе «ГосТех»

Внедрение на платформе «ГосТех» процессов и мер по разработке безопасного ПО осуществляется в следующих целях:

1) обеспечение бесперебойного функционирования государственных информационных систем на платформе «ГосТех»;

2) обеспечение конфиденциальности и безопасности обрабатываемой в государственных информационных системах с использованием платформы «ГосТех» информации;

3) сохранение качества предоставления государственных услуг, иных услуг и исполнения государственных функций посредством государственных информационных систем с использованием платформы «ГосТех»

Достижение указанных целей достигается за счет выявления и устранения недостатков и уязвимостей ПО на всех этапах жизненного цикла ПО и как следствие повышение общего уровня защищенности ПО в составе платформы «ГосТех» и ГИС на платформе «ГосТех».

Основными задачами внедрения процессов и мер по разработке безопасного ПО являются:

1) упорядочивание и формализация требований к процессам и мерам по разработке безопасного ПО, предъявляемых к объектам и субъектам платформы «ГосТех» на всех этапах жизненного цикла ПО;

2) формализация перечня и разработка процессов и организационных мер по разработке безопасного ПО на платформе «ГосТех»;

3) разработка и внедрение технических мер по разработке безопасного ПО на платформе «ГосТех», направленных на отслеживание, выявление и исправление недостатков и уязвимостей на всех этапах жизненного цикла ПО в составе ГИС на платформе «ГосТех» и сервисов;

4) повышение и поддержание на должном уровне компетенций в области разработки безопасного ПО разработчиков ПО, поставщиков сервисов, экспертных организаций и работников Оператора платформы «ГосТех»;

Внедрение процессов и мер по разработке безопасного ПО на платформе «ГосТех» позволит обеспечить:

– повышение общего уровня защищенности платформы «ГосТех» и ГИС на платформе «ГосТех»;

– устойчивое функционирование платформы «ГосТех» и ГИС на платформе «ГосТех»;

– доступность ГИС на платформе «ГосТех» и сервисов платформы «ГосТех» на требуемом уровне;

– снижение вероятности реализации угроз безопасности информации.

5. Требования по разработке безопасного программного обеспечения на платформе «ГосТех»

При разработке ПО, предназначенного для размещения и использования на платформе «ГосТех», должны выполняться требования по разработке безопасного ПО, определенные в следующих документах:

– Национальный стандарт ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– Методические рекомендации по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ в части используемых ими информационных технологий и технологий обеспечения информационной безопасности;

– Методические рекомендации по организации производственного процесса разработки государственных информационных систем с учетом применения итерационного подхода к разработке;

– Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы Российской Федерации «ГосТех»;

– Методические рекомендации «Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех». Основные требования к составу и функциям»;

– Методические рекомендации по включению сервисов в Единую цифровую платформу Российской Федерации «ГосТех»;

– Методические рекомендации по включению сервисов, обеспечивающих функции защиты информации;

– Методические рекомендации по включению инфраструктурных технологических сервисов в каталог цифровых продуктов единой цифровой платформы Российской Федерации «ГосТех».

Все вышеуказанные методические рекомендации публикуются в открытом доступе на официальном сайте Оператора платформы «ГосТех» по адресу: https://platform.gov.ru, в разделе «Документы».

Требования по реализации мер разработке безопасного ПО для ГИС на платформе «ГосТех» включаются в состав технических заданий на создание, разработку и эксплуатацию ГИС на платформе «ГосТех». Контроль наличия

указанных требований осуществляется Оператором ГИС в рамках экспертного контроля процессов создания, развития и эксплуатации ГИС на платформе «ГосТех».

Подтверждение полноты реализованных мер по разработке безопасного ПО на платформе «ГосТех» в отношении сервисов платформы «ГосТех» должно осуществляться Оператором платформы «ГосТех» в рамках действующего законодательства и в соответствии нормативно-правовыми актами уполномоченных федеральных органов исполнительной власти.

Контроль за выполнением требований по разработке безопасного программного обеспечения на платформе «ГосТех» осуществляется Оператором платформы «ГосТех» в рамках действующего законодательства Российской Федерации и его полномочий.

5.1 Требования к субъектам и объектам платформы «ГосТех»

Требования по разработке безопасного программного обеспечения также определены в утвержденных методических документах на платформу «ГосТех» и применяются с учетом типа субъекта платформы «ГосТех».

Применимость требований в утвержденных методических документах на платформу «ГосТех» в зависимости от типа субъекта представлена в Таблице 1.

Таблица 1 – Распределение требований по типам поставщиков

Тип поставщика платформы «ГосТех»	**Наименование методического документа платформы «ГосТех»**
Разработчик ПО	Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы Российской Федерации «ГосТех»
Поставщик базовых сервисов платформы «ГосТех»	Методические рекомендации Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех» Основные требования к составу и функциям

Тип поставщика платформы «ГосТех»	Наименование методического документа платформы «ГосТех»
Поставщик дополнительных сервисов платформы «ГосТех»	Методические рекомендации по включению сервисов в Единую цифровую платформу Российской Федерации «ГосТех»
Поставщик сервисов защиты информации платформы «ГосТех»	Методические рекомендации по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ в части используемых ими информационных технологий и технологий обеспечения информационной безопасности
Поставщик инфраструктурных технологических сервисов	Методические рекомендации по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ в части используемых ими информационных технологий и технологий обеспечения информационной безопасности

Требования к экспертным организациям в области разработки безопасного ПО определяются настоящей Концепцией и должны быть учтены при разработке нормативно правовых актов и методических доку ментов, регулирующих процессы функционирования платформы «ГосТех».

Экспертные организации, привлекаемые к проведению испытаний ПО в составе ГИС и сервисов на платформе «ГосТех» на предмет выявления недостатков, уязвимостей и недекларированных возможностей должны соответствовать следующим требованиям:

иметь лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации (виды работ «б», «д» или «е»);

иметь в штате не менее 5 работников, успешно прошедших повышение квалификации по программам в области технической защиты информации по направлениям фаззинг-тестирования программного

обеспечения, анализа архитектуры и экспертизы исходных кодов программного обеспечения, статического анализа исходных кодов программного обеспечения;

иметь утвержденную, Методику выявления уязвимостей и недекларированных возможностей в программном обеспечении, разработанную в соответствии с национальными стандартами Российской Федерации и руководящими документами ФСТЭК России.

Разработчик ПО, планируемого к применению на платформе «ГосТех» ПО должен соответствовать требованиям нормативно-методических документов на платформу «ГосТех» и следующим требованиям:

вид деятельности по разработке ПО отражен в учредительных документах разработчика ПО;

разработчик ПО не является иностранным агентом;

разработчик ПО не должен находится в реестре недобросовестных поставщиков (подрядчиков, исполнителей);

материально-техническая база разработчика ПО, задействованная в процессе разработки ПО, должна быть размещена на территории Российской Федерации.

Требования по разработке безопасного программного обеспечения также определены в утвержденных методических документах на платформу «ГосТех» и применяются с учетом типа объекта платформы «ГосТех».

Требования к Поставщикам сервисов защиты информации платформы «ГосТех», определяются в Методических рекомендациях по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ в части используемых ими информационных технологий и технологий обеспечения информационной безопасности в строгом соответствии с законодательством Российской Федерации и нормативно-правовыми актами ФСТЭК России и ФСБ России.

Применимость требований в утверждённых методических документах на платформу «ГосТех» в зависимости от типа объекта представлена в Таблице 2.

Таблица 2 - Распределение требований по типам объектов

Тип объекта платформы «ГосТех»	**Наименование методического документа платформы «ГосТех»**
ПО в составе ГИС	Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы Российской Федерации «ГосТех»
Базовый сервис платформы «ГосТех»	Методические рекомендации Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех» Основные требования к составу и функциям
Дополнительный сервис платформы «ГосТех»	Методические рекомендации по включению сервисов в Единую цифровую платформу Российской Федерации «ГосТех»
Сервис защиты информации платформы «ГосТех»	Методические рекомендации по включению сервисов, обеспечивающих функции защиты информации
Инфраструктурный технологический сервис	Методические рекомендации по включению инфраструктурных технологических сервисов в каталог цифровых продуктов единой цифровой платформы Российской Федерации «ГосТех»

Требования и рекомендации по разработке безопасного ПО методических документов платформы «ГосТех» являются обязательными к исполнению в рамках существующих процессов функционирования платформы «ГосТех» и в соответствии с областью применения методических документов.

Субъекты платформы «ГосТех», не соответствующие требованиям по разработке безопасного ПО, не привлекаются для выполнения работ и оказания услуг на платформе «ГосТех».

Все сервисы в составе платформы «ГосТех» подлежать категоризации на предмет возможности их использования (применения) при создании, развитии и эксплуатации с учетом классов защищенности ГИС, уровней защищенности обрабатываемых персональных данных и категорий значимости объектов критической информационной инфраструктуры Российской Федерации.

Требования к разработке безопасного программного обеспечения, реализующего функции защиты информации и используемого в составе Сервисов защиты информации платформы «ГосТех», определяются в Методических рекомендациях по включению сервисов, обеспечивающих функции защиты информации в строгом соответствии с законодательством Российской Федерации и нормативно-правовыми актами ФСТЭК России и ФСБ России.

ПО, не соответствующее требованиям документов, указанных в настоящем разделе, не допускается к размещению и использованию в продуктивных средах функционирования платформы «ГосТех», при этом допускается использование такого ПО в тестовых средах и средах разработки только в целях проведения дополнительных инструментальных исследований и обязательным применением в указанных средах компенсирующих мер по защите информации, направленных на предотвращение угроз безопасности информации, связанных с эксплуатацией уязвимостей и несанкционированным доступом к объектам платформы «ГосТех».

5.2Процессы и организационные меры по разработке безопасного ПО

Процессы управления разработкой безопасного ПО являются одной из ключевых групп процессов системы управления информационной безопасностью платформы «ГосТех».

Процессы управления разработкой безопасного ПО регулируются и регламентируются организационно-распорядительной документацией Оператора платформы «ГосТех».

Организационно-распорядительная документация Оператора платформы «ГосТех» в области разработки безопасного ПО должна учитывать

требования законодательства Российской Федерации, нормативных и правовых актов уполномоченных федеральных органов исполнительной власти и национальных стандартов в области разработки безопасного ПО.

Обеспечение внедрения и контроль организационных мер по разработке безопасного ПО на платформе осуществляется отдельным специализированным подразделением (Управлением) в составе организационно-штатной структуры Оператора платформы «ГосТех».

Оператор платформы «ГосТех» в соответствии с настоящей Концепцией и ФГАУ НИИ «Восход» (в рамках функционирования Центра проверки мобильных и веб-приложений) являются экспертными организациями в области разработки безопасного ПО на платформе «ГосТех» и могут привлекаться в соответствии с законодательством Российской Федерации к проведению испытаний ПО в составе ГИС и сервисов на платформе «ГосТех» на предмет выявления недостатков, уязвимостей и недекларированных возможностей наравне с другими экспертными организациями.

Основной состав процессов управления разработкой безопасного ПО Оператора платформы «ГосТех» включает:

- управления требованиями по разработке безопасного ПО в составе ГИС на платформе «ГосТех»;
- управления недостатками и уязвимостями компонентов сторонних разработчиков в системе управления конфигурацией ПО платформы «ГосТех;
- инструментального исследования ПО ГИС на платформе «ГосТех»;
- управления недостатками и уязвимостями ПО в составе ГИС на платформе «ГосТех»;
- проведения технической экспертизы сервисов платформы «ГосТех»;
- контроля соблюдения поставщиками платформы «ГосТех» требований по разработке безопасного ПО, описанных в требованиях по разработке безопасного программного обеспечения, определенными национальным стандартом ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», а также методических документов платформы «ГосТех»;
- обучения поставщиков платформы «ГосТех» по разработке безопасного ПО на платформе «ГосТех».

Состав процессов управления разработкой безопасного ПО на платформе «ГосТех» может меняться в зависимости от развития платформы

«ГосТех», при этом цели внедрения процессов должны строго соответствовать целям, указанным в настоящей концепции.

Процессы управления разработкой безопасного ПО должны быть интегрированы с процессами функционирования платформы «ГосТех».

5.3Технические меры по разработке безопасного ПО на платформе «ГосТех»

Технических меры по разработке безопасного ПО на платформе «ГосТех», реализуются при проведении инструментальных исследований ПО (объектов платформы «ГосТех») в рамках проводимых процедур по технической экспертизе ПО в составе ГИС на платформе «ГосТех» и сервисов.

Состав работ и процедур Оператора платформы «ГосТех» по инструментальному исследованию соответствует требованиям национального стандарта ГОСТ Р 56939 и включает в себя следующие основные процедуры:

- анализ заимствованных компонентов сторонних разработчиков из внешних репозиториев;
- антивирусная проверка компонентов сторонних разработчиков из внешних репозиториев;
- статический анализ исходного кода программы;
- экспертиза исходного кода программы;
- динамический анализ исходного кода программы;
- фаззинг-тестирование;
- тестирование на проникновение.

Тестирование на проникновение должно проводится на регулярной основе (не реже 1 раза в год) только в отношении платформы «ГосТех» и ГИС на платформе «ГосТех».

Процедура анализа заимствованных компонентов сторонних разработчиков из внешних репозиториев должно проводится не реже 1 раза в месяц и позволяет обеспечить своевременное обнаружение недостатков и уязвимостей заимствованных компонентов ПО в составе платформы «ГосТех» и ГИС на платформе «ГосТех» в процессе их эксплуатации. Актуализация информации о зависимостях ПО в составе ГИС на платформе «ГосТех» проводится не реже 3 раз за период времени между публикацией значительных изменений ПО, но не реже 1 раза в месяц.

Следующая информация и события подлежат обязательной регистрации в системе мониторинга информационной безопасности в целях последующей корреляции и своевременного выявления событий информационной безопасности:

информация о выявленных недостатках и уязвимостях ПО в составе ГИС на платформе «ГосТех»;

перечень заимствованных компонентов сторонних разработчиков ПО на платформе «ГосТех»;

информация об уязвимостях заимствованных компонентов сторонних разработчиков ПО в составе ГИС на платформе «ГосТех»;

события о фактах установки ПО в среды функционирования (дата и время выполнения работ, учетная запись и IP адрес исполнителя работ)

Анализ зависимостей ПО проводится по внешним базам уязвимостей (в том числе – БДУ ФСТЭК России). Получение информации о недостатках и уязвимостях должно обеспечиваться из источников данных, размещенных на территории Российской Федерации, а владельцами такой информации должны являться организации резиденты Российской Федерации, не являющиеся иностранными агентами.

Предоставление и хранение информации о результатах проведения инструментальных исследований ПО на наличие недостатков и уязвимостей ПО в составе платформы «ГосТех» и ГИС на платформе «ГосТех» осуществляется в стандартизированном структурированном виде и в форме электронных документов.

Информации о результатах исследований является конфиденциальной. Обработка такой информации допускается Оператором платформы «ГосТех» или Оператором ГИС на платформе «ГосТех» или юридическими лицами, осуществляющими работы по созданию, развитию и эксплуатации ГИС на законном основании с соблюдением мер и требований по защите информации, предусмотренных действующим законодательством Российской Федерации.

Оператор платформы «ГосТех» осуществляет сбор и хранение информации о недостатках, уязвимостях и уровне защищенности ПО платформы «ГосТех» и ГИС на платформе «ГосТех» на всем этапе жизненного цикла ПО. Срок хранения информации об объектах, выведенных из эксплуатации, составляет не менее 5 лет.

В разработке ПО в составе ГИС на платформе «ГосТех» используются только доверенные репозитории, владельцами которых являются

государственные органы и организации резиденты Российской Федерации, не являющиеся иностранными агентами.

5.4 Повышение и поддержание на должном уровне компетенций в области разработки безопасного ПО

Для обеспечения достижения целей настоящей концепции и решения поставленных задач на платформе «ГосТех» организуется и обеспечивается обучение субъектов платформы «ГосТех»: Разработчиков ГИС, Поставщиков, работников Оператора «ГосТех» по вопросам разработки безопасного ПО на платформе «ГосТех».

В рамках обучения рассматриваются как теоретические, так и практические вопросы проектирования и разработки безопасного ПО.

Обучение осуществляться преимущественно с использованием автоматизированной системы Оператора «ГосТех».

Курс обучения содержит как обязательные курсы, так и дополнительные курсы с разделением по типам субъектов платформы «ГосТех».

Наличие подтверждения успешного прохождения обучения субъектами платформы «ГосТех» может использоваться Оператором платформы «ГосТех» для процедур оценки компетенций и качества услуг, предоставляемых субъектами платформы «ГосТех», в том числе при осуществлении конкурсных процедур.

6. Подтверждение соответствия программного обеспечения требованиям по разработке безопасного ПО

Подтверждение соответствия ПО, не реализующего функции защиты информации, установленным требованиям по разработке безопасного ПО может проводиться:

а) в форме Протокола испытаний, проводимых Оператором платформы «ГосТех» и(или) экспертными организациями в рамках разработки ГИС на платформе «ГосТех» или добавления сервисов в платформу «ГосТех».

б) в форме испытаний, проводимых разработчиком ПО при приемке разработанного ПО с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации. Документом, подтверждающим соответствие ПО, не реализующего функции защиты информации, установленным требованиям является протокол испытаний с положительным заключением о соответствии ПО и необходимой документации установленным требованиям.

в) в форме добровольной сертификации ПО на соответствие требованиям по разработке безопасного ПО. Документом, подтверждающим соответствие ПО, не реализующего функции защиты информации, установленным требованиям является сертификат соответствия системы добровольной сертификации, выданный на ПО.

7. Порядок пересмотра концепции

Положения настоящей Концепции подлежат пересмотру не реже 1 раза в год в установленном порядке в случае существенных изменений законодательства, изменений требований в области разработки безопасного ПО на платформе «ГосТех» и возникновении условий невозможности выполнения мероприятий по внедрению организационных и технических мер по разработке безопасного программного обеспечения на платформе «ГосТех» в установленные сроки (Приложение №1).

Приложение к Концепции
разработки безопасного
программного обеспечения
на единой цифровой платформе
Российской Федерации «ГосТех»

План мероприятий по внедрению организационных и технических мер по разработке безопасного программного обеспечения на платформе «ГосТех»

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
Формализация и актуализация требований по разработке безопасного ПО					
1.	Разработка и актуализация требований по разработке безопасного ПО в соответствии с настоящей Концепцией	1 августа 2023 г.	Рабочая группа по защите информации в ЕЦП «ГосТех» (далее – Рабочая группа по ЗИ), ФКУ «ГосТех»	Разработаны и актуализированы требования. Требования включены в проекты методических рекомендаций, определяющих требований по разработке безопасного ПО на платформе «ГосТех»	

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
2.	Согласование проектов методических рекомендаций, определяющих требований по разработке безопасного ПО на платформе «ГосТех» с МРГ[1]	30 ноября 2023 г.	Члены МРГ, ФКУ ГосТех, Минцифры России	Проекты одобрены протоколом заседания МРГ	
3.	Вынесение проектов методических рекомендаций, определяющих требования по разработке безопасного ПО на платформе «ГосТех» на голосование в Президиум Правительственной комиссии	31 декабря 2023 г.	Минцифры России, ФКУ ГосТех	Проекты документов вынесены на голосование в Президиум Правительственной комиссии в установленном порядке	

[1] Межведомственная рабочая группа по архитектуре базовых информационных ресурсов и принципам обработки данных, состав которой утвержден Заместителем Председателя Правительства Российской Федерации Д.Н. Чернышенко 17 ноября 2021 г. № ДЧ-П10-16443

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
4.	Проведение оценки и принятие решения о необходимости актуализации корректировки настоящей Концепции и плана мероприятий	не реже1 раз в год	Рабочая группа по ЗИ, Минцифры России, ФКУ «ГосТех»,	Внесены изменения в Концепцию и план мероприятий (при наличии необходимости)	
Внедрение организационных мер по разработке безопасного ПО					
5.	Разработка и утверждение регламентов и методик проведения инструментальных исследований ПО	1 апреля 2024 г.	ФКУ «ГосТех»	Документы, разработаны и утверждены ФКУ «ГосТех»	Реализация мероприятия возможна после успешного внедрения подсистемы анализа защищенности ПО в составе ГИС Управления платформой «ГосТех» в соответствии с п. 9 настоящего Плана

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
6.	Разработка и утверждение порядка включения цифровых продуктов в каталог цифровых продуктов платформы «ГосТех»	1 июня 2023 г.	ФКУ «ГосТех», Минцифры России	Документ определяющий порядок включения цифровых продуктов в каталог цифровых продуктов платформы «ГосТех», утвержден нормативно-правовым актом Минцифры России	
7.	Проведение оценки сервисов, включаемых в состав платформы «ГосТех» на соответствие требованиям по разработке безопасного ПО и в соответствии в соответствии с порядком включения цифровых продуктов в каталог цифровых продуктов платформы «ГосТех»	На регулярной основе	ФКУ «ГосТех»	В каталог цифровых продуктов платформы «ГосТех» включается не менее 10 цифровых продуктов в год	
Технические меры по разработке безопасного ПО					
8.	Выделение дополнительного финансирования на развитие ГИС Управления платформой «ГосТех», в части реализации подсистемы анализа защищенности ПО в составе ГИС Управления платформой «ГосТех»	30 июня 2023	Минцифры России, ФКУ «ГосТех» (в части определения объема затрат)	Финансирование доведено	

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
9.	Разработка и внедрение подсистемы анализа защищенности ПО в составе ГИС Управления платформой «ГосТех»	1 апреля 2024 г.	ФКУ «ГосТех» Исполнитель по ГК	Заключен государственный контракт (ГК) или заключено дополнительное соглашение к действующему ГК. Подсистема внедрена в рамках ГИС Управления платформой «ГосТех»	
10.	Разработка плана проверок ГИС, размещаемых на платформе «ГосТех», в ГЦА ФГАУ НИИ Восход	30 июня 2023 г.	Минцифры России, ФКУ «ГосТех» ФГАУ НИИ Восход	План проверок ГИС на платформе «ГосТех», в ГЦА ФГАУ НИИ Восход	План разрабатывается на основании плана создания и развития ГИС на платформе «ГосТех»
11.	Выделение финансирования на проведение проверок ГИС, размещаемых на платформе «ГосТех», в ГЦА ФГАУ НИИ Восход	1 августа 2023 г.	Минцифры России, ФГАУ НИИ Восход	Финансирование доведено в объеме запланированного объема проверок	
12.	Проведение проверок ПО в составе ГИС на платформе «ГосТех»	По отдельному плану	ФГАУ НИИ Восход ФКУ ГосТех	Заключение и протоколы проверки ГИС	Сроки проведения проверок определяются планом проверок ГИС на платформе «ГосТех»

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
13.	Разработка требований по развитию ГЦА ФГАУ НИИ Восход в части реализации функционала в соответствие с требованиями по разработке безопасного ПО на платформе «ГосТех»	1 июня 2023 г.	ФГАУ НИИ Восход, ФКУ «ГосТех»	Проект технического задания на развитие ГЦА разработан	
14.	Выделение финансирования на развитие ГЦА ФГАУ НИИ Восход	30 июня 2023 г.	Минцифры России, ФГАУ НИИ Восход	Финансирование доведено	
15.	Проведение модернизации ГЦА ФГАУ НИИ Восход в части реализации функционала в соответствие с требованиями по разработке безопасного ПО на платформе «ГосТех»	1 апреля 2024 г.	ФГАУ НИИ Восход	Функционал ГЦА ФГАУ НИИ Восход реализован в соответствии требованиям по разработке безопасного ПО (в части технических мер)	
16.	Разработка регламента взаимодействия с ГЦА ФГАУ НИИ Восход по проверке ГИС в соответствии с требованиями РБПО	30 июня 2023 г.	ФКУ ГосТех ФГАУ НИИ Восход	Регламент взаимодействия с ГЦА ФГАУ НИИ Восход по проверке ГИС согласован и утвержден.	
Информирование и обучение по вопросам разработки безопасного ПО					
17.	Разработка инструкций для разработчиков ГИС на платформе	30 сентября 2024 г.	ФКУ ГосТех	Инструкции для разработчиков на платформе	

№ п/п	Наименование мероприятия	Срок реализации	Ответственные	Ожидаемый результат	Комментарий
18.	Выделение дополнительного финансирования на создание подсистемы обучения в составе ГИС Управления платформой «ГосТех»	30 июня 2023	Минцифры России, ФКУ «ГосТех» (в части определения объема затрат)	Финансирование доведено	
19.	Разработка и внедрение подсистемы обучения платформы в составе ГИС Управления платформой «ГосТех»	1 апреля 2024 г.	Исполнитель по ГК, ФКУ «ГосТех»	Заключен государственный контракт (ГК) или заключено дополнительное соглашение к действующему ГК. Подсистема внедрена в рамках ГИС Управления платформой «ГосТех»	
20.	Разработка обучающих и информационных материалов по разработке безопасного ПО для подсистемы обучения платформы в составе ГИС Управления платформой «ГосТех»	1 апреля 2024 г.	ФКУ ГосТех, Исполнитель по ГК	Материал разработан и загружен в подсистему обучения	
21.	Организация и проведение обучения субъектов платформы «ГосТех»	На регулярной основе с 1 апреля 2024 г.	ФКУ ГосТех	Обучающие и информационные материалы доступны всем субъектам платформы «ГосТех»	