ПРИЛОЖЕНИЕ № 1
к протоколу заседания Межведомственной
рабочей группы по разработке и реализации
Национальной технологической инициативы
при Правительственной комиссии по модернизации
экономики и инновационному развитию России
от 7 апреля 2026 г. № 1пр

ПЛАН
мероприятий («дорожной карты») «Сейфнет» Национальной технологической инициативы

I. Паспорт плана мероприятий («дорожной карты»)

Наименование рабочей группы	Сейфнет
Руководитель и (или) соруководитель рабочей группы	Андрей Иванович Тихонов Александр Михайлович Шойтов Василий Викторович Шпак
Ответственный федеральный орган исполнительной власти	Минпромторг России
Заинтересованные федеральные органы исполнительной власти	Минпромторг России Минцифры России Минобрнауки России
Цели плана мероприятий («дорожной карты»)	К 2035 году сформировать глобально конкурентоспособную российскую индустрию Конструктивной Безопасности
Перечень целевых показателей плана мероприятий («дорожной карты»)	Целевой показатель 1: Объем рынка решений Конструктивной Безопасности Целевой показатель 2: Уровень уязвимости продуктов, доверенных программно-аппаратных комплексов (далее – ДПАК) и систем, созданных на основе методики Конструктивной Безопасности Целевой показатель 3: Уровень технической готовности методики Конструктивной Безопасности Целевой показатель 4: Уровень технической готовности Архитектур Безопасности Целевой показатель 5: Уровень технической готовности Гарантий Целостности на основе криптографических методов Целевой показатель 6: Количество центров компетенции по Конструктивной Безопасности

	Целевой показатель 7: Количество центров по подготовке кадров по Конструктивной Безопасности Целевой показатель 8: Количество компаний-участников экосистемы Конструктивной Безопасности Целевой показатель 9: Количество зарегистрированных специалистов-участников профессионального сообщества Конструктивной Безопасности
Этапы и сроки реализации	Первый этап (2026-2027 годы) Второй этап (2028-2030 годы) Третий этап (2030-2035 годы)
Направления реализации плана мероприятий ("дорожной карты")	1. Анализ целевых рынков 2. Развитие методики Конструктивной Безопасности 3. Развитие Архитектуры Безопасности 4. Развитие гарантий целостности криптографическими методами 5. Доверенные аппаратные средства (включая электронную компонентную базу (далее – ЭКБ))
Значимые контрольные результаты реализации	Объем и доля рынка в Российской Федерации Объем и доля рынка за рубежом
Общий объем финансового обеспечения по основным этапам, включая оценку объемов государственной поддержки реализации мероприятий	2026-2027 гг. – 10 млрд руб.[1] 2028-2030 гг. – 25 млрд руб.[1] 2030-2035 гг. – 50 млрд руб.[1]

II. Описание сферы реализации плана мероприятий («дорожной карты»)

1. Краткое описание возникающего в результате реализации плана мероприятий («дорожной карты») рынка (далее – возникающий рынок)

Современная критическая инфраструктура, обеспечивающая повседневные потребности населения, немыслима без применения современных информационно-коммуникационных технологий. Устойчивость ее функционирования является залогом безопасности, благополучия и экономической стабильности граждан, поэтому критические информационные системы (далее – ИС), телекоммуникации и автоматические системы управления категорируются и регулируются Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. В силу существующей международной обстановки, объекты критической информационной инфраструктуры (далее –

[1] Расчет общего объема финансового обеспечения осуществлен в результате экспертной оценки членов рабочей группы «Сейфнет» НТИ и не несет обязательств для федерального бюджета

КИИ) подвержены рискам и угрозам безопасности, спектр которых постоянно растет:

- расширяется список киберугроз, в том числе с применением Искусственного Интеллекта (далее – ИИ);
- создаются новые технологии преодоления средств кибербезопасности, в том числе с помощью квантовых вычислений;
- растет количество программного и аппаратного обеспечения в КИИ, в том числе зарубежного производства, доверие к которому неуклонно снижается в связи с наличием недокументированных возможностей;
- меняется профиль нарушителей – помимо киберпреступников и кибертеррористов в действие вступают спецслужбы недружественных государств;
- социальные сети, средства массовой персонализации, технологии ИИ позволяют активно воздействовать на ответственных исполнителей, превращая их в потенциальных нарушителей.

Все это ставит вопрос о будущем облике критической информационной инфраструктуры, которая должна обладать изначально заложенными свойствами доверия и безопасности, а также обладать устойчивостью к внешним и внутренним угрозам.

Основной целью инициатив и мероприятий дорожной карты «Сейфнет» является создание методов, технологий и продуктов повышения технологической устойчивости функционирования объектов критической информационной инфраструктуры.

В качестве основных источников рисков и угроз рассматриваются:

- иностранные государства и аффилированные с ними лица, действующие с целью нанесения ущерба экономике, безопасности и обороне Российской Федерации;
- факторы, затрудняющие и замедляющие создание и воспроизводство объектов КИИ, связанные с отсутствием или недостаточностью суверенной технологической базы Российской Федерации.

В частности, в качестве основных факторов рисков и угроз рассматриваются:

- внедрение недокументированных возможностей;
- ограничение на поставку в Российскую Федерацию комплектующих и материалов;
- вывод создания и производства технологий за пределы Российской Федерации;
- блокирование счетов и финансовых средств, необходимых для закупки комплектующих, средств разработки и производства;
- запрет технической поддержки и гарантийного обслуживания;
- блокирование функционирования через удаленные каналы управления;
- недоступность средств разработки;
- отзыв лицензий на применение технологий;

- отсутствие компетенций по собственному воспроизведению технологий;
- применение инструментов ИИ злоумышленниками;
- увеличение темпов атак на КИИ.

Существующий портфель технологий Российской Федерации не позволяет в полной мере обеспечить потребности отечественной критической информационной инфраструктуры. При этом:

- к сильным сторонам отечественного набора технологий относятся отечественная школа информационной и кибербезопасности, отечественная школа криптографии, собственные средства защиты информации, полный набор отечественных средств разработки и доверенного Искусственного Интеллекта;
- к слабым сторонам относятся широкое использование зарубежных технологий в рамках критических систем, доминирование зарубежных стандартов, архитектур и методик, а также ограниченные возможности отечественного микроэлектронного производства.

Таким образом, основным вызовом является невозможность заменить все зарубежные продукты и технологии российскими аналогами, а основной возможность стало использование передовых отечественных разработок в области безопасности для создания доверенных и безопасных систем КИИ из доверенных и недоверенных модулей с использованием передовых отечественных методик и архитектурных средств, микроядерных операционных систем, инструментов разработки, валидации и верификации, а также средств защиты информации, включая криптографические. При этом применение данных средств должно быть максимально эффективным и минимально затратным, а также гарантировать быструю и гибкую адаптацию уже эксплуатируемых систем к новым угрозам информационной и кибербезопасности.

Именно поэтому в качестве базового подхода для повышения технологической устойчивости объектов критической инфраструктуры используется Конструктивная Безопасность («Secure by Design») – прорывное направление в области информационной и кибербезопасности, позволяющее создавать критическую информационную инфраструктуру, обладающую иммунитетом против существующих и будущих угроз, и позволяющее создавать доверенные и безопасные системы на основе как доверенных, так и недоверенных модулей с использованием современных отечественных средств защиты.

Для реализации данного подхода в дорожной карте «Сейфнет» Национальной технологической инициативы (далее – НТИ) предусматривается развитие сквозных технологий доверия и безопасности:

- методики Конструктивной Безопасности, которая позволяет на основе работы с рисками и требованиями, на основе существующих моделей и шаблонов, сформировать безопасный дизайн систем и продуктов, а также реализовать требования безопасности на всех стадиях разработки продуктов

и систем, проводить сквозную верификацию и валидацию на предмет соответствия заявленным характеристикам;

- Архитектура Безопасности – набор архитектурных решений, средств защиты информации и методик их применения для реализации безопасных и доверенных продуктов и систем, состоящих из доверенных и недоверенных элементов;
- средства обеспечения гарантий целостности криптографическими методами – набор средств криптографической защиты, включая корень доверия, электронную подпись, удостоверяющие центры.

Применение этих технологий и методов позволит отечественной индустрии создать полный стек продуктов, необходимых для построения критической инфраструктуры, устойчивых к современным и будущим киберугрозам, включая:

- платформенные средства защиты информации, включая криптографические – реализующие полный набор функций безопасности от идентификации и профилактики угроз до восстановления и киберкриминалистики на всех уровнях реализации КИИ – включая ЭКБ, радиоэлектронную аппаратуру (далее – РЭА), ДПАК, программное обеспечение, объекты и субъекты КИИ (уровень предприятия);
- безопасную и защищенную радиоэлектронную аппаратуру, включая вычислительную технику (далее – ВТ), телеком-оборудование (далее – ТКО) и автоматизированную систему управления технологическим процессом (далее – АСУТП), имеющую в своем составе средства обеспечения доверия и безопасности, защищенную ЭКБ, ЭКБ безопасности и др.;
- безопасную и защищенную ЭКБ, созданную на основе защищенной процессорной архитектуры, реализующей функции доверия и безопасности, имеющей в своем составе функциональные модули безопасности, созданную с учетом требований безопасной разработки.

Применение сквозных технологий и методик Конструктивной Безопасности, безопасного жизненного цикла и безопасной архитектуры на основе политик безопасности, а также продуктов на их основе позволит:

- создавать доверенные и безопасные продукты и системы на основе доверенных и недоверенных элементов, потенциально содержащих недокументированные возможности;
- уменьшить количество уязвимостей в системах и продуктах, содержащих недоверенные элементы, потенциально содержащие недокументированные возможности;
- увеличить устойчивость существующих объектов критической инфраструктуры к существующим и новым киберугрозам, в первую очередь – на основе Искусственного Интеллекта;
- повысить эффективность защиты существующих и новых объектов критической инфраструктуры, снизив затраты на их создание и модернизацию;

- создавать новые типы критической инфраструктуры, требующие высокой степени защиты автономных систем, таких как беспилотные и космические аппараты, территориально-распределенные системы управления инфраструктурой, энергетики, транспорта и др.

В силу глобального роста угроз кибербезопасности, а также снижения доверия к традиционным западным поставщикам информационных и промышленных систем, информационно-коммуникационных технологий (далее – ИКТ) и средств информационной и кибербезопасности, подобные продукты будут обладать повышенной конкурентоспособностью на международном рынке, в первую очередь – на рынках дружественных стран.

2. Описание основных участников возникающего рынка

2.1.Ключевые международные участники возникающего рынка

К ключевым международным участникам рынка относятся: IBM, Microsoft, Cisco, Intel, MacAfee, Semantec, Fortinet.

2.2.Ключевые российские участники возникающего рынка

К ключевым российским участникам рынка относятся:

- Акционерное общество «Лаборатория Касперского» (АО «Лаборатория Касперского»);
- Группа компаний «Солар» (ГК «Солар»);
- Общество с ограниченной ответственностью «Код Безопасности» (ООО «Код Безопасности»);
- Акционерное общество «Инфотекс» (АО «Инфотекс»);
- Акционерное общество «Научно-технический центр «Атлас» (АО «НТЦ «Атлас»);
- ГК Элемент, АО Микрон, НИИМЭ, НИИМА Прогресс;
- Группа компаний «Инфотактика» (ГК «Инфотактика»);
- Общество с ограниченной ответственностью «Базальт Свободное Программное Обеспечение (ООО «Базальт СПО»),
- Институт системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН);
- Федеральное государственное автономное учреждение «Федеральный научный центр «Научно-исследовательский институт системных исследований» Национального исследовательского центра «Курчатовский институт» (ФГУ ФНЦ НИИСИ РАН);
- Национальный исследовательский университет «Московский институт электронной техники» (НИУ МИЭТ);
- Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ);

- Федеральное государственное автономное образовательное учреждение высшего образования Томский государственный университет систем управления и радиоэлектроники (ТУСУР);
- Автономная некоммерческая организация «Национальный технологический центр цифровой криптографии» (АНО «НТЦ ЦК»);
- Общество с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»).

3. Сведения о глобальном контексте возникновения нового рынка

3.1. Глобальные технологические тренды и трансформационные изменения в традиционных отраслях, вызванные внедрением сквозных технологий и находящиеся в сфере реализации плана мероприятий («дорожной карты»)

К глобальным технологическим трендам, которые необходимо учитывать при разработке и реализации «дорожной карты», относятся:

- технологии ИИ, позволяющие революционно изменить ландшафт информационных и киберугроз;
- квантовые вычисления, позволяющие преодолеть традиционные средства криптографической защиты;
- новые технологии разработки, позволяющие закладывать недокументированные возможности на всех этапах жизненного цикла;
- новые технологии производства, позволяющие создавать недокументированные возможности, которые невозможно выявить традиционными средствами;
- технологии распределенного нотариата, позволяющие создать платформы и интеграционную среду для автоматического обмена автономных устройств.

3.2. Глобальные политические, экономические, социальные, экологические и регуляторные тренды

К иным трендам относятся:

- деглобализация – слом существующих и формирование новых технологических цепочек;
- социальные сети с массовым профилированием и персонификацией;
- применение технологий ИИ для формирования персонализированного контента с целью управления мировосприятием и поведением.

4. Сегментация возникающего рынка, оценка конкурентности и темпов роста сегментов в их текущем виде

Сегментация рынка Сейфнет осуществлена по следующим направлениям:

- Отраслевые рынки Критической Инфраструктуры;
- Конструктивная Безопасность и безопасная разработка на основе анализа рисков устойчивого функционирования;
- Архитектура доверия и безопасности;
- Обеспечение гарантий целостности криптографическими методами;
- Доверенные и безопасные аппаратные средства, ЭКБ и радиоэлектронная продукция (далее – РЭП).

5. Сформированный в Российской Федерации научно-технический задел для реализации плана мероприятий («дорожной карты»)

На сегодняшний день в Российской Федерации уже сформирован научно-технологический задел для становления рынка Сейфнет, который включает:

- Методика Конструктивной Безопасности;
- Методики безопасной разработки;
- Передовая отечественная школа криптографии;
- Технологии доверенного Искусственного Интеллекта;
- Технологии работы с требованиями и рисками при проектировании инженерных систем;
- Технологии распределенного нотариата;
- Прорывные технологии защиты информации, в том числе криптографические;
- Дизайн радиоэлектронной продукции;
- Национальные архитектуры и дизайн ЭКБ;
- Технологии Фотоники.

6. Основные направления реализации плана мероприятий («дорожной карты»)

6.1.Создание, развитие и продвижение передовых технологий, продуктов и услуг, обеспечивающих приоритетные позиции российских компаний на формируемых глобальных рынках

Название направления плана мероприятий («дорожной карты»)	Краткое описание направления плана мероприятий («дорожной карты»)
1. Целевые рынки применения сквозных технологий доверия и безопасности	Рынок новой критической информационной инфраструктуры, формирующейся из территориально распределенных автономных высокотехнологических устройств, объединенных в единую сеть с помощью современных систем связи
2. Максимальный уровень критичности уязвимостей	Максимальный уровень уязвимости продуктов, ДПАК и систем, достигаемый за счет применения методики

продуктов, ДПАК и систем, созданных на основе методики Конструктивной Безопасности	Конструктивной Безопасности, архитектур безопасности и гарантий целостности на основе криптографических методов
3. Конструктивная Безопасность и разработка безопасного программного обеспечения (далее – РБПО)	Развитие передовой отечественной методики проектирования и создания новой критической и информационной инфраструктуры с учетом рисков и угроз, оценки технологических рисков устойчивого функционирования и безопасной разработки
4. Архитектура Безопасности и Доверия	Архитектурные решения и средства защиты информации, позволяющие создавать доверенные информационные системы из элементов с разным уровнем доверия
5. Обеспечение гарантий целостности криптографическими методами	Архитектурные решения и отечественные средства цифровой криптографии, позволяющие гарантировать целостность жизненного цикла информационных систем
6. Доверенные аппаратные средства, ЭКБ и процессорные архитектуры	Защищенные процессорные архитектуры, ЭКБ для обеспечения гарантий безопасности и доверия, методики построения доверенных и защищенных аппаратных систем, вычислительной техники, телеком-оборудования и АСУТП

6.2.Совершенствование системы образования для обеспечения перспективных кадровых потребностей динамично развивающихся компаний, научных и творческих коллективов, участвующих в создании новых глобальных рынков

Основные направления плана мероприятий («дорожной карты»)	Краткое описание направления плана мероприятий («дорожной карты»)
Академические центры компетенции по Конструктивной Безопасности и безопасному жизненному циклу	Создание Центров Компетенции на базе: 1. ИСП РАН. 2. Академических центров. 3. Отраслевых центров.
Передовая инженерная школа (далее – ПИШ) по Конструктивной Безопасности и безопасному жизненному циклу	Создание ПИШ по Конструктивной Безопасности (СпБПУ)
Высшие учебные заведения с программами по Конструктивной Безопасности и безопасному жизненному циклу	Формирование образовательных программ: МГУ имени М.В. Ломоносова, МГТУ им. Н.Э. Баумана, НИЯУ МИФИ, МФТИ, ТУСУР и др.

6.3.Развитие системы профессиональных сообществ и популяризация Национальной технологической инициативы

Название направления плана мероприятий («дорожной карты»)	Краткое описание направления плана мероприятий («дорожной карты»)
Формирование профессионального сообщества в области Конструктивной Безопасности	Формирование профессионального сообщества, системы лучших практик, нормативно-правовых актов и стандартов, реализующих преимущества Конструктивной Безопасности

Создание системы стандартов Конструктивной Безопасности	Формирование предложений по системе стандартов в области сквозных технологий доверия и безопасности: Конструктивной Безопасности, Безопасного Жизненного Цикла, Архитектур на основе Политик Безопасности, безопасных процессорных архитектур и др.
Популяризация НТИ и «дорожной карты» «Сейфнет»	Популяризация «дорожной карты» «Сейфнет». Построение совместных планов с другими рабочими группами по реализации «дорожных карт» НТИ. Формирование планов по выводу Конструктивной Безопасности на дружественные зарубежные рынки

6.4. Организационно-техническая и экспертно-аналитическая поддержка, информационное обеспечение Национальной технологической инициативы

Название направления плана мероприятий («дорожной карты»)	Краткое описание направления плана мероприятий («дорожной карты»)
Организационно-техническая и экспертно-аналитическая поддержка, информационное обеспечение	Сквозное мероприятие для всех направлений «дорожной карты». Взаимодействие с другими рабочими группами по реализации «дорожных карт» НТИ и экспертным сообществом НТИ
Создание Инфраструктурного центра (далее – ИЦ) «Сейфнет» НТИ	Проведение экспертно-аналитических мероприятий на базе Инфраструктурного центра «Сейфнет» НТИ

6.5.Создание механизмов акселерации компаний Национальной технологической инициативы и механизмов экспортного продвижения создаваемых продуктов

Название направления плана мероприятий («дорожной карты»)	Краткое описание направления плана мероприятий («дорожной карты»)
Акселерация проектов	Мероприятия по акселерации перспективных проектов и технологий для всех направлений «дорожной карты» Мероприятия по развитию кооперации с центрами компетенций (далее - ЦК), ИЦ, направленных, в том числе, на поддержку патентования

7. Оценка рисков, а также технологических, рыночных и общественных барьеров, препятствующих реализации плана мероприятий («дорожной карты»), и сведения об инструментах их минимизации и преодоления

7.1.Технологические риски

- Отсутствие необходимой технологической базы промышленности;

- Ограниченные возможности отечественной радиоэлектронной промышленности;
- Отсутствие объективных систем контроля защищенности инфраструктуры КИИ;
- Высокая наукоемкость отдельных направлений развития.

7.2.Санкционные риски

К санкционным рискам относится отсутствие доступа к технологической базе.

7.3.Нормативные риски

- Отсутствие стандарта Конструктивной Безопасности;
- Отсутствие отраслевых стандартов доверия и безопасности;
- Отсутствие сквозных требований конструктивной безопасности;
- Фрагментированность нормативной базы.

7.4.Макроэкономические риски

- Ограниченная возможность заказчиков инвестировать в развитие безопасности инфраструктуры;
- Отсутствие стимулов потребления доверенных и безопасных решений;
- Отсутствие целевых мер поддержки для разработки и внедрения защищенных продуктов.

7.5.Прочие риски

- Отсутствие или ограничение компетенций в ряде областей;
- Риск нехватки профессиональных кадров;
- Зависимость от зарубежных стандартов и инструментов.

III. План реализации мероприятий («дорожной карты»)

1. План-фактный анализ выполнения плана мероприятий («дорожной карты») за прошедший период

Заполняется при актуализации плана мероприятий («дорожной карты») НТИ по прошествии периода исполнения.

2. Перечень целевых показателей плана мероприятий («дорожной карты»), их значений и методика их расчета

Наименование целевых показателей	Единица измерения	Текущее значение	2026-2030	2030-2035	2035-2040
1. Объем реализации решений на основе Конструктивной Безопасности	Млрд руб./год	1	1-25	25-50	50-100
2. Уровень уязвимости продуктов, созданных на основе Конструктивной Безопасности	Максимальный уровень уязвимости продуктов, созданных на основе КБ по методике оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утверждена ФСТЭК России 30 июня 2025 г.)	7	5	3	1
3. Уровень технологической готовности Конструктивной Безопасности	УГТ по ГОСТ Р71726-2024	1	2-8	9	9
4. Уровень технической готовности Архитектур Безопасности	УГТ по ГОСТ Р71726-2024	1	2-8	9	9
5. Уровень технической готовности Гарантий Целостности на основе криптографических методов	УГТ по ГОСТ Р71726-2024	5	5-9	9	9
6.Научные исследования в области Конструктивной Безопасности	Количество академических и исследовательских центров	1	1-5	5-10	10-25
7. Подготовка кадров в области Конструктивной Безопасности	Количество образовательных центров	1	3-5	7-10	10+
8. Экосистема Конструктивной Безопасности	Количество компаний участников	1	5-50	50-100	100-500
9. Профессиональное сообщество Конструктивной Безопасности	Количество специалистов	100	100-1000	1000-10000	10000-25000

3. Плановый график реализации плана мероприятий («дорожной карты»)

3.1.Создание, развитие и продвижение передовых технологий, продуктов и услуг, обеспечивающих приоритетные позиции российских компаний на формируемых глобальных рынках

Основные направления плана мероприятий («дорожной карты»)	Срок начала реализации	Срок окончания реализации	Значимые контрольные результаты реализации плана мероприятий («дорожной карты»)	Ожидаемый результат	Исполнители
1.1 Целевые рынки применения сквозных технологий доверия и безопасности	2026	2030	Выведены на рынок новые типы устройств, содержащие в своем составе средства управления, вычислений и связи, способные надежно выполнять свои функции в условиях растущих угроз информационной и кибербезопасности	Выведены на рынок новые типы услуг, осуществляемые с помощью централизованных систем, имеющих в своем составе автономные, интеллектуальные, территориально распределенные устройства	АНО «Платформа НТИ». Фонд НТИ, Минцифры России, Минпромторг России, Минобрнауки России
1.1.1 Определение понятия Критической Инфраструктуры (НИР)	2026	2027	Проведен анализ лучших мировых практик (из открытых источников) и нормативного ландшафта. Сформированы предложения по определению и глоссарию критической инфраструктуры. Определены основные свойства и характеристики критической инфраструктуры. Проведен анализ нормативно-правовой базы, включая анализ действующего законодательства в РФ и других стран. Проведен форсайт с регуляторами, заказчиками и компаниями – лидерами отрасли.	Предложено определение критической инфраструктуры Сформированы предложения по составу глоссария, определению основных свойств Предложен проект предварительного национального стандарта (далее – ПНСТ)	АНО «Платформа НТИ», Фонд НТИ

1.1.2 Анализ и оценка целевых рынков сквозных технологий доверия и безопасности (НИР)	2026	2027	Определены целевые рынки сквозных технологий доверия и безопасности, а именно рынки: - беспилотных систем, в том числе летательных и наземных; - беспилотных космических и спутниковых систем; - средств видеонаблюдения, контроля доступа и физической защиты; - средств связи, телекоммуникаций и цифровых сервисов; - интеллектуальных автоматизированных транспортных систем и инфраструктуры; - интеллектуальных автоматизированных систем в промышленности и энергетике. Представлена оценка объемов целевых рынков (в рублях и единицах), определена сегментация. Определены возможные сценарии технологического развития, включая: новые методы и архитектуры, развитие технологического суверенитета, развитие прорывных технологий (доверенный ИИ), стандартов и НПА. Проведен форсайт с регуляторами, заказчиками и компаниями – лидерами отрасли. Предоставлен отчет, публикации.	Определены перспективные целевые рынки (Топ-10) сквозных технологий доверия и безопасности. Представлена оценка объемов рынка в млрд руб. и ед/шт, сегментация и сценарии развития. Представлены рекомендации по целевым показателям развития: - новых методов и архитектур; - технологического суверенитета; - прорывных технологий (ИИ); - стандартов и НПА. Предложен проект ПНСТ	АНО «Платформа НТИ». Фонд НТИ, Минпромторг России, Минцифры России
1.1.3 Анализ ландшафта и прогноз развития рисков и угроз устойчивому функционированию КИИ (НИР)	2026	2027	Проведен анализ (из открытых источников) ландшафта рисков и угроз устойчивому функционированию КИИ Проведена оценка потенциального ущерба, связанного с технологическими рисками и угрозами устойчивого функционирования. Проведено исследование лучших практик, архитектуры и методики построения, требований безопасности: - беспилотных систем; - беспилотных космических и спутниковых систем; - средств видеонаблюдения, контроля доступа и физической защиты; - средств связи, телекоммуникаций и цифровых сервисов; - интеллектуальных автоматизированных транспортных систем и инфраструктуры;	Проведена оценка рисков и угроз устойчивому функционированию КИИ. Представлены рекомендации по применению методов Конструктивной Безопасности, архитектуры безопасности, обеспечения гарантий целостности криптографическими методами и создания доверенных аппаратных средств. Предложен проект ПНСТ	АНО «Платформа НТИ», Фонд НТИ Минпромторг России, Минцифры России

			- интеллектуальных автоматизированных систем в промышленности и энергетике. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли Предоставлен отчет, публикации.		
1.1.4 Исследование рисков и угроз устойчивому функционированию КИИ (НИР)	2026	2027	Проведено исследование и оценка рисков и угроз устойчивого функционирования систем, оценка потенциального ущерба в зависимости от сценария. Проведено исследование основных известных и потенциальных уязвимостей. Проведен анализ рисков и угроз кибербезопасности: идентифицированы основные угрозы кибербезопасности, оценены их вероятность и потенциальные последствия. Проведено исследование и анализ потенциальных сценариев кибератак, мотивации и профиля нарушителей. Определены сценарии развития киберугроз на основе новых технологий (ИИ). Сформированы предложения по отраслевым моделям угроз с учетом новых угроз, включая ИИ. Проведен анализ существующего оборудования, попадающего в категорию элементов обеспечения кибербезопасности. Определена концепция обеспечения доверия и безопасности. Проведен анализ нормативно-правовой базы, включая действующее законодательство в России и других странах. Проведен анализ технических стандартов. Определены приоритетные области стандартизации. Разработан план стандартизации. Составлена дорожная карта реализации плана стандартизации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Определена модель рисков и угроз для ключевых отраслей (покрытие до 80 % известных угроз), определен состав потенциальных уязвимостей, сценарии развития рисков и угроз, определена модель нарушителя (5+ категорий). Сформулированы рекомендации и требования к модели угроз с учетом применения ИИ. Сформулирована концептуальная структура системы обеспечения безопасности и доверия. Сформулированы требования к сквозным технологиям и системам доверия и безопасности. Определен перечень требований к технологиям и элементам обеспечения доверия и безопасности, снижающая возможный ущерб от известных уязвимостей на 80 %. Предложен проект ПНСТ	Минпромторг России, Минцифры России

1.1.5 Анализ лучших практик, архитектуры безопасности и обеспечения доверия беспилотных систем (НИР)	2026	2027	Проведен анализ международного опыта (из открытых источников) и лучших практик построения подсистем обеспечения доверия и безопасности беспилотных систем. Определен типовой состав экосистемы, архитектура построения систем управления и жизнеобеспечения беспилотных средств. Проведен анализ применимости методики Конструктивной Безопасности, архитектуры безопасности и доверия, а также обеспечения гарантий целостности криптографическими методами. Определен состав систем и элементов обеспечения доверия и безопасности. Определен задел российских компаний. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Определен технологический ландшафт, прогноз и сценарии развития, типовая архитектура, состав функции обеспечения доверия и безопасности беспилотных систем. Сформировано задание на исследование перспективных методик, архитектурных принципов безопасности и обеспечения доверия беспилотных систем (1.1.6)	АНО «Платформа НТИ», Фонд НТИ Минпромторг России, Минцифры России
1.1.6 Исследование перспективных методик, архитектурных принципов безопасности и обеспечения доверия беспилотных систем (Линейный НИР)	2026	2027	Определена концепция обеспечения доверия и безопасности беспилотных средств. Проведено исследование основных уязвимостей. Проведено исследование и оценка рисков и угроз, прогноз потенциального ущерба в зависимости от сценария. Проведен анализ рисков и угроз кибербезопасности: идентифицированы основные угрозы кибербезопасности, оценены их вероятность и потенциальные последствия Проведено исследование и анализ потенциальных сценариев кибератак, мотивации и профиля нарушителей Определены сценарии развития киберугроз на основе новых технологий (ИИ) Проведен анализ существующего оборудования, попадающего в категорию элементов обеспечения кибербезопасности Проведен анализ нормативно-правовой базы, включая действующее законодательство в России и других странах. Проведен анализ технических стандартов. Определены приоритетные области стандартизации. Разработан план	Определена модель рисков и угроз экосистемы беспилотных средств (покрытие до 80% известных угроз), определен ландшафт угроз, определена модель нарушителя (5+ категорий). Определен перечень требований к технологиям и элементам обеспечения доверия и безопасности, снижающая возможный ущерб от известных уязвимостей на 80%. Сформулирована концептуальная структура системы обеспечения безопасности и доверия. Определены области работы по плану стандартизации в части технического регулирования и области нормативно-технических	АНО «Платформа НТИ», Фонд НТИ Минпромторг России, Минцифры России

			стандартизации. Составлена дорожная карта реализации плана стандартизации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли Предоставлен отчет, публикации.	документов в части информационной и кибербезопасности. Предложен проект ПНСТ	
1.1.7 Разработка архитектуры безопасности экосистемы высокоавтоматизированного и беспилотного движения (далее – ЭВиБД) (НИР)	2026	2027	Проведен анализ международного опыта (статей и выступлений на конференции) Определена концепция кибербезопасности экосистемы подключенного высокоавтоматизированного и беспилотного движения. Проведено исследование основных уязвимостей элементов ЭВиБД. Проведено исследование и оценка рисков и угроз, прогноз потенциального ущерба в зависимости от сценария. Построена модель рисков и угроз экосистемы подключенного высокоавтоматизированного и беспилотного движения. Проведено исследование и анализ потенциальных сценариев кибератак, мотивации и профиля нарушителей. Построена модель нарушителя экосистемы подключенного высокоавтоматизированного и беспилотного движения. Проведен анализ рисков и угроз кибербезопасности: идентифицированы основные угрозы кибербезопасности для беспилотного транспорта, оценены их вероятность и потенциальные последствия (на основе НИР). Определено общее видение будущего развития киберугроз экосистемы для агентов отношения экосистемы беспилотного и высокоавтоматизированного движения и определение тенденций в области обеспечения кибербезопасности. Проведен анализ существующего оборудования, попадающего в категорию элементов обеспечения кибербезопаности. Проведен анализ аналогов и недостающих элементов, определены требования к ним. Проведен анализ нормативно-правовой базы, включая действующее законодательство в России и других странах,	Сформулирована концептуальная структура ЭВиБД с перечнем требований к банку стандартных элементов системы. Определена модель рисков и угроз экосистемы (покрытие до 40% известных угроз), определен ландшафт угроз, определена модель нарушителя ЭВиБД (5+ категорий). Сформированы требования к системе кибербезопасности, обеспечивающей снижение времени реагирования на угрозы на 20-30%, а также снижение издержек сервисов ВАТС по причине киберуязвимостей до 25%. Определен перечень требований к Технологическому центру Кибербезопасности и его функционал. Определены области работы по плану стандартизации в части технического регулирования и области нормативно-технических документов в части инфо-кибербезопасности подключенного высокоавтоматизированного и беспилотного движения. Предложен проект ПНСТ	АНО «Платформа НТИ», Фонд НТИ Минпромторг России, Минцифры России,

			регулирующее вопросы безопасности дорожного движения, информационной безопасности и беспилотного транспорта. Проведен анализ технических стандартов: изучены существующие международные и национальные стандарты в области автомобилестроения, информационной безопасности и связи, применимые к беспилотному транспорту. Определены приоритетные области стандартизации. Разработан план стандартизации. Составлена дорожная карта реализации плана стандартизации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.		
1.1.8 Разработка архитектуры безопасности защищенной АСУТП (НИР)	2026	2027	Проведен анализ международного опыта (статей и выступлений на конференции). Проведено исследование основных уязвимостей элементов АСУТП. Проведено исследование и оценка современных рисков и угроз, прогноз потенциального ущерба в зависимости от сценария. Построена модель рисков и угроз экосистемы АСУТП. Проведено исследование и анализ потенциальных сценариев кибератак, мотивации и профиля нарушителей. Сформирован прогноз развития рисков и угроз кибербезопасности: идентифицированы основные угрозы кибербезопасности для АСУТП, в том числе- связанных с использованием ИИ и внутреннего нарушителя в качестве инструмента реализации целевых атак. Оценены их вероятность и потенциальные последствия (на основе НИР), определены основные тенденции в области обеспечения кибербезопасности. Проведен анализ существующего оборудования, попадающего в категорию элементов обеспечения кибербезопасности. Проведен анализ аналогов и недостающих элементов, определены требования к ним.	Определена модель рисков и угроз экосистемы (покрытие до 80 % известных угроз), определен ландшафт угроз, определена модель нарушителя (5+ категорий). Представлены рекомендации по нейтрализации уязвимостей, связанных с недокументированными возможностями (далее - НДВ) используемых недоверенных элементов. Сформированы рекомендации по противодействию новым высокотехнологическим угрозам, в первую очередь – с использованием ИИ. Разработаны архитектурные решения и рекомендации по использованию отечественных доверенных аппаратных средств,	Минпромторг России, Минцифры России

			Проведен анализ нормативно-правовой базы, включая действующее законодательство в России и других странах. Проведен анализ технических стандартов: изучены существующие международные и национальные стандарты в области безопасности и технологической устойчивости АСУТП. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли Предоставлен отчет, публикации.	отечественной ЭКБ и элементов доверия и безопасности. Сформированы предложения по увеличению технологической устойчивости АСУТП к технологическим рискам и угрозам. Определены приоритетные области стандартизации. Предложен проект ПНСТ	
1.1.9 Разработка архитектуры безопасности систем физической защиты, видеонаблюдения и системы контроля и управления доступом (далее – СКУД) (НИР)	2026	2027	Проведен анализ международного опыта (статей и выступлений на конференции) Проведено исследование основных уязвимостей элементов систем физической безопасности. Проведено исследование и оценка современных рисков и угроз, прогноз потенциального ущерба в зависимости от сценария. Построена модель рисков и угроз экосистемы физической безопасности. Проведено исследование и анализ потенциальных сценариев кибератак, мотивации и профиля нарушителей Сформирован прогноз развития рисков и угроз кибербезопасности: идентифицированы основные угрозы кибербезопасности для систем физической безопасности, в том числе- связанных с использованием ИИ и внутреннего нарушителя в качестве инструмента реализации целевых атак. Оценены их вероятность и потенциальные последствия (на основе НИР), определены основные тенденции в области обеспечения кибербезопасности. Проведен анализ существующего оборудования, попадающего в категорию элементов обеспечения кибербезопасности. Проведен анализ аналогов и недостающих элементов, определены требования к ним. Проведен анализ нормативно-правовой базы, включая действующее законодательство в России и других странах.	Определена модель рисков и угроз экосистемы (покрытие до 80 % известных угроз), определен ландшафт угроз, определена модель нарушителя (5+ категорий). Представлены рекомендации по нейтрализации уязвимостей, связанных с НДВ используемых недоверенных элементов. Сформированы рекомендации по противодействию новым высокотехнологическим угрозам, в первую очередь – с использованием ИИ. Разработаны архитектурные решения и рекомендации по использованию отечественных доверенных аппаратных средств, отечественной ЭКБ и элементов доверия и безопасности. Сформированы предложения по увеличению технологической устойчивости систем физической	Минпромторг России, Минцифры России

			Проведен анализ технических стандартов, включая существующие международные и национальные стандарты в области безопасности и технологической устойчивости систем физической безопасности. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли Предоставлен отчет, публикации.	безопасности к технологическим рискам и угрозам. Определены приоритетные области стандартизации. Предложен проект ПНСТ	
1.1.10 Прототипы и пилотные проекты (НИР)	2027	2030	Определен состав якорных и пилотных заказчиков, систем и применений. Разработано техническое задание (далее – ТЗ) на прототипы защищенных: - беспилотных систем; - беспилотных космических и спутниковых систем; - средств видеонаблюдения, контроля доступа и физической защиты; - средств связи, телекоммуникаций и цифровых сервисов; - интеллектуальных автоматизированных транспортных систем и инфраструктуры; - интеллектуальных автоматизированных систем в промышленности и энергетике. Разработано ТЗ с учетом моделей угроз, известных уязвимостей и модели технологических рисков устойчивого функционирования. Разработаны прототипы с применением методов Конструктивной Безопасности, на основе анализа требований и безопасной разработки, имеющие в своем составе аппаратно-программные подсистемы доверия и безопасности. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Представлен отчет и работающие прототипы.	Созданы прототипы интеллектуальных автономных систем, обладающих устойчивостью к известным рискам и угрозам (покрытие до 80% известных угроз) и моделям нарушителя (5+ категорий).	Минпромторг России, Минцифры России, АНО «Платформа НТИ», Фонд НТИ
1.1.11 Тестирование, испытания продуктов, содержащих	2027	2029	Определен состав якорных и пилотных полигонов для испытания: - беспилотных систем; - беспилотных космических и спутниковых систем;	Проведено тестирование прототипов систем, продуктов, элементов и технологий: - беспилотных систем;	Минпромторг России, Минцифры России, АНО «Платформа

сквозных технологий доверия и безопасности (НИР)			- средств видеонаблюдения, контроля доступа и физической защиты; - средств связи, телекоммуникаций и цифровых сервисов; - интеллектуальных автоматизированных транспортных систем и инфраструктуры; - интеллектуальных автоматизированных систем в промышленности и энергетике. Сформулировано ТЗ и программа и методика испытаний (далее – ПМИ) на основе анализа требований регуляторов и заказчиков, требований технологической безопасности и устойчивого функционирования систем. Проведена валидация и верификация всех систем, подсистем и элементов на предмет устойчивости к известным типам рисков, угроз и уязвимостей.	- беспилотных космических и спутниковых систем; - средств видеонаблюдения, контроля доступа и физической защиты; - средств связи, телекоммуникаций и цифровых сервисов; - интеллектуальных автоматизированных транспортных систем и инфраструктуры; - интеллектуальных автоматизированных систем в промышленности и энергетике.	НТИ», Фонд НТИ
1.1.12 Внедрение сквозных технологий доверия и безопасности	2028	2030	Определен состав якорных и пилотных заказчиков для внедрения: - беспилотных систем; - беспилотных космических и спутниковых систем; - средств видеонаблюдения, контроля доступа и физической защиты; - средств связи, телекоммуникаций и цифровых сервисов; - интеллектуальных автоматизированных транспортных систем и инфраструктуры; - интеллектуальных автоматизированных систем в промышленности и энергетике.	Определен состав якорных и пилотных заказчиков для внедрения Определены принципы и приоритеты внедрения Предложены рекомендации к НПА	Минпромторг России, Минцифры России, АНО «Платформа НТИ», Фонд НТИ

1.2 Конструктивная Безопасность	2026	2030	Разработка передовой методики создания доверенных систем с использованием доверенных и недоверенных модулей и подсистем с целью повышения надежности и устойчивости функционирования в условиях растущих угроз информационной и кибербезопасности	Архитектура и методика создания КИИ, обладающих повышенной устойчивостью к современным и перспективным угрозам информационной и кибербезопасности	Исполнители
1.2.1 Анализ лучших практик построения систем на основе методики Secure by Design (НИР)	2026	2027	Проведена оценка лучших практик и методов создания систем с конструктивной информационной безопасностью. Проведено исследование отечественных и международных требований и лучших практик обеспечения конструктивной безопасности: ИС, информационно-телекоммуникационные сети (далее – ИТКС) и АСУТП, программного обеспечения, ДПАК и РЭА, ЭКБ и модулей. Сформированы выводы применительно к подходам, методам и моделям, сценарии и рекомендации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Определен ландшафт – лучшие практики, существующий задел, требования международных стандартов. Сформировано задание на исследование и разработку принципов, архитектуры и методов Конструктивной Безопасности (1.2.2). Сформировано задание на исследование и разработку методики оценки и снижения технологических рисков и угроз устойчивого функционирования технологий, продуктов и систем (1.2.3).	АНО «Платформа НТИ», Фонд НТИ Минцифры России, Минпромторг России
1.2.2 Разработка принципов, архитектуры и методов Конструктивной Безопасности (НИР)	2026	2027	Проведено сопоставление, анализ и унификация требований международных стандартов в области информационной безопасности и защиты информации с требованиями методологии создания систем с конструктивной информационной безопасностью. Сформированы требования к междисциплинарному анализу при создании сложных систем и сетей для обеспечения создания и достижения целей информационной безопасности в процессах создания систем с конструктивной информационной безопасности.	Сформирован концептуальный и технический облик систем на основе конструктивной безопасности. Разработаны методические основы, подходы и модели построения систем с конструктивной безопасностью. Сформированы требования к методам разработки и инструментам, позволяющих на этапе проектирования и разработки	Минцифры России, Минпромторг России

			Проведена оценка моделей разграничения доступа, применяемых для обеспечения функциональной и информационной безопасности, и обобщение их в терминах архитектуры систем. Проведено исследование принципов и подходов к верификации и валидации архитектурных и проектных решений в создании систем с конструктивной информационной безопасностью. Сформированы подходы, методы и модели верификации и валидации архитектурных и проектных решений. Проведено исследование возможности применения методов безопасной разработки ПО при создании систем с конструктивной информационной безопасностью. Сформированы требования к процессам управления разработкой в организации для реализации методов конструктивной информационной безопасности. Сформированы требования к взаимодействию заинтересованных сторон при разработке для реализации методов конструктивной информационной безопасности. Сформированы подходы, методы и модели. Разработаны архитектурные рекомендации, модели и методы оценки устойчивости к рискам и угрозам. Разработаны модели, методы и рекомендации по повышению устойчивости к рискам и угрозам. Разработаны модели оценки соответствия нормативным актам государственных регуляторов. Разработаны требования к средствам моделирования, прототипирования и разработки, аналитическим и программным продуктам. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	обеспечить покрытие 80 % известных киберугроз. Разработаны архитектурные рекомендации, модели и инструменты оценки и повышения устойчивости к рискам и угрозам. Разработаны аван-проекты национальных стандартов внедрения технологий и процессов конструктивной безопасности. Предложен проект ПНСТ	
1.2.3 Разработка принципов,	2026	2027	Проведена оценка применимости методов конструктивной безопасности к безопасному жизненному циклу.	Сформирована интегрированная концептуальная база технологий	Минпромторг России

архитектуры и методов применения Конструктивной Безопасности к РБПО (НИР)			Проведено исследование возможности применения моделей разграничения доступа, применяемых для обеспечения функциональной и информационной безопасности, и обобщение их в терминах архитектуры систем. Проведено исследование возможности применения принципов и подходов к верификации и валидации архитектурных и проектных решений в создании систем. Представлен анализ моделей разграничения доступа, применяемых для обеспечения функциональной и информационной безопасности, и обобщение их в терминах архитектуры систем. Представлен анализ и описание принципов и подходов к верификации и валидации архитектурных и проектных решений в создании систем с конструктивной информационной безопасностью. Представлен анализ методов РБПО в создании систем с конструктивной информационной безопасности. Разработаны принципы и методы применения конструктивной безопасности к безопасному жизненному циклу, включая: - модели разграничения доступа, применяемых для обеспечения функциональной и информационной безопасности, и обобщение их в терминах архитектуры систем; - принципы и подходов к верификации и валидации архитектурных и проектных решений в создании и эволюционном развитии систем; - модели разграничения доступа, применяемых для обеспечения функциональной и информационной безопасности, и обобщение их в терминах архитектурных моделей программных и программно-аппаратных систем. Сформированы требования к процессам управления разработкой в организации для реализации методов конструктивной информационной безопасности.	конструктивной безопасности и жизненного цикла РБПО. Разработаны методические основы для внедрения принципов конструктивной безопасности и технологий жизненного цикла. РБПО в процессы разработчиков и поставщиков программных и программно-аппаратных комплексов КИИ. Разработаны аван-проекты проектов национальных стандартов внедрения технологий и процессов конструктивной безопасности и РБПО. Разработаны методы, модели рекомендации и требования по созданию инструментов РБПО на основе конструктивной безопасности, позволяющих обеспечить покрытие 80 % известных угроз на этапе проектирования и разработки. Сформированы предложения к ПНСТ.	Минцифры России

			Сформированы требования к взаимодействию заинтересованных сторон при разработке для реализации методов конструктивной информационной безопасности. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.		
1.2.4 Реализация принципов безопасной разработки для различных уровней КИИ (НИР)	2026	2028	Разработаны модели рисков и угроз, требований к безопасной разработке, средств и методик статического и динамического анализа, валидации и верификации: - автоматизированных информационных систем; - программного обеспечения; - доверенных программно-аппаратных комплексов; - радиоэлектронной аппаратуры; - электронной компонентной базы. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Разработаны единые подходы, методики и модели реализации безопасной разработки для различных уровней КИИ: ПО, ДПАК, РЭА и ЭКБ. Разработана модель рисков и угроз, требований, средств и методик статического и динамического анализа, валидации и верификации. Сформированы предложения к ПНСТ.	Минцифры России, Минобрнауки России
1.2.5 Разработка перспективных методов и инструментов проектирования безопасных систем (НИОКР)	2026	2028	Проведена разработка методов и инструментов моделирования программных систем и программно-аппаратных комплексов. Проведена разработка методов и инструментов исследования поверхности атак. Проведена разработка методов и разработка доверенных компиляторов. Проведена разработка методов и инструментов обфускации программ. Проведена разработка автоматического анализатора приложений на предмет уязвимостей, базирующийся на искусственном интеллекте. Проведена разработка средств интеграции традиционных языков (C/C++) с языками с безопасной работой с памятью (memory-safe languages) для повышения уровня безопасности гетерогенных (многоязыковых) программных комплексов.	Повышен уровень развития перспективных методов и инструментов моделирования, проектирования и разработки доверенных, безопасных и защищенных систем. Разработаны научно-технические и технологические основы перспективных средств проектирования, разработки, анализа и сопровождения ПО КИИ на основе новейших достижений науки и техники, включая ИИ. Разработаны 2 инструмента моделирования (уровень технологической готовности (далее – УТГ) 4-5).	Минпромторг России Минцифры России

			Проведена разработка декомпилятора кода на основе ИИ, позволяющий в том числе восстановить виртуализированный и обфусцированный код. Проведена разработка методов и средств поддержки непрерывной разработки и интеграции программных решений (CI/CD). Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли Предоставлен отчет, публикации.	Разработаны методы и инструменты исследования поверхности атак (5+2 языков программирования, 3+1 ОС). Разработаны доверенные компиляторы для 2+2 языков программирования (УТГ5). Разработан 1 декопилятор на основе ДИИ. Сформированы предложения к ПНСТ.	
1.2.6 Разработка методов и инструментов анализа, валидации и верификации ПО (НИОКР)	2026	2028	Разработаны методы и инструменты анализа, валидации и тестирования. Разработаны статические анализаторы для JavaScript, Python, Go, Rust и других языков программирования. Разработаны специализированные API (Программные Интерфейсы Приложений) для реализации средств статического анализа, в том числе язык запросов и средств детекторов. Разработаны методы и инструменты динамического анализа. Разработаны инструментальные платформы поддержки динамического анализа. Разработаны средства распределенного статического и динамического анализа для исследования сверхкрупных программных систем (объекты КИИ). Разработана среда создания моделей управления доступом для различных языков моделирования. Разработаны средства формальной верификации моделей управления доступом при помощи дедуктивной верификации и model checking. Разработаны средства избирательной и сквозной верификации. Разработаны средства динамической верификации средств защиты информации (далее – СЗИ) и тестирования СЗИ на основе формальных моделей.	Разработаны прототипы и продукты индустриального уровня, реализующие методы анализа, валидации и тестирования. Разработаны научно-технические и технологические основы для внедрения приоритетных средств проектирования, разработки, анализа и сопровождения ПО КИИ. Разработаны методы и инструменты анализа, валидации и тестирования, позволяющие реализовать защиту от 80% известных угроз. Разработаны методы бесшовной интеграции различных технологий формальной верификации для программных стеков на C/Python. Разработаны методы и инструменты формальной верификации, позволяющие обеспечить гарантию соответствия критических компонентов требованиям доверия и безопасности.	Минцифры России Минпромторг России

			Разработаны средства моделирования и верификации телекоммуникационных и криптографических протоколов. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Сформированы предложения к ПНСТ.	
1.2.7 Разработка методов, стандартов и прототипов инструментов выявления и оценки уязвимостей ДПАК (НИР)	2026	2027	Проведен анализ лучших мировых практик выявления уязвимостей в программно-аппаратных комплексах, содержащих недоверенные элементы, потенциально содержащие НДВ	Разработаны рекомендации и требования к методикам и инструментам выявления и оценки уязвимостей Сформированы предложения к ПНСТ.	Минпромторг России Минцифры России
1.2.8 Применение ИИ для безопасной разработки (НИР)	2026	2027	Проведено исследование лучших практик и методик применения доверенного ИИ в безопасной разработке для различных уровней КИИ – автоматизированных информационных системах, ПО, ДПАК, РЭА и ЭКБ. Проведено исследование лучших практик и методик, сформированы рекомендации и требования по применению ИИ в области статического анализа. Проведено исследование лучших практик и методик, сформированы рекомендации и требования по применению ИИ в задачах динамического анализа. Проведено исследование лучших практик и методик, сформированы рекомендации и требования по применению ИИ в задачах верификации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Проведено исследование лучших практик и методик применения доверенного ИИ в безопасном жизненном цикле для различных уровней КИИ, в области статического и динамического анализа, а также в задачах верификации. Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России
1.2.9 Разработка методики	2026	2027	Исследованы лучшие зарубежные и отечественные практики, модели и методики комплексной оценки устойчивости функционирования субъектов КИИ, объектов	Разработана модель оценки технологических рисков устойчивого функционирования	Минпромторг России,

оценки и снижения технологических рисков и угроз устойчивого функционирования технологий, продуктов и систем (НИР)			КИИ, ПО, ДПАК, РЭА, модулей и ЭКБ. Разработаны модели технологической безопасности и методики комплексной оценки устойчивости функционирования. Проведен анализ зарубежных источников, форсайт с регуляторами, основными заказчиками и лидерами рынка, определены лучшие практики, методики и модели оценки устойчивости функционирования технологий, продуктов и систем, связанных с: - подконтрольностью технологий, продуктов и систем; - информационной и кибербезопасностью технологий, продуктов и систем; - безопасностью жизненного цикла технологий, продуктов и систем; - функциональной надежностью технологий, продуктов и систем. Исследованы возможности снижения рисков и угроз нарушения технологической устойчивости функционирования КИИ, связанных с подконтрольностью, информационной и кибербезопасностью, безопасностью жизненного цикла и функциональной надежностью технологий, продуктов и систем. Разработаны методы снижения рисков и угроз с применением сквозных технологий доверия и безопасности. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	технологий, продуктов и систем, используемых при реализации объектов КИИ. Разработана методика снижения технологических рисков и угроз устойчивого функционирования объектов КИИ. Представлены предложения по организации независимой экспертной оценки, аудиту, контролю и надзору за параметрами устойчивости функционирования технологий, продуктов и систем, используемых при реализации объектов КИИ. Сформированы предложения к ПНСТ	Минцифры России

1.2.10 Создание инженерных подходов для повышения уровня устойчивости функционирования и технологической безопасности КИИ (НИР)	2027	2028	Исследованы лучшие мировые практики. Сформирован реестр рисков и угроз устойчивого функционирования и технологической безопасности КИИ. Разработаны требования технологической безопасности и устойчивости КИИ. Разработаны рекомендации по архитектурным и технологическим решениям, технологической безопасности, функциональной надежности, безопасному жизненному циклу, средствам обеспечения доверия и безопасности, средствам защиты информации, в т. ч. криптографическим для объектов КИИ, их компонент, элементов, модулей и технологий с целью усиления технологической безопасности и устойчивости КИИ. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Сформирован облик отечественных и международных требований и лучших практик обеспечения конструктивной безопасности. Сформированы инженерные подходы для повышения уровня устойчивости функционирования и технологической безопасности КИИ путем формирования реестра рисков и угроз, разработки требований технологической безопасности и устойчивости. Разработаны архитектуры, модели и инструменты оценки и повышения устойчивости к рискам и угрозам. Разработаны рекомендации для усиления технологической безопасности и устойчивости объектов КИИ, их компонент, элементов, модулей и применяемых технологий. Представлен ПНСТ.	Минпромторг России
1.2.11 Анализ лучших практик автоматизированной работы с требованиями и рисками (НИР)	2026	2027	Проведено исследование лучших зарубежных и отечественных практик, автоматизированной работы с требованиями и рисками. Проведен анализ возможности применения методов и инструментов на основе доверенного Искусственного Интеллекта для автоматизированной обработки требований и рисков при проектировании сложных инженерных систем. Определены приоритетные направления и типы инженерных систем, для проектирования которых необходима автоматизированная работа с рисками. Проведена оценка вычислительной сложности автоматизированной обработки, количества и сложности требований при проектировании систем.	Сформированы сценарии развития систем и методов автоматизированной работы с требованиями и рисками при построении сложных инженерных систем Сформирован технический облик и требования к перспективным системам автоматизированной работы с требованиями и рисками при построении сложных инженерных систем	АНО «Платформа НТИ», Фонд НТИ Минпромторг России Минобрнауки России

			Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Представлено задание на разработку методов и алгоритмов автоматизированной работы с требованиями и рисками (п. п. 1.2.11, 1.2.12). Представлен ПНСТ.	
1.2.12 Разработка методов и алгоритмов автоматизированной работы с требованиями и рисками (НИР)	2026	2027	Проведено исследование и анализ методов автоматизированной оценки критериев применимости стандартов в проектной деятельности при проектировании объектов КИИ. Проведено исследование и анализ методов автоматизированной выборки (атомизации) и идентификации требований из первоисточников. Проведено исследование и анализ методов автоматизированной формализации требований под заданную модель данных. Проведено исследование и анализ методов автоматизированных классификаций и распределения требований по планируемым к выпуску документам / объектам конфигурации / стадиям ЖЦ. Проведено исследование и анализ методов автоматизированной переработки и верификации требований под типовые синтаксические конструкции. Проведено исследование и анализ методов автоматизированной оценки характеристик (качества) неформализованных требований. Проведено исследование и анализ методов автоматизированной оценки влияния изменения на документацию или соответствующие объекты конфигурации. Проведено исследование и анализ методов оценки целостности комплекта проектной документации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации. Сформированы предложения к ПНСТ.	Разработаны методы и алгоритмы автоматизированной работы с требованиями на основе методов и инструментов Доверенного ИИ. Сформированы рекомендации и требования по созданию автоматизированного комплекса на основе доверенного ИИ, обеспечивающего обработку до 100 тысяч требований в час при обеспечении 80% совпадения результатов классификации с оценками экспертов (инженеров). Сформированы предложения к ПНСТ.	Минпромторг России, Минобрнауки России

1.2.13 Разработка методов и алгоритмов автоматизированной работы с требованиями и рисками значимых объектов КИИ (далее - ЗОКИИ) (НИР)	2026	2028	Разработаны методы автоматизированной разработки, верификации и валидации комплекса требований к тактико-техническим характеристикам (далее – ТТХ) значимых объектов КИИ, обеспечивающих полноту и корректность на этапе разработки. Разработаны технологии автоматизированной разработки, верификации и валидации комплекса требований к ТТХ значимых объектов КИИ, обеспечивающих полноту и корректность на этапе разработки. Проведено исследование возможностей автоматизированного проектирования, моделирования, валидации и верификации архитектуры и проектных решений значимых объектов КИИ. Разработаны технологии и методы автоматизированного проектирования, моделирования, валидации и верификации архитектуры и проектных решений значимых объектов КИИ. Проведен форсайт с регуляторами, заказчиками и компаниями – лидерами рынка. Предоставлен отчет, публикации.	Разработаны методы автоматизированной разработки, верификации и валидации требований и рисков ЗоКИИ. Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России, Минобрнауки России
1.2.14 Анализ лучших практик и методов применения доверенного ИИ и онтологий для работы с требованиями (НИР)	2026	2027	Проведен анализ лучших мировых практик по использованию ИИ при работе с требованиями, опыта разработки и эксплуатации фреймворков машинного обучения и базовых библиотек.	Представлена оценка применимости онтологий в области безопасности, работы с требованиями, безопасного жизненного цикла и безопасности КИИ. Сформировано задание на исследование и разработку методов применения доверенного ИИ и онтологий для работы с требованиями (1.2.14)	Минцифры России

1.2.15 Разработка методов применения доверенного ИИ и онтологий для работы с требованиями (НИР)	2026	2028	Проведен анализ угроз, рисков и моделей возможных атак на программные системы на основе технологий ИИ, работающие с требованиями. Проведен анализ отечественных аппаратных решений для построения доверенных решений на базе технологий ИИ и определены направления работ для оснащения отечественных аппаратных решений полным стеком доверенного ПО, включая средства для работы с генеративными моделями ИИ и с большими языковыми моделями. Разработаны методические рекомендации по применению Доверенного ИИ при работе с требованиями. Представлен анализ лучших отечественных и мировых практик применения онтологий в области безопасного проектирования, жизненного цикла и безопасности критической инфраструктуры. Разработана методология применения онтологий в области работы с требованиями. Разработана методология применения онтологий в области безопасного проектирования и жизненного цикла. Разработана методология применения онтологий в области безопасности КИИ. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Разработаны методы применения доверенного ИИ в задачах, связанных с работой с требованиями. Разработаны методы, модели, архитектурные решения и инструментарий для применения онтологий в области безопасности, работы с требованиями, безопасного жизненного цикла и безопасности КИИ. Сформированы рекомендации и требования по созданию онтологий, позволяющие на основе доверенного ИИ парировать 80% угроз известных в технологиях машинного обучения. Разработаны предложения по стандартизации онтологий в области безопасности, работы с требованиями, безопасного жизненного цикла и безопасности КИИ.	Минпромторг России, Минцифры России,

1.2.16 Прототипы (НИР/НИОКР)	2027	2028	Проведено исследование лучших практик, доступных технологий и перспективных продуктов. Разработаны дорожные карты средств моделирования, прототипирования и разработки, аналитических и программных продуктов. Разработан репозиторий шаблонов проектирования и реализации безопасных КИИ. Разработаны прототипы программных средств моделирования, прототипирования и разработки. Разработаны прототипы средств моделирования, прототипирования и разработки, аналитических и программных продуктов. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли.	Сформирована дорожная карта средств моделирования, прототипирования и разработки: - аналитических и программных продуктов; - программного обеспечения. Предоставлен отчет.	Минцифры России, Минпромторг России
1.2.17 Пилотные проекты и внедрение (НИОКР)	2026	2029	Определен состав пилотных заказчиков, систем, применений и требований. Определены пилотные и первоочередные проекты внедрения методики Конструктивной Безопасности на уровне: - субъектов КИИ; - типовых объектов КИИ; - программного обеспечения; - ДПАК; - Радиоэлектронной аппаратуры и модулей; - электронной компонентной базы. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет.	Определен состав якорных и пилотных заказчиков для внедрения Определены принципы и приоритеты внедрения Предложены рекомендации к НПА	Минцифры России, Минпромторг России

1.3 Архитектура безопасности и доверия	2026	2030	Разработка архитектурных решений, принципов и технологий для создания конструктивно безопасной информационной инфраструктуры, основанной на политиках безопасности	Архитектурные решения, операционные системы, средства защиты информации и средства разработки, обеспечивающие создание систем КИИ, обладающих повышенной устойчивостью к современным и перспективным угрозам информационной и кибербезопасности	Исполнители
1.3.1 Анализ лучших практик и перспектив развития архитектур безопасности (НИР)	2026	2027	Проведен анализ лучших отечественных и международных практик и методов создания систем на основе идеологии «нулевого доверия». Представлен анализ перспективных ниш, где обеспечение безопасности за счет архитектуры будет наиболее эффективно как с экономической точки зрения, так и с точки зрения нивелирования рисков информационной безопасности (далее – ИБ). Представлены предложения по определению базовых понятий архитектуры безопасности и доверия: микроядра, ядра разделения, MILS, FLASK. Представлены предложения по реализации базовых гарантий для обеспечения безопасной архитектуры аппаратных средств и ДПАК, в том числе: корень доверия, доверенная среда, аппаратно-программный модуль доверия. Проведена оценка возможности реализации элементов архитектуры безопасности и доверия на основе существующих отечественных технологий микроэлектронного производства. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Представлен отчет по лучшим международным практикам в области безопасных архитектур. Представлен существующий глоссарий в области архитектуры безопасности и доверия. Представлена оценка возможности реализации элементов архитектуры безопасности и доверия на основе существующих отечественных технологий микроэлектронного производства. Представлено ТЗ на разработку архитектуры безопасности и доверия (1.3.2) Сформированы предложения к ПНСТ.	АНО «Платформа НТИ», Фонд НТИ Минцифры России, Минпромторг России

1.3.2 Разработка архитектур безопасности и доверия (НИР)	2026	2027	Представлен анализ концептуального и терминологического базиса архитектур безопасности и доверия. Представлен анализ типов рисков безопасности и доверия, связанных с особенностями архитектурных решений при создании программных систем. Представлено описание общих принципов построения архитектурных моделей. Проведено исследование лучших отечественных и международных практик и методов создания систем на основе идеологии «нулевого доверия». Представлен анализ перспективных ниш, где обеспечение безопасности и доверия за счет архитектуры будет наиболее эффективно как с экономической точки зрения, так и с точки зрения нивелирования рисков ИБ. Определены понятия микроядра, ядра разделения, MILS, FLASK для реализации архитектуры безопасности и доверия. Определены понятия базовых гарантий и формы их реализации для обеспечения безопасной архитектуры аппаратных средств и ДПАК, в том числе: корень доверия, доверенная среда, аппаратно-программный модуль доверия. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Сформирован облик архитектуры безопасности и доверия, требования к базовым элементам. Подготовлена модель противодействия актуальным угрозам на основе архитектуры безопасности и доверия. Разработаны требования к архитектурным моделям, обеспечивающим покрытие 80% известных уязвимостей и угроз. Подготовлен анализ требований к архитектуре безопасности и доверия для реализации ДПАК на основе сквозных технологий доверия и безопасности. Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России
1.3.3 Разработка методических основ построения доверенных (защищенных) систем из элементов с различной степенью	2026	2027	Проведен анализ требований уполномоченного ФОИВ, предъявляемых к средствам защиты информации, средствам обеспечения безопасности информационных технологий, иному программному и программно-аппаратному обеспечению, используемому для построения доверенных (защищенных) систем. Проведен анализ требований уполномоченного ФОИВ, предъявляемых к защите информации в информационных системах, с целью определения возможностей построения доверенных (защищенных) систем из элементов с различной степенью доверенности.	Сформированы концептуальные основы построения доверенных (защищенных) систем из элементов с различной степенью доверенности с учетом требований уполномоченных ФОИВ. Сформированы принципы и общие требования к построению доверенных (защищенных) систем из элементов с различной степенью доверенности.	Минцифры России, Минпромторг России

доверенности (НИР)			Проведено исследование принципов и подходов к структуризации и сегментации информационной инфраструктуры и систем, подлежащих защите, для обеспечения возможности использования для их построения элементов с различной степенью доверенности. Проведено исследование возможности и лучших практик применения элементов аппаратной платформы, обеспечивающих защиту многофункциональных программно-аппаратных средств от угроз вмешательства через сетевые интерфейсы взаимодействия. Проведено исследование возможности и лучших практик применения в защищаемых системах доверенных элементов защиты средства вычислительной техники при одновременной работе в нескольких контурах обработки информации. Проведено исследование возможности и лучших практик применения в защищаемых системах доверенных средств однонаправленной передачи информации при взаимодействии различных сегментов систем между собой и с внешними системами. Проведено исследование и развитие подходов применения мониторинговых мер защиты информации при использовании в защищаемых системах элементов с различной степенью доверенности. Сформированы принципы и общие требования к построению доверенных (защищенных) систем из элементов с различной степенью доверенности. Разработаны архитектурные рекомендации по построению доверенных (защищенных) систем из элементов с различной степенью доверенности. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Разработаны архитектурные рекомендации по построению доверенных (защищенных) систем из элементов с различной степенью доверенности. Разработаны рекомендации, позволяющие сократить на 70 % время разработки и внедрения систем защиты информации, повысить на 50% эффективность защиты от угроз безопасности информации, увеличить в 2-3 раза номенклатуру средств защиты информации. Сформированы предложения к ПНСТ.	

1.3.4 Исследование лучших практик изоляции и контроля за элементами с низким уровнем доверия (НИР)	2026	2027	Проведено исследование лучших мировых практик обеспечения изоляции элементов, потенциально содержащих недокументированные возможности. Проведено исследование архитектур (MILS, Separation Kernel), позволяющих создавать доверенные системы с использованием элементов, потенциально содержащих НДВ Определены модели, архитектурные решения, рекомендации и требования по обеспечению безопасной эксплуатации элементов, потенциально содержащих НДВ на следующих уровнях реализации: - системы уровня предприятия; - автоматизированные системы (ОКИИ); - вычислительная техника; - телекоммуникационное оборудование; - промышленные контроллеры и АСУТП; - доверенные ПАК; - радиоэлектронное оборудование; - электронные элементы и модули; - электронная компонентная база. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации. Сформированы предложения к ПНСТ.	Сформированы концептуальные основы построения доверенных (защищенных) систем из элементов, потенциально содержащих недокументированные возможности. Представлен сравнительный анализ лучших практик и концепций (MILS, FLASK, Separation Kernel и др). Разработаны архитектурные рекомендации, принципы и общие требования к построению доверенных (защищенных) систем из элементов с различной степенью доверенности на различных уровнях – от ЭКБ до уровня предприятия. Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России

1.3.5 Анализ лучших практик, моделей и архитектур для построения инфраструктуры на основе политик безопасности (НИР)	2026	2027	Проведен анализ лучших отечественных и международных практик и методов создания систем на основе политик безопасности. Представлен обзор средств обеспечения безопасности и доверия и повышения уровня доверия на основе моделирования и анализа архитектуры программных систем и применения политик безопасности. Представлен анализ перспективных ниш в области современных средств защиты информации на основе политик безопасности. Представлен анализ потребностей предприятий в перечисленных решениях, а также потенциальных рисков, связанных с отсутствием подобных решений, а также модель противодействия актуальным угрозам на основе автоматизированного контроля за политиками безопасности анализа взаимодействия средств защиты информации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Определены понятия политик безопасности, определена технологическая основа для применения подобных систем. Разработаны требования к исследованию моделей, архитектур и базовых элементов систем на основе политик безопасности (1.3.6, 1.3.7, 1.3.8) Сформированы предложения к ПНСТ.	Минцифры России, Минобрнауки России, АНО «Платформа НТИ», Фонд НТИ
1.3.6 Исследование методов и архитектур для построения инфраструктуры на основе политик безопасности (НИР)	2026	2027	Представлен обзор средств обеспечения безопасности и повышения уровня доверия на основе моделирования и анализа архитектуры программных систем и применения политик безопасности. Подготовлен анализ потребностей предприятий в части существующих средств защиты и сформирован перечень дополнительных функций и требований. Представлены рекомендации по использованию средств автоматизированного контроля за политиками безопасности анализа взаимодействия средств защиты информации. Представлены рекомендации по внедрению средств автоматизированного контроля за политиками безопасности анализа взаимодействия средств защиты информации с расчетом вероятной экономической целесообразности. Представлены требования к решениям средств	Представлена модель противодействия актуальным угрозам на основе автоматизированного контроля за политиками безопасности и взаимодействия средств защиты информации. Сформированы рекомендации по реализации архитектуры безопасности на основе базовых элементов и политик безопасности. Сформирован облик систем автоматизации контроля политик безопасности, подготовлена технологическая основа для применения подобных систем.	Минцифры России, Минобрнауки России, Минпромторг России

			автоматизированного контроля за политиками безопасности анализа взаимодействия средств защиты информации. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Разработаны требования к политикам безопасности, обеспечивающим покрытие 80% известных уязвимостей и угроз. Сформированы предложения к ПНСТ.	
1.3.7 Определение базовых понятий, концепций и архитектуры информационной инфраструктуры, основанной на политиках безопасности (НИР)	2026	2026	Определены перспективы и сценарии применения методов Конструктивной Безопасности, безопасной разработки и архитектуры безопасности и доверия к информационной инфраструктуре. Определены базовые понятия, концепции и архитектуры информационной инфраструктуры, основанной на политиках безопасности, включая: - модели разграничения доступа; - методики формирования доменов безопасности, средств безопасности и доверия, изоляции, политик разделения и др.; - методики управления безопасностью, базирующиеся на политиках безопасности; - аналитики инфраструктуры и политик безопасности на основе ИИ; - методики аналитики инфраструктуры и политик безопасности на основе ИИ. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Представлен анализ моделей разграничения доступа, применяемых для обеспечения функциональной и информационной безопасности, и обобщение их в терминах архитектуры систем. Создана методика формирования доменов безопасности, средств безопасности, изоляции, политик разделения и др. Создана методика управления безопасностью, базирующиеся на политиках безопасности. Проведено исследование лучших практик аналитики инфраструктуры и политик безопасности на основе ИИ. Создана методика аналитики инфраструктуры и политик безопасности на основе ИИ. Сформированы предложения к ПНСТ.	Минцифры России, Минобрнауки России, Минпромторг России
1.3.8 Разработка архитектуры конструктивно безопасных	2026	2027	Сформированы принципы построения конструктивно безопасных операционных систем. Принципы оформлены в виде научной статьи в журналах ВАК. Подготовлен аналитический отчет по сравнению классических и микроядерных операционных систем в части	Определены концептуальный и терминологический базис построения конструктивно безопасных операционных систем.	Минцифры России, Минобрнауки России

операционных систем (НИР)			устойчивости, надежности и безопасности. Результаты опубликованы в журналах ВАК. Подготовлен аналитический отчет о влиянии микроядерных ОС на эффективность, надежность и безопасность приложений. Результаты исследования опубликованы в журналах ВАК. Подготовлен аналитический отчет об основных технологических вызовах в разработке микроядерных операционных систем и идентифицированы способы их преодоления. Результаты исследования опубликованы в журналах ВАК. Проведен анализ, как микроядерные ОС влияют на эффективность, надежность и безопасность приложений. Проведен анализ экономической эффективности применения микроядерных ОС. Определены сценарии, где использование микроядерных операционных систем является наиболее эффективным с точки зрения обеспечения устойчивости, надежности и безопасности. По результатам исследований опубликована научная статья в журналах ВАК. Проведено исследование необходимости и роли применения наложенных средств защиты информации в конструктивно безопасных ОС. Разработаны принципы кросс платформенной разработки для повторного использования существующих компонентов в конструктивно безопасных ОС. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Предоставлен отчет, публикации.	Проведено сравнение классических и микроядерных операционных систем в части обеспечения устойчивости, надежности и безопасности. Проведен анализ сценариев использования микроядерных операционных систем с целью выявления таких сценариев, где такие ОС обеспечивают лучшую эффективность по сравнению с классическими ОС. Проведено исследование целей, задач, возможностей, и ограничений наложенных средств защиты информации в микроядерных операционных системах. Проведено сравнение с не менее чем 2 классическими ОС. Разработаны требования, позволяющие обеспечить покрытие до 80 % известных угроз на основе микроядерных ОС. Сформированы предложения к ПНСТ.	

1.3.9 Реализация конструктивно-безопасной ОС, построенной на политиках безопасности (НИОКР)	2026	2030	Разработана конструктивно безопасная микроядерная ОС на основе политик безопасности для: - встроенных применений; - для систем реального времени; - для реализации СЗИ/СКЗИ; - для сетевой аппаратуры; - для промышленных контроллеров и шлюзов; - для мобильных телефонов и планшетов; - для беспилотных аппаратов; - для высоконадежных систем.	Создана универсальная защищенная микроядерная ОС, построенная на принципах Конструктивной Безопасности, реализующая политики безопасности Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России
1.3.10 Исследование лучших практик и разработка безопасных архитектур и средств защищенной виртуализации (НИР)	2026	2027	Созданы типовые модели развертывания и внедрения средств защищенной виртуализации. Проанализированы и описаны необходимые интегрированные средства обеспечения доверия и безопасности новых средств защищенной виртуализации. Произведен сравнительный анализ стоимости владения и внедрения средств защищенной виртуализации. Показан положительный результат в части снижения рисков и угроз при использовании средств защищенной виртуализации. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлены предложения по ПНСТ. Разработана новая нормативно-методическая база для использования предложенного подхода в КИИ и ФОИВах.	Определены базовые понятия, концепции и сетевая архитектура для построения виртуальной защищенной инфраструктуры. Созданы типовые модели развертывания для различных инфраструктур. Разработаны сценарии использования защищенной виртуальной инфраструктуры, позволяющие обеспечить защиту от 80% известных уязвимостей и угроз. Сформированы рекомендации и требования к прототипам (1.3.11). Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России
1.3.11 Разработка прототипов средств защищенной виртуализации (НИР)	2026	2028	Разработаны прототипы программно-аппаратных платформ и средства защищенной виртуализации.	Создан прототип универсальная программно-аппаратная среда защищенной виртуализации, построенная на принципах Конструктивной Безопасности, реализующая политики безопасности	Минцифры России, Минпромторг России,

				Сформированы предложения к ПНСТ.	
1.3.12 Исследование лучших практик и разработка безопасных архитектур облачных и сетевых инфраструктур на базе программно-определяемых сетей (НИР)	2026	2027	Созданы типовые модели развертывания и внедрения программно-определяемых сетей для различных сетевых архитектур предприятий. Проанализированы и описаны необходимые интегрированные средства обеспечения кибербезопасности новых видов сетевых архитектур. Произведен сравнительный анализ стоимости владения и внедрения новых и старых сетевых архитектур. Показан положительный результат (экономия денежных средств при использовании нового подхода). Разработана нормативно-методическая база для создания новых облачных сервисов со встроенными средствами безопасности для обеспечения киберустойчивости инфраструктуры построенной на базе данной технологии. Разработана новая нормативно-методическая база для использования предложенного подхода в ФОИВ. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности.	Определены базовые понятия, концепции и сетевая архитектура для построения сетей на базе технологии программно-определяемых сетей. Созданы типовые модели развертывания новых видов сетей для различных инфраструктур. Разработаны сценарии использования программно-определяемых сетей, позволяющие обеспечить защиту от 80% известных уязвимостей и угроз. Представлены предложения по ПНСТ.	Минцифры России, Минпромторг России
1.3.13 Анализ перспектив применения ИИ для защиты КИИ (НИР)	2026	2027	Проведен анализ лучших международных практик применения Искусственного Интеллекта для защиты КИИ от угроз кибербезопасности. Проведен анализ возможностей реализации функционала на основе суверенных российских технологий – доверенного ИИ, ЭКБ и др. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности.	Представлен анализ возможностей и перспектив использования Доверенного ИИ для защиты КИИ от угроз кибербезопасности. Сформировано задание на исследование возможностей и перспектив использование доверенного ИИ в области защиты – предотвращение, детектирование, реагирование, восстановление и расследование киберинцидентов (1.3.15-16). Представлен проект ПНСТ.	Минцифры России, Минпромторг России

1.3.14 Исследование перспектив использования средств доверенного ИИ для построения инновационных СЗИ (НИР)	2026	2027	Проведено исследование перспектив применения ИИ в СЗИ/СКЗИ. Проведено исследование использования ИИ для целей противодействия злоумышленникам. Проведено исследование принципов обеспечения ИБ для решений с использованием ИИ, формирование доверенной среды для использования ИИ. Созданы методики и стандартов автоматического анализа приложений на предмет уязвимостей, базирующийся на Доверенном ИИ. Проведено исследование лучших практик аналитики инфраструктуры и политик безопасности на основе ИИ. Исследование возможности создание средств машинного обучения в целях предотвращения компрометации учетных сведений пользователя. Проведено исследование использования ИИ для целей обучения безопасной разработке и безопасной эксплуатации. Проведено исследование использования ИИ для целей упрощения принятия решений и снижения рутинной нагрузки в ИБ.	Представлен анализ возможностей и перспектив внедрения Доверенного ИИ Разработаны рекомендации и требования по реализации ИБ и СЗИ на основе Доверенного ИИ Разработаны рекомендации и требования по безопасному жизненному циклу Доверенного ИИ. Созданы рабочие прототипы СЗИ на основе доверенного ИИ. Представлен проект ПНСТ.	Минцифры России, Минпромторг России
1.3.15 Разработка перспективных средств защиты на основе доверенного ИИ (НИР)	2026	2028	Разработаны модели противодействия внутреннему нарушителю с учетом инновационных технологий. Созданы инструменты и средства противодействия внутреннему нарушителю с учетом инновационных технологи. Созданы методики и стандарты автоматического создания отчетов по инцидентам с использованием ИИ. Создана методология и инструментарий применения ИИ для формирования признаков новых компьютерных инцидентов, в т. ч. для исследования аномалий трафика. Разработаны модели использования средств машинного обучения в целях предотвращения компрометации учетных сведений пользователя.	Созданы рабочие прототипы средств определения и противодействия внутреннему нарушителю на основе Доверенного ИИ, включая: - средства определения признаков компьютерных инцидентов; - средства определения и классификации аномалий трафика; - средства определения и классификации аномалий деятельности ОС и программ; - средства реагирования на киберинциденты; - средства автоматического создания отчетов;	Минцифры России, Минпромторг России

			Разработан ИИ-специалист по реагированию на киберинциденты, решающий задачу реагирования для типовых инцидентов в полностью автономном режиме. Разработана методика анонимизации и псевдоанонимизации данных для последующего применения тестировании систем работы с большими данными и обучения искусственного интеллекта.	- средства обучения. Представлен проект ПНСТ.	
1.3.16 Разработка СЗИ на основе доверенного ИИ (НИР)	2026	2030	Разработка интеллектуальных систем раннего определения, распознавания и расследования киберпреступлений: • Разработана методология применения ИИ для прогнозирования векторов атак и угроз безопасности, в т.ч. таргетированных; • Разработан прототип решения; • Проведена опытная эксплуатация. ИИ для целей обучения безопасной разработке и безопасной эксплуатации • Проведен НИР по исследованию возможностей и барьеров, определению требований, формированию модели инструмента; • Разработан прототип инструмента с элементами ИИ для формирования оптимального наполнения обучающего курса по безопасной разработке ПО и безопасной эксплуатации СЗИ с учетом отраслевой специфики субъекта КИИ; • Проведена опытная эксплуатация. ИИ для целей противодействия злоумышленникам (дезориентация и ловушки) • Проведено исследование возможностей и барьеров, определены требования, сформированы модели инструмента; • Разработан прототип решения; • Проведена опытная эксплуатация. Инструменты на базе ИИ для безопасной разработки	• Сокращён срок выявления, распознавания и расследования киберпреступлений, снижена вероятность ошибки, тяжести последствий; • Повышено качество и безопасность разрабатываемого ПО и его применения; • Снижена вероятность проникновения киберпреступников во внутренний контур ОКИИ и тяжесть ущерба от их действий; • Существенно снижен объем компрометированных сведений, тем самым повышена защищённость ОКИИ • Представлен проект ПНСТ.	Минцифры России, Минпромторг России

			• Проведен НИР по исследованию возможностей и барьеров, определению требований, формированию модели инструмента; • Разработан прототип инструментальной надстройки с элементами ИИ для первичной обработки информации от инструментов тестирования ПО в рамках безопасной разработки; • Проведена опытная эксплуатация. Создание средств машинного обучения в целях предотвращения компрометации учетных сведений пользователя • Проведено исследование возможностей и барьеров; • Определены требования, сформирована модель инструмента; • Создан ряд «цифровых двойников» с применение усовершенствованной технологии, использующей машинное обучение.		
1.3.17 Внедрение инструментов ИИ в СЗИ, разработка инструментов и средств адаптированных под встраивание в существующие СЗИ в целях ускорения процессов и оптимизации функционала (НИР)	2026	2030	Создание инструментов и средств противодействия внутреннему нарушителю с учётом инновационных технологий • Построена системно-динамическая модель внутреннего нарушителя ИБ с учётов рисков воздействия инструментов социальной инженерии, сформированных с использованием ИИ; • Разработан прототип инструментов и средств противодействия внутреннему нарушителю. Методология и инструментарий применения ИИ для формирования признаков новых компьютерных инцидентов, в т.ч. для исследования аномалий трафика • Разработана методология; • Разработан прототип инструмента определения новых инцидентов; • Проведена опытная эксплуатация.	• Снижены риски и последствия от действий внутреннего нарушителя, повышена устойчивость ОКИИ; • Повышена эффективность безопасной разработки, повышена защищенность ПО; • Ускорение процессов, снижение вероятности ошибки и, как следствие, уменьшение ущерба и тяжести последствий; • Представлен проект ПНСТ.	Минцифры России, Минпромторг России

			Внедрение ИИ для целей упрощения принятия решений и снижения рутинной нагрузки в ИБ • Проведено исследование возможностей и барьеров, определены требования, сформированы модели инструмента; • Разработан прототип инструмента для замены рутиной деятельности и помощи в принятии решений ИБ специалистами на основе ИИ; • Проведена опытная эксплуатация.		
1.3.18 Разработка и апробация методик автоматизированной оценки уровня защищённости ИС и объектов Интернета вещей на ОКИИ (НИР)	2026	2029	• Разработана методика оценки и рейтингования уровня защищенности ИС и объектов Интернета вещей, автоматизации оценки, разработаны требования к испытательному стенду; • Создан испытательный стенд, проведена апробация методики; • Разработаны предложения по развитию НПА; • Проведена опытная эксплуатация.	Сокращено время подбора СЗИ и сервисов, повышена устойчивость ОКИИ; Сформирована нормативная правовая база; Представлен проект ПНСТ.	Минцифры России, Минпромторг России

1.3.19 Разработка унифицированной методики тестирования производительности, устойчивости функционирования и функциональных возможностей СЗИ (НИР)	2026	2028	• Разработана унифицированная методика тестирования производительности, устойчивости функционирования и функциональных возможностей СЗИ • Разработаны требования к испытательному стенду; • Создан испытательный стенд; • Проведена апробация методологии.	Устранена проблема задержки распространения СЗИ на объектах защиты и выхода на рынок, а также проблема дополнительной финансовой и административной нагрузки как на разработчиков решений, так и на их потребителей Представлен проект ПНСТ.	Минцифры России, Минпромторг России
1.3.20 Создание комплексных систем ИБ с учётом особенности их интеграции в ОКИИ (НИР)	2026	2029	• Сформирован экосистемный подход в разработке комплексных систем информационной безопасности и их отдельных компонентов; • Проведена унификация механизмов интеграции в ОКИИ средств защиты информации; • Разработаны предложения по развитию НПА; • Проведено пилотирование.	Обеспечено комплексное решение проблемы киберустойчивости ОКИИ на всех стадиях жизненного цикла; Типизация систем обеспечения безопасности; Оптимизация затрат на создание СЗИ. Представлен проект ПНСТ.	Минцифры России, Минпромторг России

1.3.21 Разработка перспективных методов и средств идентификации угроз кибербезопасности (НИР)	2026	2027	Разработана система оценки возможных путей атак, симуляторов, анализаторов площади атак, исследование методов и способов оценки. Разработана методика идентификации активов в сетях IT и OT пассивными методами. Разработана методика автоматизированной оценки уровня защищенности ИС и объектов Интернета вещей на ОКИИ. Разработана автоматическая система контроля уязвимостей на внешнем контуре объектов КИИ. Подготовлен анализ ПО по требованиям оценочного уровня доверия 4 (далее – ОУД4).	Созданы рабочие прототипы средств идентификации угроз на основе Доверенного ИИ, включая: - средства оценки возможных путей атак; - анализаторы площади атак; - анализаторов и контроля наличия уязвимостей; - анализа защищенности объектов КИИ; - идентификации активов в сетях IT и OT. Представлены рекомендации и требования по реализации функций идентификации угроз в рамках ДПАК. Представлен проект ПНСТ	Минцифры России, Минпромторг России
1.3.22 Разработка перспективных методов и средств детектирования угроз кибербезопасности (НИР)	2026	2027	Проведено исследование лучших отечественных и международных практик и методов детектирования угроз кибербезопасности на основе ИИ. Созданы эффективные алгоритмы детектирования угроз кибербезопасности, в том числе – на основе доверенного ИИ. Разработаны методологии построения доверенных программно-аппаратных комплексов с интегрированной поддержкой детектирования угроз кибербезопасности.	Созданы рабочие прототипы средств детектирования угроз на основе доверенного ИИ. Разработаны рекомендации и требования по интеграции в ДПАК функций детектирования угроз кибербезопасности. Разработаны рекомендации и требования по реализации платформенных средств детектирования угроз кибербезопасности. Представлен проект ПНСТ.	Минцифры России, Минпромторг России
1.3.23 Разработка перспективных методов и	2026	2027	Проведено исследование лучших отечественных и международных практик и методов создания программно-аппаратных систем с поддержкой функций восстановления после киберинцидентов.	Созданы рабочие прототипы средств восстановления после киберинцидентов.	Минцифры России, Минпромторг России

средств восстановления (НИР)	2026	2027	Разработаны методологии построения доверенных программно-аппаратных комплексов с интегрированной поддержкой восстановления после киберинцидентов. Созданы методики и требования по обеспечению восстановления данных в результате киберинцидентов.	Разработаны рекомендации и требования по реализации функций поддержки восстановления данных в рамках ДПАК. Разработаны рекомендации и требования по реализации платформенных средств детектирования угроз кибербезопасности. Представлен проект ПНСТ.	
	2027	2030	Созданы эффективные алгоритмы сжатия и разжатия данных для применения системах бэкапирования и восстановления. Созданы платформенные решения и инструменты для обеспечения восстановления данных в результате киберинцидентов. Созданы автоматизированные системы бэкапирования данных в изолированные среды для обеспечения восстановления в том числе при атаках троянов-шифровальщиков.		
1.3.24 Разработка перспективных методов и средств расследования киберинцидентов (НИР)	2026	2027	Проведено исследование лучших практик создания программно-аппаратных платформ класса форенсик.	Разработаны подходы, методы и архитектурные решения, позволяющие сократить время расследования киберинцидентов и увеличить раскрываемость. Созданы рабочие прототипы средств расследования киберинцидентов. Разработаны рекомендации и требования по реализации функций расследования киберинцидентов в рамках ДПАК. Разработаны рекомендации и требования по реализации платформенных средств расследования киберинцидентов. Представлен проект ПНСТ.	Минцифры России, Минпромторг России
	2026	2027	Разработаны методики по увеличению отслеживаемости киберинцидентов (форенсик). Разработка интеллектуальных систем раннего определения, распознавания и расследования киберпреступлений. Разработаны требования к встроенным системам обеспечения сбора информации об инцидентах, обеспечивающих надежное хранение и неизменность данных для киберкриминалистики. Разработка методологии построения доверенных программно-аппаратных комплексов с интегрированной поддержкой фиксации параметров функционирования, необходимых для расследования киберинцидентов.		
	2027	2030	Создан универсальный мультиплатформенный фреймворк для автоматизированного сбора артефактов, необходимых в рамках реагирования на киберинциденты. Разработана система класса «черный ящик» для сбора информации об инцидентах на основе блокчейна,		

			обеспечивающий надежное хранение и неизменность данных для последующей форензики и кибер-криминалистики.		
1.3.25 Разработка прототипов перспективных платформенных средств обеспечения безопасности и доверия для разных уровней КИИ (НИР/НИОКР)	2026	2027	Разработаны прототипы средств расширенного детектирования киберугроз (XDR), использующие телеметрию с широкого набора устройств в корпоративной сети (как с конечных точек и сетевых экранов, так и с видеокамер и датчиков температуры). Разработана единая консоль управления продуктами безопасности ИТ и операционных технологий (далее – ОТ) (промышленных систем управления – ICS). Разработаны средства выявления атак и аномалий в ОТ оборудовании на базе анализа трафика. Разработаны комплексные решения для идентификации и управления ОТ активами, включая выявление уязвимых устройств / прошивок. Разработаны средства идентификации и управления ОТ активами, включая выявление уязвимых устройств / прошивок. Разработаны комплексные решения по сбору телеметрии с конечных точек под управлением операционных систем на базе Linux.	Обеспечено комплексное решение проблемы киберустойчивости ОКИИ на всех стадиях жизненного цикла. Сформирован экосистемный подход в разработке комплексных систем информационной безопасности и их отдельных компонентов. Проведена унификация механизмов интеграции средств защиты информации в ОКИИ. Сокращено время подбора СЗИ и сервисов, повышена устойчивость ОКИИ. Подготовлена методика оценки и рейтингования уровня защищённости ИС и объектов Интернета вещей, автоматизации оценки. Созданы комплексные системы ИБ с учётом особенности их интеграции в ОКИИ. Представлен проект ПНСТ	Минцифры России, Минпромторг России
1.3.26 Оптимизация и гармонизация требований к СЗИ (НИР)	2026	2027	Проведено исследование регуляторного пространства ИБ с целью создания оптимального пути внедрения стандартов и требований к СЗИ и процессам их использования. Разработаны унифицированные методики тестирования производительности, устойчивости функционирования и функциональных возможностей СЗИ с гармонизацией требований к СЗИ.	Представлен отчет по исследованию регуляторного пространства ИБ, выработаны рекомендации по оптимизации пути внедрения стандартов и требований к СЗИ и процессам их использования.	Минцифры России, Минпромторг России

			Построены модели оценки соответствия нормативным актам государственных регуляторов.		
1.3.27 Пилотные проекты и внедрение	2029	2030	Определен состав пилотных заказчиков, систем, применений и требований. Сформирована дорожная карта внедрения. Представлена дорожная карта. Проведен форсайт с регуляторами, заказчиками и компаниями-лидерами отрасли. Представлены проекты ТЗ, протоколы испытаний, отчет об успешном внедрении.	Проведены пилотные и первоочередные проекты внедрения конструктивно-безопасных КИИ в области: - беспилотных систем; - видеонаблюдения, обеспечения контроля доступа и физической защиты; - обеспечения мобильности и цифровых сервисов; - телекоммуникаций и связи; - транспортных систем; - промышленности, энергетики и строительства.	Минцифры России, Минпромторг России, Минобрнауки России

1.4 Обеспечение гарантий целостности криптографическими методами	2026	2030	Разработка инновационных СЗИ/СКЗИ, способных обеспечить надежное и устойчивое функционирование КИИ в условиях растущих угроз информационной и кибербезопасности	Архитектура и методика создания КИИ, обладающих повышенной устойчивостью к современным и перспективным угрозам информационной и кибербезопасности	Исполнители
1.4.1 Прогноз и сценарии развития средств цифровой массовой криптографии (НИР)	2026	2027	Представлено исследование зарубежных лучших практик применения средств цифровой криптографии. Представлено исследование и прогноз рисков и угроз, определяющих развитие и применение средств цифровой криптографии. Представлена оценка различных сценариев реализации квантовой угрозы и разработка практических рекомендаций по созданию эффективных СКЗИ. Сформирован прогноз развития технологий и средств цифровой криптографии и их реализации в Российской Федерации, включая квантовую угрозу, гомоморфное шифрование, ИИ и ИИ IoT Представлены сценарии развития средств цифровой криптографии для рынков вычислительной техники, ТКО, ИоТ/ИИоТ. Представлена оценка рынка и дорожная карта развития средств цифровой криптографии. Сформированы требования к составу программных и аппаратных средств криптографических средств, обязательных к применению на объектах КИИ в составе ПО и оборудования. Созданы унифицированные методики тестирования производительности, устойчивости функционирования и совместимости СКЗИ с гармонизацией требований к СКЗИ, ТЗ на испытательный стенд, публикации.	Определен ландшафт рисков и угроз, определяющих развитие и применение средств цифровой криптографии, в том числе – квантового вычислителя и ИИ. Сформирован прогноз развития зарубежных и отечественных средств цифровой криптографии в горизонте 5-10 лет. Проведена оценка технологических возможностей реализации аппаратно-программных средств криптографической защиты, включая отечественную компонентную базу. Определены возможности и сценарии применения средств цифровой криптографии в вычислительной технике, ТКО, П, ИоТ/ИИоТ и др. Сформированы требования к составу программных и аппаратных средств криптографических средств, обязательных к применению на объектах КИИ в составе ПО и оборудования.	Минцифры России, Минпромторг России, Минобрнауки России

			Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлены сценарии развития, требования к технологиям и продуктам. Представлен ПНСТ (корень доверия, СА). Сформированы предложения по развитию НПА и мер поддержки.		
1.4.2 Развитие перспективных криптографических методов для обеспечения целостности жизненного цикла (НИР)	2026	2027	Проведено исследование встраивания криптографических механизмов в рамках ГОСТ. Проведено исследование перспективных механизмов защиты данных в условия квантового вычислителя. Проведено исследование перспектив внедрения технологий квантового распределения ключей в типовые механизмы обеспечении информационной безопасности. Разработана методика использования технологий гомоморфного шифрования для определенных классов данных.	Разработаны рекомендации и требования встраивания криптографических механизмов в соответствии с ГОСТ. Разработаны рекомендации и требования внедрения технологий квантового распределения ключей в типовые механизмы обеспечении информационной безопасности Сформированы предложения к ПНСТ	Минцифры России, Минпромторг России, Минобрнауки России
1.4.3 Развитие Удостоверяющих Центров для обеспечения гарантий целостности криптографическими методами (НИР)	2026	2030	Проведено исследование лучших практик применения удостоверяющих центров (УЦ) для обеспечения гарантий целостности криптографическими методами. Определены возможности и требования использования УЦ для работы с программным обеспечением, операционными системами, доверенными аппаратными средствами, доверенными программно-аппаратными комплексами. Сформированы требования по реализации гарантий целостности в программном обеспечении, операционных системах, доверенных аппаратных средствах, доверенных программно-аппаратных комплексах.	Сформированы требования к УЦ, обеспечивающими гарантии целостности криптографическими методами при работе с ПО, ОС, ДАС, ДПАК. Сформированы требования, в том числе архитектурные, к реализации гарантий целостности в ПО, ОС, ДАС, ДПАК. Сформированы предложения к ПНСТ.	Минцифры России, Минпромторг России, Минобрнауки России
1.4.4 Разработка методов повышения безопасности и доверия	2026	2027	Представлены результаты исследования лучших практик защиты и повышения устойчивости на основе применения аппаратных решений и программных решений корня доверия Представлены результаты исследования лучших практик защиты и повышения устойчивости на основе защиты управляющего трафика.	Разработаны методы обеспечения доверия и безопасности вычислительной техники, телеком оборудования и др. с помощью базовых элементов доверия и безопасности: корня доверия,	Минцифры России, Минпромторг России, Минобрнауки России

оборудования массового производства с использованием российских криптографических механизмов (НИР)			Представлены результаты исследования лучших практик защиты и повышения устойчивости телеком оборудования и совместимости коммуникационных протоколов. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлены сценарии развития, требования к технологиям и продуктам, предложения по развитию НПА и мер поддержки. Представлены предложения по ПНСТ. Представлен отчет.	интегрированной защищенной доверенной среды и защиты управляющего трафика. Сформированы предложения по составу и архитектуре средств защиты. Сформированы предложения к ПНСТ.	
1.4.5 Исследование телекоммуникационных линий связи и межмашинных каналов управления на физическом уровне для задач обеспечения безопасности (НИР/НИОКР)	2026	2030	Дооснащен ПАК Балисет-2 для обеспечения возможности генерации на физическом уровне сигналов высокоскоростных телекоммуникационных линий связи и межмашинных интерфейсов. Перевыпущен основной СБИС ПАК Балисет-2 на фабрике SMIC 28 нм. для обеспечения диверсификации по производству основного компонента ПАК. Увеличена производительность ПАК Балисет-2 не менее чем до 100 Гигавыборок в секунду на канал, дооснащение ПАК входным предусилителем собственной разработки. Произведен переход в ПАК Балисет-2 на модульную архитектуру для снижения стоимости ПАК не менее чем в 2 раза при полном сохранении функциональных возможностей. Увеличена производительность ПАК Балисет-2 не менее чем до 200 Гигавыборок в секунду на канал. Дооснащен ПАК Балисет-2 технологической оснасткой для прямого внедрения на физическом уровне в высокоскоростные телекоммуникационные линии связи и межмашинные интерфейсы.	ПАК Балисет-2 с возможностью генерации телеком. сигналов и межмашинных интерфейсов. Диверсификации ПАК Балисет-2 по производству основных компонентов. ПАК Балисет-2 с производительностью не менее до 100 Гигавыборок в сек на канал. ПАК Балисет-2 модульной архитектуры. ПАК Балисет-2 с производительностью не менее до 200 Гигавыборок в сек на канал. Технологическая оснастка для внедрения в каналы на физическом уровне.	Минцифры России, Минпромторг России, Минобрнауки России
1.4.6 Создание отечественных микропроцессорных решений и электронных модулей с	2026	2030	Создана платформа испытаний массовых микропроцессорных решений и электронных модулей отечественных разработчиков с использованием российских криптографических алгоритмов. Обеспечено развитие платформы.	Сформирован состав функций и элементов безопасности, предназначенных к обязательному встраиванию в доверенные программно-аппаратные комплексы.	Минцифры России, Минпромторг России, Минобрнауки России

использование м российских криптографических алгоритмов (НИР)			Проведено исследование возможностей реализации функций безопасности на основе существующих отечественных технологий микропроцессорного производства.	Представлен анализ возможностей реализации функций безопасности на основе существующих отечественных технологий микропроцессорного производства. Сформирован состав рекомендованных элементов безопасности, реализуемых на основе отечественных технологий микропроцессорного производства.	
1.4.7 Создание архитектуры реализации КРК для последующего применения КРК (НИР)	2026	2030	Проведено исследование перспектив использования квантового распределения ключей (далее – КРК) для обеспечения гарантий целостности жизненного цикла объектов КИИ. Разработаны рекомендации по составу элементной базы и внедрению квантозависимых ключей в типовые механизмы обеспечении информационной безопасности. Проведено исследование возможностей реализации элементной базы для КРК на основе существующих отечественных технологий микропроцессорного производства.	Сформированы рекомендации по использования КРК для обеспечения гарантий целостности жизненного цикла объектов КИИ Сформирован состав и требования к ЭКБ для реализации систем с использованием КРК. Определены возможности использования отечественного микроэлектронного производства. Сформированы предложения к ПНСТ.	Минпромторг России, Минцифры России
1.4.8 Пилотирование и внедрение криптографических методов (НИР)	2028	2030	Определен состав пилотных заказчиков, систем, применений и требований в области: - беспилотных КИИ; - видеонаблюдения, обеспечения контроля доступа и физической защиты; - обеспечения мобильности и цифровых сервисов; - телекоммуникаций и связи; - транспортных систем; - промышленности, энергетики и строительства.	Представлены Дорожная карта, проект ТЗ, протоколы испытаний, отчет об успешном внедрении.	Минпромторг России Минцифры России

1.5 Доверенные аппаратные средства	2026	2030	Разработка инновационной архитектуры доверенных аппаратных средств, ДПАК и ЭКБ, позволяющей создавать КИИ, способные противостоять перспективным угрозам информационной и кибербезопасности	Защищенная архитектура ЭКБ, средства и методики разработки, обеспечивающие создание ДАС и ДПАК с повышенной устойчивостью к современным и перспективным угрозам информационной и кибербезопасности	Исполнители
1.5.1 Анализ лучших практик повышения защищенности ДАС (Поисковый НИР)	2026	2027	Проведен анализ существующих мировых практик защиты оборудования. Проведено исследование лучших практик защиты и повышения устойчивости ВТ, ТКО, АСУТП, БПЛА и др. с помощью базовых элементов доверия и безопасности: корня доверия, интегрированной защищенной доверенной среды и защиты управляющего трафика. Изучены перспективы и сценарии применения методов Конструктивной Безопасности, безопасного жизненного цикла и архитектур безопасности с целью создания доверенных аппаратных средств. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлены сценарии развития, требования к технологиям и продуктам, предложения по развитию НПА и мер поддержки. Представлен отчет.	Представлены результаты исследования лучших практик защиты и повышения устойчивости ВТ, ТКО, АСУТП, ИоТ и БПЛА. Представлены результаты анализа лучших практик защиты и повышения устойчивости на основе корня доверия, аппаратно-программных модулей доверия, интегрированной защищенной доверенной среды, аппаратных модулей защиты управляющего трафика. Представлена оценка рынка, аппаратных средств обеспечения доверия и безопасности	АНО «Платформа НТИ», Фонд НТИ
1.5.2 Исследование рисков и угроз на уровне аппаратных средств (Линейный НИР)	2026	2027	Проведено исследование потенциальных целей кибератак, мотивации и профиля нарушителей. Проведено исследование и анализ рисков и угроз на уровне аппаратных средств. Проведено исследование и оценка рисков и угроз, прогноз потенциального ущерба в зависимости от сценария. Проведено исследование основных целей кибератак. Проведено исследование и анализ статистики киберинцидентов.	Представлены результаты анализа статистики киберинцидентов, известных и потенциальных уязвимостей, угроз и рисков, целей и методов кибератак на уровне аппаратных средств. Сформированы предложения по противодействию угрозам на основе	Минпромторг России ФПИ РНФ

			Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлен отчет.	методов Конструктивной Безопасности. Представлены предложения на исследование методов и архитектурных решений для создания доверенных аппаратных средств. Сформировано ТЗ на разработку требований к аппаратным компонентам доверия и безопасности (1.5.3), их жизненного цикла (1.5.4), возможности реализации на отечественном производстве (1.5.5) и микросборок (1.5.6), нейроморфных вычислений (1.5.7) и защищенной процессорной архитектуры (1.5.8).	
1.5.3 Разработка требований к аппаратным компонентам, реализующим базовые функции доверия и безопасности (НИР)	2026	2027	Проведено исследование лучших мировых практик создания и применения специализированных аппаратных элементов и модулей, реализующих функции доверия и безопасности в составе радиоэлектронного оборудования. Определен состав аппаратных модулей доверия и безопасности, в том числе: корня доверия, интегрированной защищенной доверенной среды, модули защиты управляющего трафика и др. Определены архитектурные решения, позволяющие повысить уровень доверия и безопасности ДПАК с использованием аппаратных элементов безопасности. Представлены сценарии развития, требования к технологиям и продуктам, предложения по развитию НПА и мер поддержки. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности.	Разработаны требования к аппаратным модулям доверия и безопасности, в том числе: корню доверия, интегрированной защищенной доверенной среды, модулей защиты управляющего трафика. Учтены требования рисков и угроз (1.5.2), реализации отечественной криптографии (1.4.2-1.4.6). Определены требования к реализации в составе микросборок (1.5.6), защищенной архитектуры (1.5.8) и решений (1.5.10) Представлен ПНСТ. Представлены рекомендации по мерам поддержки и НПА.	Минпромторг России, Минцифры России

1.5.4 Разработка требований к жизненному циклу аппаратных модулей доверия и безопасности (НИР)	2026	2027	Разработана технология управления сетью доверенных ПАК на основе цифровых двойников и встроенных модулей безопасности. Разработаны требования и рекомендации к жизненному циклу производства доверенных ПАК, использующих аппаратные корни доверия, в том числе с использованием Квантового Распределения Ключей. Разработаны методики анализа защищённости аппаратных корней доверия против атак по побочным каналам. Разработаны требования и рекомендации по реализации комплексной системы тестирования аппаратных корней доверия. Разработаны образовательные программы по встраиванию и использованию модулей безопасности и аппаратных корней доверия.	Разработана технология использования аппаратного корня доверия для доверенной загрузки и удалённого защищённого управления доверенными программно-аппаратными комплексами БПЛА, IoT, информационные системы и АСУ ЗО КИИ. Разработана система удалённого управления и мониторинга модулей безопасности БПЛА, IoT, информационные системы и АСУ ЗО КИИ. Представлен ПНСТ. Представлены рекомендации по мерам поддержки и НПА.	Минпромторг России, Минцифры России
1.5.5 Исследование возможности реализации ЭКБ доверия и безопасности на базе отечественного производства электронных компонентов (НИР)	2026	2027	Определены возможности и состав аппаратных модулей доверия и безопасности для реализации ДАС, в том числе: корня доверия, аппаратно-программного модуля доверия, интегрированной защищенной доверенной среды, модули защиты управляющего трафика и др. Сформирована дорожная карта реализации ЭКБ доверия и безопасности, проведена оценка стоимости реализации. Определены технологические барьеры Представлены рекомендации по мерам поддержки и НПА Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности.	Представлен анализ возможностей реализации функций безопасности на базе отечественного производства электронных компонентов, включая микропроцессоры и микроконтроллеры, системы хранения ключевой информации и др (ИС1 250/180/130/90нм). Учтены требования реализации отечественной криптографии (1.4.2-1.4.6). Определены требования к реализации в составе микросборок (1.5.6) и решений (1.5.10). Представлен ПНСТ. Представлены рекомендации по мерам поддержки и НПА.	Минпромторг России ФПИ, Минцифры России

1.5.6 Разработка типовых аппаратных решений безопасности и доверия на основы микросборок (НИР)	2026	2027	Проведено исследование лучших мировых практик по реализации функций доверия и безопасности на основе чиплетов. Определены основные принципы, методики и архитектурные решения. Разработаны основные принципы создания аппаратных решений безопасности и доверия на основы микросборок для применения в ДПАК. Разработаны типовые рекомендации и требования к реализации решений безопасности и доверия на основы микросборок. Проведен форсайт с регуляторами, ключевыми заказчиками, разработчиками СБИС, систем и компонент доверия и безопасности.	Представлены основные принципы создания аппаратных решений безопасности и доверия на основы микросборок. Разработан прототип. Представлены предложения по требованиям и рекомендации по реализации архитектуры безопасности на базе аппаратных решений безопасности и доверия на основы микросборок. Учтены требования рисков и угроз (1.5.2), требования реализации отечественной криптографии (1.4.2-1.4.6). Определены требования к реализации в составе решений (1.5.10). Представлены предлоежения по ПНСТ. Представлены рекомендации по мерам поддержки и НПА.	Минпромторг России, Минцифры России
1.5.7 Исследование возможностей использования нейроморфных вычислений для реализации интегрированных функций доверия и безопасности (НИР)	2026	2028	Разработаны прорывные технологии нейроморфных вычислений. Разработаны типовые сценарии применения нейроморфных вычислений и Доверенного ИИ для реализации функций доверия и безопасности. Разработаны требования и рекомендации по реализации принципов Конструктивной Безопасности для создания безопасных ДПАК и систем на основе нейроморфных вычислений и Доверенного ИИ. Разработаны типовые платформенные решения для создания распределенных нейроморфных систем, обладающих повышенной надежностью и устойчивостью. Разработаны прототипы типовых решений с целью применения нейроморфных вычислений в составе	Представлены предложения по требованиям и рекомендации по реализации Доверенных систем и ДПАК на основе Доверенного ИИ и нейроморфных вычислений. Представлены сценарии развития, требования к технологиям и продуктам на основе нейроморфных технологий. Учтены требования рисков и угроз (1.5.2). Разработан прототип ЭКБ и ДПАК с использованием нейроморфных	Минпромторг России РНФ

			Вычислительной Техники, Телеком Оборудования, АСУТП и др Представлены сценарии развития, требования к технологиям и продуктам, предложения по развитию НПА и мер поддержки. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности.	вычислений для обеспечения функций безопасности Представлен ПНСТ. Представлены предложения по развитию НПА и мер поддержки.	
1.5.8 Разработка доверенной защищенной микропроцессорной архитектуры (НИР)	2026	2027	Произведено исследование лучших мировых практик создания защищенных процессорных архитектур. Определены перспективы и сценарии применения методов Конструктивной Безопасности, безопасного жизненного цикла и архитектур безопасности с целью формирования защищенной процессорной архитектуры. Сформирован состав элементов архитектуры, реализующих функции доверия и безопасности, а также защиту информации на этапах обработки, хранения и передачи информации. Сформированы предложения по реализации доверия и безопасности в составе микропроцессорной архитектуры, включая архитектуру приоритетов, защиту памяти, защищенную виртуализацию и защищенный ввод-вывод. Сформированы требования по обеспечению доверия, включая выделение типовых узлов, архитектурные требования, стандартизацию и верификацию. Сформированы предложения по реализации с учетом компоновки системы в корпусе с применением отечественных ИС1 в качестве корня доверия. Проведено исследование необходимого состава интегрированного ПО безопасности. Определен необходимый состав компонент, модулей и СФ-Блоков, реализующих функции безопасности. Проведен форсайт с регуляторами, поставщиками систем и средств защиты информации. Предоставлен отчет.	Разработана процессорная архитектура, позволяющая обеспечить защиту от 80% известных угроз, связанных с использованием уязвимостей организации памяти, побочных каналов, спекулятивным исполнением и др. Учтены требования рисков и угроз (1.5.2), требования реализации отечественной криптографии (1.4.2-1.4.6). Представлены рекомендации и ТЗ на разработку методов создания ДАС, ПО и ДПАК на основе защищенной архитектуры (1.5.9-11). Представлен ПНСТ. Представлены рекомендации по мерам поддержки и НПА.	Минпромторг России, РНФ, Минцифры России

	2027	2028	Создание прототипа ЭКБ на основе защищенной процессорной архитектуры	Создан прототип ЭКБ на основе защищенной процессорной архитектуры	Минпромторг России, ФПИ, Минцифры России
1.5.9 Разработка методов создания ДАС, ПО и ДПАК на основе защищенной архитектуры (НИР)	2027	2028	Проведено исследование лучших практик и сформированы требования к применению интеллектуальных средств валидации и верификации дизайна аппаратных средств. Разработаны требования и рекомендации по применению технологий управления требованиями для разработки безопасного ПО на основе безопасной архитектуры системы на кристалле (далее - СнК). Разработаны требования и рекомендации по применению компиляторных технологий для разработки безопасного ПО на основе безопасной архитектуры СнК. Разработаны требования и рекомендации по применению технологий статического анализа для разработки безопасного ПО на основе безопасной архитектуры СнК. Разработаны требования и рекомендации по применению технологий динамического анализа для разработки безопасного ПО на основе безопасной архитектуры СнК. Разработаны требования и рекомендации по применению средств функционального тестирования для разработки безопасного ПО на основе безопасной архитектуры СнК. Созданы технологии верификации, включая дедуктивную верификацию, динамическую верификацию (run-time verification), проверку моделей (model checking), тестирование на основе формальных моделей, тестирование на основе атрибутов (property-based testing). Созданы инструменты глубокого анализа, включая анализ формальных моделей информационной безопасности, формальной верификации системного ПО с адаптацией к заданной конфигурации аппаратуры.	Разработаны методы создания архитектурные решения, рекомендации и требования к реализации ДАС, ПО и ДПАК на основе защищенной процессорной архитектуры, позволяющие обеспечить защиту от 80% известных угроз информационной и кибербезопасности. Учтены требования рисков и угроз (1.5.2), требования реализации отечественной криптографии (1.4.2-1.4.6), требования к доверенным аппаратным элементам (1.5.3-4), реализации на основе отечественных технологий и микросборок (1.5.5-6) и защищенной архитектуры (1.5.8). Созданы прототипы ДПАК на основе защищенной архитектуры. Представлены сценарии развития, требования к технологиям и продуктам, предложения по развитию НПА и мер поддержки.	Минпромторг России ФПИ, Минцифры России

			Созданы инструменты формальной верификации драйверов устройств с использованием моделей контролируемых устройств. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлен отчет.		
1.5.10 Разработка архитектуры безопасности типовых сетевых ДАС (НИР)	2028	2029	Проведено исследование лучших практик по созданию типовых доверенных аппаратных средств. Определены основные принципы создания типовых ДАС. Разработаны предложения по требованиям и рекомендации по реализации архитектуры безопасности ДАС: - средств однонаправленной передачи информации; - сетевых интерфейсов (адаптеров); - аппаратных платформ межсетевых экранов. Проведен форсайт с регуляторами, поставщиками систем и средств защиты информации. Предоставлен отчет.	Представлены основные принципы создания ДАС. Представлены предложения по требованиям и рекомендации по реализации архитектуры безопасности ДАС. Учтены требования рисков и угроз (1.5.2), требования реализации отечественной криптографии (1.4.2-1.4.6)	Минпромторг России, Минцифры России

1.5.11 Разработка типовых защищенных решений в области ВТ, ТКО, АСУТП, БПЛА и IoT (НИР/НИОКР)	2028	2029	Разработаны типовые защищенные решения в области ВТ на основе методики Конструктивной Безопасности с применением корня доверия, доверенной среды и аппаратно-программный модуля доверия (далее – АПМД). Разработаны типовые защищенные решения с применением модулей управления, доверия и безопасности на основе отечественной ЭКБ (ИС1/2). Реализована защита управляющего трафика с применением отечественной криптографии на основе отечественной ЭК. Разработаны типовые защищенные решения с применением ЭКБ (ИС1/2) на основе защищенной отечественной процессорной архитектуры. Представлены сценарии развития, требования к технологиям и продуктам, предложения по развитию НПА и мер поддержки. Проведен форсайт с регуляторами, ключевыми заказчиками, поставщиками систем и компонент доверия и безопасности. Представлен отчет.	Разработаны типовые защищенные решения в области вычислительной техники на основе методики Конструктивной Безопасности с применением корня доверия, доверенной среды и АПМД, в том числе: - вычислительной техники; - телеком оборудования; - АСУТП; - БПЛА; - IoT /IIoT. Представлен ПНСТ. Представлены рекомендации по мерам поддержки и НПА.	Минпромторг России

3.2. Совершенствование системы образования для обеспечения перспективных кадровых потребностей динамично развивающихся компаний, научных и творческих коллективов, участвующих в создании новых глобальных рынков

Основные направления плана мероприятий ("дорожной карты")	**Срок начала реализации**	**Срок окончания реализации**	**Значимые контрольные результаты реализации плана мероприятий («дорожной карты»)**	**Ожидаемый результат**	**Исполнители**
3.2.1. Формирование академического и исследовательского направления в области Конструктивной Безопасности	2026	2027	Создан академический центр исследования вопросов Конструктивной Безопасности (ИСП РАН)	Создана научная и методическая основа Конструктивной Безопасности	Российская академия наук
	2026	2027	Создан академический центр исследования вопросов киберустойчивости (СПбПУ)	Создана научная и методическая основа киберустойчивости	
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области ЭКБ (МИЭТ)	Создана научная и методическая основа Конструктивной Безопасности в области ЭКБ	
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области процессорных архитектур (НИИСИ)	Создана научная и методическая основа Конструктивной Безопасности в области процессорных архитектур	
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области экосистемы высокоавтоматизированного и беспилотного движения (МАДИ)	Создание научной и методической основы Конструктивной безопасности в области экосистемы высокоавтоматизированного и беспилотного движения	
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области доверенных систем (ТУСУР)		
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области инженерных систем (МГТУ)		

	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в ядерной отрасли (МИФИ)		
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области экосистемы высокоавтоматизированного и беспилотного движения (МАДИ).		
	2026	2027	Создан исследовательский центр по вопросам Конструктивной Безопасности в области беспилотных систем (МФТИ).		
3.2.2. Создание передовой инженерной школы (далее - ПИШ) по Конструктивной Безопасности	2026	2026	Сформированы требования к ПИШ по Конструктивной Безопасности.	Подготовлены аналитический отчет, требования к ПИШ и образовательным программам.	Минобрнауки России
	2026	2027	Проведен конкурс на ПИШ по Конструктивной Безопасности.	Подготовлен отчет о проведении конкурса.	
	2026	2027	Сформированы дисциплины курсы ПИШ по Конструктивной Безопасности.	Разработана номенклатура дисциплин и курсов ПИШ по Конструктивной Безопасности.	
	2026	2027	Сформирован финансовый план ПИШ по Конструктивной Безопасности.	Подготовлен финансовый план ПИШ по Конструктивной Безопасности.	
	2026	2027	Получено финансирование на ПИШ по Конструктивной Безопасности.		
	2026	2027	Запущен ПИШ по Конструктивной Безопасности.		
3.2.3. Создание системы профессиональных стандартов, подготовки и повышения квалификации кадров в области	2026	2027	Проведен анализ количественных и качественных потребностей рынка в специалистах Конструктивной Безопасности.	Выполнен Форсайт. Подготовлен аналитический отчет.	Минобрнауки России
			Сформированы требования к специальностям в области Конструктивной Безопасности.		
			Сформированы требования к системе подготовки специалистов в области Конструктивной Безопасности.		
			Сформированы требования к системе повышения квалификации в области Конструктивной Безопасности.		
			Сформированы требования к преподавателям в области Конструктивной Безопасности.		

Конструктивной Безопасности			Созданы отраслевые и технологические центры компетенций по Конструктивной Безопасности.		
			Произведен пилотный запуск программы подготовки и повышения квалификации в области Конструктивной Безопасности.		
			Подготовлен анализ результатов пилотного запуска программы.		
			Запущена программа подготовки и повышения квалификации в области Конструктивной Безопасности.		

3.3. Развитие системы профессиональных сообществ и популяризация Национальной технологической инициативы

Основные направления плана мероприятий ("дорожной карты")	Срок начала реализации	Срок окончания реализации	Значимые контрольные результаты реализации плана мероприятий («дорожной карты»)	Ожидаемый результат	Исполнители
3.1 Формирование профессионального сообщества в области Конструктивной Безопасности	2026	2026	Запущен Инфраструктурный центр «Сейфнет»	Создан центр экспертизы для развития профессионального сообщества и популяризации Конструктивной Безопасности.	АНО «Платформа НТИ»
	2026	2027	Проведены Форсайты, семинары, профессиональные мероприятия на основе ИЦ	Определены требования к квалификации, образованию и профессиям. Определение лучших практик, опыта пилотных внедрений, разработка методик, архитектурных рекомендаций.	
	2026	2030	Проведены Форсайты, семинары, профессиональные мероприятия на основе ИЦ	Проведены онлайновые и очные мероприятия для популяризации Конструктивной Безопасности.	
3.2 Создание системы стандартов сквозных технологий доверия и безопасности	2026	2026	Разработана и представлена Дорожная карта стандартов и НПА	Сформированы предложения по системе стандартов в области Конструктивной Безопасности, безопасного жизненного цикла, архитектур на основе политик безопасности и др.	АНО «Платформа НТИ»
	2026	2027	Разработан ПНСТ и внесен в Росстандарт.	Публикации, ПНСТ	
	2027	2028	Разработана Дорожная карта реализации стандартов.	Разработаны прототипы и запущены пилотные проекты на основе предстандартов.	

	2028	2030		Введена единая система стандартов Конструктивной Безопасности	
3.3 Популяризация НТИ и дорожной карты «Сейфнет»	2026	2027	Проведены мероприятия в области КИИ, ИБ, ИТ и высокотехнологичных отраслях, в том числе мероприятия в рамках проектно-образовательного интенсива «Архипелаг».	Произведена популяризация дорожной карты «Сейфнет»	АНО «Платформа НТИ», «Университет 2035», Фонд НТИ
	2026	2027	Проведены совместные мероприятия с другими дорожными картами.	Построены совместные планы с другими дорожными картами НТИ.	
	2027	2030	Разработана дорожная карта, проведены международные мероприятия.	Сформированы планы по выводу Конструктивной Безопасности на зарубежные рынки, в первую очередь – в страны БРИКС	
3.4. Проведение технологического конкурса по преодолению технологических барьеров в области Конструктивной Безопасности	2026	2027	Проведен технологический конкурс по преодолению технологических барьеров в области Конструктивной Безопасности с целью поиска новых технологических команд и решений	Найдены технологические решения, направленные на преодоление технологических барьеров в области Конструктивной Безопасности.	Фонд НТИ, АНО «Платформа НТИ»

3.4.Организационно-техническая и экспертно-аналитическая поддержка, информационное обеспечение Национальной технологической инициативы

Мероприятия по организационно-технической и экспертно-аналитической поддержке будут определены в программе деятельности Инфраструктурного центра «Сейфнет» НТИ.

3.5.Создание механизмов акселерации компаний Национальной технологической инициативы и механизмов экспортного продвижения создаваемых продуктов

Мероприятия по акселерации перспективных проектов и технологий для основных направлений плана мероприятий («дорожной карты») «Сейфнет» НТИ будут определены в программе деятельности Инфраструктурного центра «Сейфнет» НТИ.

4. Ожидаемые социально-экономические эффекты от реализации плана мероприятий («дорожной карты») в среднесрочном и долгосрочном периодах

- Повышение технологической устойчивости объектов КИИ, предоставляющих товары и услуги первой необходимости, от которых зависят жизнь и здоровье людей, с учетом растущих угроз информационной и кибербезопасности;
- формирование нового высокотехнологичного сектора экономики, ориентированного на создание сквозных технологий доверия и безопасности на основе передовой школы отечественной информационной и кибербезопасности;
- создание новых типов товаров и услуг, реализуемых с помощью новых типов критической информационной инфраструктуры и требующих высокого уровня информационной и кибербезопасности;
- снижение зависимости от зарубежных высокотехнологических продуктов и технологий, подверженных санкционным ограничениям и потенциально содержащих недокументированные возможности, в первую очередь – в области информационной и кибербезопасности;
- формирование новых производственных цепочек, обеспечивающих спрос на отечественные технологии и обеспечивающие рост высокотехнологичного сегмента отечественной экономики;
- увеличение экспортного потенциала российских высокотехнологических продуктов за рубежом, развитие зарубежных рынков сбыта;

- увеличение количества высококвалифицированных специалистов в области информационной и кибербезопасности, безопасной разработки;
- повышение уровня занятости населения за счет создания рабочих мест в высокотехнологичных отраслях, расширения дистанционных форм совместной деятельности, увеличение трудоспособного возраста за счет достижений в области технологий информационной и кибербезопасности.

Меры по совершенствованию технического регулирования в целях обеспечения реализации плана мероприятий («дорожной карты»):

- развитие нормативной базы Конструктивной Безопасности – ПНСТ в рамках ТК-362, отраслевые ПНСТ;
- развитие нормативной базы безопасного жизненного цикла – ПНСТ в рамках технического комитета по стандартизации «Защита информации» (ТК-362), технического комитета по стандартизации «Программно-аппаратные комплексы для критической информационной инфраструктуры и программное обеспечение для них» (ТК-167), иных отраслевых технических комитетов по стандартизациии др.;
- развитие нормативной базы защищенных решений в области радиоэлектронного оборудования и ЭКБ;
- создание стандартов национальных процессорных архитектур и интегрированных средств безопасности.

5. Документы стратегического планирования, относящихся к категории разрабатываемых на федеральном уровне, по отраслевому и территориальному принципу, а также в рамках прогнозирования, положения которых учтены при разработке плана мероприятий («дорожной карты»)

- Указ Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 № 250;
- Указ Президента Российской Федерации «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30.03.2022 № 166;
- Указ Президента Российской Федерации «Об Основах государственной политики в области обеспечения технологической независимости критической информационной инфраструктуры Российской Федерации на период до 2030 года» от 29.10.2024 г. № 927;
- Национальный проект «Национальная программа «Цифровая экономика Российской Федерации»;
- Национальный проект «Экономика данных и цифровая трансформация государства»;
- Государственная программа «Развитие электронной и радиоэлектронной промышленности» (утвержден решением Правительства Российской Федерации – протокол от 24.09.2025 № 32).