

ПАСПОРТ
федерального проекта "Информационная безопасность"
национальной программы "Цифровая экономика Российской Федерации"

1. Решение об утверждении федерального проекта, дата и номер *Указывается после утверждения федерального проекта*
2. Федеральный орган исполнительной власти, ответственный за реализацию федерального проекта
Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
3. Должностное лицо федерального органа исполнительной власти, ответственное за реализацию федерального проекта
А.В. Соколов, заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации
4. Соисполнители - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и иные организации, участвующие в реализации федерального проекта
Банк России, МВД России, МИД России, Минкомсвязь России, Минобороны России, Минобрнауки России, Минпромторг России, Минпросвещения России, Минстрой России, Минтранс России, Минтруд России, Минфин России, Минэкономразвития России, Минэнерго России, Минюст России, МЧС России, Росгвардия, Роскомнадзор, Роспатент, Росстандарт, ФАС России, ФНС России, ФСБ России, ФСО России, ФСТЭК России, Академия криптографии Российской Федерации, АНО «Центр компетенций по импортозамещению в сфере ИКТ», АНО «Цифровая экономика», АО «Российская венчурная компания», АО «Российский экспортный центр», АО «Российское агентство по страхованию экспортных кредитов и инвестиций», АО «Смартс», АО «Альфа-Банк», АО «Газпромбанк», АО «Лаборатория Касперского», АО «НПО РусБИТех», АО НСПК, АРПП «Отечественный софт», Ассоциация банков России, Ассоциация разработчиков программных продуктов, Всероссийский Союз Страховщиков, ГК «Внешэкономбанк», Госзнак, ИТМО, МОО «Ассоциация Защиты Информации», Московский Государственный Университет, ОАО «РЖД», ОГО «Ассоциация документальной электросвязи», ООО «АльтЭль», ООО «ВЭБ Инновации», ООО «Группа АЙБи ТДС», ООО «Бизон», ООО «МастерКард», ООО «Платежная система «Виза», Организации-члены ТК122, ПАО «ГИПРОСВЯЗЬ», ПАО «Ростелеком», ПАО «Сбербанк», ПАО «Банк ВТБ», РТУ МИРЭА, ФГБУ «ВНИИ труда» Минтруда России, ФГБУ НИИ Восход, ФГУП «Российская телевизионная и радиовещательная сеть», Фонд «Сколково», Фонд развития интернет-инициатив (ФРИИ), Фонд развития промышленности, Фонд содействия развитию малых форм предприятий в научно-технической сфере, ФУМО ВО ИБ, ФУМО СПО ИБ, АНО «Агентство стратегических инициатив по продвижению новых проектов»
5. Рабочие группы
Рабочая группа федерального проекта "Информационная безопасность" национальной программы "Цифровая экономика Российской Федерации", руководитель - Касперская Наталья Ивановна, генеральный директор группы компаний АО "ИнфоВотч"
6. Центры компетенций
Центр компетенций федерального проекта "Информационная безопасность" национальной программы "Цифровая экономика Российской Федерации", Кузнецов Станислав Константинович, заместитель председателя правления ПАО "Сбербанк России"
7. Цели федерального проекта
1. Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом.
2. Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств.
3. Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями

	<p>Объем затрат на продукты и услуги в области информационной безопасности (млрд руб.)*</p> <p>Средний срок простоя государственных информационных систем в результате компьютерных атак, часов</p> <p>Доля населения, использовавшего отечественные средства защиты информации по субъектам Российской Федерации (в процентах от общей численности населения, использовавшего сеть "Интернет" в течение последних 12 месяцев, соответствующего субъекта)</p> <p>Количество подготовленных специалистов по образовательным программам в области информационной безопасности, с использованием в образовательном процессе отечественных высокотехнологичных комплексов и средств защиты информации, тыс. чел.</p> <p>Стоимостная доля закупаемого и (или) арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов и иными органами государственной власти отечественного программного обеспечения, проценты</p> <p>Стоимостная доля закупаемого и (или) арендуемого государственными корпорациями, компаниями с государственным участием отечественного программного обеспечения, проценты**</p>
8. Показатели и индикаторы федерального проекта	
9. Значимые контрольные результаты реализации федерального проекта на первый плановый год	<p>05.01.001.002 Разработана система мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов за рубежом</p> <p>05.02.001.002 Определены методики оценки показателей информационной безопасности на сетях связи общего пользования (включая российский сегмент сети "Интернет"), их текущие и целевые значения</p> <p>05.02.001.003 Приняты подзаконные акты, устанавливающие требования к проектированию, управлению и эксплуатации сетей связи общего пользования с учетом рисков и угроз информационной безопасности</p> <p>05.03.001.008 Законодательно установлены требования к использованию отечественного компьютерного, серверного и телекоммуникационного оборудования на объектах инфраструктуры обработки данных</p> <p>05.03.001.009 Создана система стимулов для развития отечественных организаций, обеспечивающих потребности отраслей экономики в электронной компонентной базе, и использования отечественных комплектующих компаниями-производителями компьютерного, серверного и телекоммуникационного оборудования</p> <p>05.03.001.010 Создана система стимулов для приобретения и использования компьютерного, серверного и телекоммуникационного оборудования отечественного производства</p> <p>05.03.001.011 Созданы механизмы стимулирования разработки отечественного программного обеспечения и увеличения его доли в условиях цифровой экономики с помощью акселерации перспективных бизнес идей, венчурного финансирования, льготного кредитования, премирования за найденные уязвимости</p>
10. Ожидаемые результаты на год окончания периода реализации федерального проекта	<p>05.01.001.003 Созданы и функционируют механизмы информационно-аналитического обеспечения и координации участия российских экспертов в деятельности основных международных организаций, осуществляющих разработку стандартов в области криптографии и безопасности информационных технологий</p> <p>05.02.001.005 Обеспечена целостность, устойчивость и безопасность функционирования российского сегмента сети "Интернет"</p> <p>05.02.001.012 Обеспечена информационная безопасность функционирования отечественной инфраструктуры телерадиовещания</p> <p>05.02.001.015 Создана защищенная цифровая среда взаимодействия двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 для нужд МВД России, МЧС России, Росгвардии</p> <p>05.02.002.003 Разработаны требования к операторам промышленного Интернета, требования и методики проверки киберфизических систем, проекты стандартов безопасности для киберфизических систем, включая "Интернет вещей"</p> <p>05.02.002.005 Разработаны технологические решения и реализованы пилотные проекты с использованием технологий распределённых реестров, внедрением методов и технологий искусственного интеллекта анализа данных, а также "Интернета вещей"</p> <p>05.02.002.006 Обеспечено развитие перспективных технологий идентификации участников информационного взаимодействия, включая технологии биометрической идентификации, многофакторной идентификации, методов криптографической аутентификации и иных технологий идентификации</p> <p>05.02.002.009 Создан специализированный ресурс, предназначенный для взаимодействия с уполномоченными органами в части оперативной передачи данных о признаках противоправных действий в области информационных технологий (компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем) в целях противодействия компьютерной преступности, в том числе в финансовой сфере, а также иных случаев криминального и противоправного использования информационных технологий</p> <p>05.02.002.010 Создан прототип общедоступного антивирусного мультисканера для проверки на наличие признаков вредоносной активности, определены необходимые ресурсы</p> <p>05.02.002.011 Введена в эксплуатацию система фильтрации интернет-трафика при использовании информационных ресурсов детьми</p>

05.02.002.013 Создан специализированный ресурс, обеспечивающий гражданам России доступ к информации о случаях использования их персональных данных, а также возможность отказа от такого использования

05.02.002.014 Разработаны предложения по популяризации добровольного страхования рисков ИБ и повышению киберкультуры

05.02.002.016 Сформированы условия для эффективного применения шифровальных (криптографических) средств защиты информации в условиях цифровой экономики

05.02.002.017 Обеспечено развитие значимых платежных систем и обеспечение их информационной безопасности, в том числе в части использования в них российских криптографических средств.

05.02.002.020 Система профессионального образования в области информационной безопасности работает в объеме достаточном для нужд рынков цифровой экономики.

05.03.001.001 Обеспечено функционирование Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий

05.03.001.004 Обеспечена информационная безопасность национальных волоконно-оптических сетей связи с применением квантовых технологий

05.03.001.009 Создана система стимулов для развития отечественных организаций, обеспечивающих потребности отраслей экономики в электронной компонентной базе, и использования отечественных комплектующих компаниями-производителями компьютерного, серверного и телекоммуникационного оборудования

11. Объемы и источники финансирования

Ассигнования федерального бюджета в размере 15 286,5 млн рублей, в том числе:

в 2018 году - 363,00 млн рублей;

в 2019 году - 4 815,3 млн рублей;

в 2020 году - 5 568,8 млн рублей;

в 2021 году - 4 902,4 млн рублей;

Внебюджетные средства в размере 12 636,4 млн рублей, в том числе:

в 2018 году - 21,96 млн рублей;

в 2019 году - 2832,0 млн рублей;

в 2020 году - 4104,7 млн рублей

в 2021 году - 5677,8 млн рублей

Общий объем необходимого финансирования в размере 27 922,9 млн рублей

**ПЛАН ДОСТИЖЕНИЯ ПОКАЗАТЕЛЕЙ И ИНДИКАТОРОВ
федерального проекта "Информационная безопасность"**

№ п/п	Наименование показателей и индикаторов, единица измерения	2017 год	2018 год	2019 год	2020 год	2021 год	2022 год	2023 год	2024 год
05.01. Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом									
1.	Объем затрат на продукты и услуги в области информационной безопасности (млрд руб.)*	-	56,00	67,20	80,64	96,77	116,12	139,35	167,22
05.02. Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств									
2.	Средний срок простоя государственных информационных систем в результате компьютерных атак, часов	-	65	48	24	18	12	6	1
3.	Доля населения, использовавшего отечественные средства защиты информации по субъектам Российской Федерации (в процентах от общей численности населения, использовавшего сеть "Интернет" в течение последних 12 месяцев, соответствующего субъекта)	-	86	87	88	89	90	95	97
4.	Количество подготовленных специалистов по образовательным программам в области информационной безопасности, с использованием в образовательном процессе отечественных высокотехнологичных комплексов и средств защиты информации, тыс. чел.	-	7	8,40	10,08	12,10	14,52	17,42	20,90
05.03. Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями									
5.	Стоимостная доля закупаемого и (или) арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов и иными органами государственной власти отечественного программного обеспечения, проценты	-	>50	>60	>70	>75	>80	>85	>90
6.	Стоимостная доля закупаемого и (или) арендуемого государственными корпорациями, компаниями с государственным участием отечественного программного обеспечения, проценты**	-	>40	>45	>50	>55	>60	>65	>70

* - В настоящее время отсутствует методология сбора и расчета внутренних затрат на развитие цифровой экономики. Федеральным проектом «Цифровое государственное управление» предусмотрены мероприятия по разработке методологии статистических наблюдений и организации измерения параметров развития цифровой экономики, включая эффекты цифровой трансформации отраслей экономики и социальной сферы со сроком исполнения до 31 декабря 2019 года.

** - базовое значение рассчитано на основе экспертных оценок. Предполагается уточнение показателя, в том числе базового значения 2017 года, по итогам завершения методологических работ в 2019 году.

ПЛАН МЕРОПРИЯТИЙ
федерального проекта "Информационная безопасность"

№	Цель	Задача	Веха	Наименование мероприятия	Срок исполнения		Ответственные исполнители		Контрольные события	
					Начало	Конец	ФОИВ	Организации - исполнители		
05.01	Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом									
05.01.001	Созданы условия для глобальной конкурентоспособности в области экспорта отечественных разработок и технологий обеспечения безопасности информации									
05.01.001.001.001				Разработка предложений по продвижению отечественных решений в области информационной безопасности за рубежом	02.2019	06.2019	Минкомсвязь России, Минэкономразвития России, Минпромторг России	АО "Российский экспортный центр", Ассоциация разработчиков программных продуктов	Утверждены предложения.	
05.01.001.001				Разработаны предложения по продвижению отечественных решений в области информационной безопасности за рубежом		06.2019				
				Ожидаемые результаты: 1. Предложения по продвижению отечественных решений в области информационной безопасности за рубежом одобрены.						
05.01.001.002.001				Разработка системы мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов за рубежом	02.2019	12.2021	Минкомсвязь России, Роспатент, Банк России	АО "Российский экспортный центр", ЦК "Цифровые технологии"	Утвержден ежегодный отчет (за 2019, 2020, 2021 гг.) о разработанной системе мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов за рубежом.	
05.01.001.002.002				Осуществляется поддержка экспортно-ориентированных разработчиков программного обеспечения.	06.2019	12.2021	Минкомсвязь России	АО "Российское агентство по страхованию экспортных кредитов и инвестиций"	Утвержден ежегодный отчет (за 2019, 2020, 2021 гг.) об осуществлении стимулирования разработки отечественного программного обеспечения и увеличения его доли в условиях цифровой экономики.	
05.01.001.002				Разработана система мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов за рубежом		12.2021				
				Ожидаемые результаты: 1. Определена система мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов за рубежом. 2. Осуществляется стимулирование разработки отечественного программного обеспечения 3. Увеличена доля отечественного программного обеспечения в условиях цифровой экономики.						
05.01.001.003.001				Создание в Академии криптографии Российской Федерации специализированного подразделения, осуществляющего информационно-аналитическое обеспечение и координацию участия российских экспертов в деятельности основных международных организаций, осуществляющих разработку стандартов в области криптографии и безопасности информационных технологий	01.2019	12.2019	ФСБ России, Росстандарт	Академия криптографии Российской Федерации	Утверждены документы, определяющие задачи, функции, обязанности, права, организационно-штатную структуру и ресурсное обеспечение деятельности подразделения, а также (при необходимости) изменения нормативной базы органов исполнительной власти Российской Федерации, обеспечивающие его создание и функционирование.	
05.01.001.003.002				Обеспечение непрерывного и скоординированного участия российских экспертов в деятельности основных международных организаций, осуществляющих разработку стандартов в области криптографии и безопасности информационных технологий.	01.2019	12.2021	ФСБ России, Минкомсвязь России, ФСТЭК России, Росстандарт	Академия криптографии Российской Федерации	Академией криптографии Российской Федерации утвержден ежегодный план работ специализированного подразделения и ежегодный отчет о его реализации.	
05.01.001.003				Созданы и функционируют механизмы информационно-аналитического обеспечения и координации участия российских экспертов в деятельности основных международных организаций, осуществляющих разработку стандартов в области криптографии и безопасности информационных технологий		12.2021				

		Ожидаемые результаты: 1. Международные стандарты (проекты стандартов) в области криптографии и безопасности информационных технологий, оказывающие влияние на информационную безопасность Российской Федерации, разрабатываются с учетом национальных интересов Российской Федерации в информационной сфере.						
05.01.001.004.001		Подготовлены проекты нормативных актов, направленные на обеспечение использования сети "Интернет" для устойчивого развития экономики, включающие вопросы юрисдикции и определения субъектов правоотношений при использовании сети "Интернет", на основе равноправного участия членов мирового сообщества в управлении глобальной информационной сетью и ее ресурсами с учетом уникальности данной сферы. Определен перечень международных организаций.	02.2020	12.2021	Минкомсвязь России, МИД России	ОГО "Ассоциация документальной электросвязи"	Утвержден перечень международных организаций. Проекты нормативных актов внесены в международные организации.	
05.01.001.004.002		Проведен анализ текущего и проектирование целевого состояния международной нормативной базы, направленные на обеспечение использования сети "Интернет" для устойчивого развития экономики, включающие вопросы юрисдикции и определения субъектов правоотношений при использовании сети "Интернет", на основе равноправного участия членов мирового сообщества в управлении глобальной информационной сетью и ее ресурсами с учетом уникальности данной сферы	02.2020	12.2021	Минкомсвязь России		Утвержден отчет.	
05.01.001.004.003		Организация на постоянной основе мониторинга и анализа политики зарубежных стран в сфере сетевой и информационной безопасности	02.2019	12.2021	Минкомсвязь России		Утвержден ежегодный отчет	
05.01.001.004		В международные организации внесены проекты нормативных актов, направленные на обеспечение использования сети "Интернет" для устойчивого развития экономики, включающие вопросы юрисдикции и определения субъектов правоотношений при использовании сети "Интернет", на основе равноправного участия членов мирового сообщества в управлении глобальной информационной сетью и ее ресурсами с учетом уникальности данной сферы		12.2021				
		Ожидаемые результаты: 1. Определен перечень международных организаций, в которые необходимо внести проекты нормативных актов, направленных на обеспечение использования сети "Интернет" для устойчивого развития экономики, включающих вопросы юрисдикции и определения субъектов правоотношений при использовании сети "Интернет", на основе равноправного участия членов мирового сообщества в управлении глобальной информационной сетью и ее ресурсами с учетом уникальности данной сферы. 2. В международные организации внесены проекты нормативных актов. 3. Сормирована и на постоянной основе актуализируется информационно-правовая база, содержащая сведения о политике зарубежных стран в сфере сетевой и информационной безопасности						
05.01.001.005.001		Разработка методик расчета показателей и индикаторов	02.2019	12.2019	Минкомсвязь России		Методики утверждены.	
05.01.001.005		Разработка методик расчета показателей и индикаторов по федеральному проекту "Информационная безопасность"		12.2019				
		Ожидаемые результаты: 1. Разработаны и утверждены методики расчета показателей и индикаторов. Методики используются для анализа достижения показателей при реализации мероприятий Национальной программы "Цифровая экономика Российской Федерации"						
05.02	Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств							
05.02.001	Обеспечена устойчивость и безопасность функционирования информационной инфраструктуры и сервисов передачи, обработки и хранения данных							
05.02.001.001.001		Проведение исследования по теме: "Анализ устойчивости, рисков и угроз безопасного функционирования ЕСЭ Российской Федерации, в том числе системы управления ЕСЭ и оценка адекватности им существующих стандартов информационной безопасности"	10.2018	03.2019	Минкомсвязь России, ФСБ России, ФСО России, Роскомнадзор	ПАО "ГИПРОСВЯЗЬ", АО "КОНЦЕРН "АВТОМАТИКА"	Подписан акт об оказанных услугах.	
05.02.001.001		Проведен анализ устойчивости, рисков и угроз безопасного функционирования единой сети электросвязи Российской Федерации (далее - ЕСЭ), в том числе функционированию и взаимодействию центров и систем управления сетями связи ЕСЭ, и оценка адекватности им существующих стандартов информационной безопасности		03.2019				

		Ожидаемые результаты: 1. Определены факторы, влияющие на устойчивость и безопасность функционирования ЕСЭ РФ в условиях современного технологического развития инфраструктуры сетей электросвязи. 2. Разработаны подходы к формированию единой отраслевой модели угроз и нарушителя для сетей электросвязи, функционирующих в составе ЕСЭ Российской Федерации. 3. Подготовлены предложения по внесению изменений в нормативные правовые акты и национальные стандарты Российской Федерации с учетом обеспечения их соответствия актуальным рискам нарушения устойчивости и безопасности функционирования ЕСЭ Российской Федерации.					
05.02.001.002.001		Проведение исследования по разработке перечня показателей устойчивости, информационной безопасности сетей связи общего пользования и методов их измерения	02.2019	08.2019	Минкомсвязь России, ФСБ России	ПАО "ГИПРОСВЯЗЬ"	Подписан акт об оказанных услугах.
05.02.001.002		Определены методики оценки показателей информационной безопасности на сетях связи общего пользования (включая российский сегмент сети "Интернет"), их текущие и целевые значения		08.2019			
		Ожидаемые результаты: 1. Разработана система целевых показателей и индикаторов устойчивости, информационной безопасности сетей связи общего пользования. 2. Разработан инструментарий для оценки и мониторинга текущих значений целевых показателей и индикаторов устойчивости, информационной безопасности сетей связи общего пользования. 3. Разработаны системные, организационные и технические меры обеспечения автоматизированного мониторинга значений целевых показателей и индикаторов устойчивости, информационной безопасности сетей связи общего пользования.					
05.02.001.003.001		Проведение исследования по теме: "Разработка требований к проектированию, управлению и эксплуатации сетей связи общего пользования с учетом рисков и угроз информационной безопасности"	02.2019	09.2019	Минкомсвязь России	ПАО "ГИПРОСВЯЗЬ"	Подписан акт об оказанных услугах.
05.02.001.003.002		Разработка и принятие отраслевых нормативных правовых актов по результатам исследования по теме: "Разработка требований к проектированию, управлению и эксплуатации сетей связи общего пользования с учетом рисков и угроз информационной безопасности"	09.2019	12.2019	Минкомсвязь России, ФСБ России	ПАО "Ростелеком", Фонд "Сколково", ПАО "ГИПРОСВЯЗЬ"	Утверждены отраслевые нормативные правовые акты.
05.02.001.003		Приняты подзаконные акты, устанавливающие требования к проектированию, управлению и эксплуатации сетей связи общего пользования с учетом рисков и угроз информационной безопасности		12.2019			
		Ожидаемые результаты: 1. Разработаны и приняты на законодательном уровне целевые меры и требования по обеспечению устойчивости и безопасности сетей связи общего пользования в части: - управления средствами связи; - организационно-технического обеспечения устойчивого функционирования сетей связи, в том числе в чрезвычайных ситуациях; - защиты сетей связи от несанкционированного доступа к ним и передаваемой по ним информации; - порядка ввода сетей связи в эксплуатацию; - организационно-технического обеспечения устойчивого функционирования сетей связи в интересах критической информационной инфраструктуры.					
05.02.001.004.001		Проведение исследования по теме: "План разработки стандартов обеспечения информационной безопасности сетей связи общего пользования"	10.2018	03.2019	Минкомсвязь России, Росстандарт	ПАО "ГИПРОСВЯЗЬ", АО "КОНЦЕРН "АВТОМАТИКА"	Подписан акт об оказанных услугах.
05.02.001.004.002		Проведение исследования по теме: "Разработка комплекса стандартов обеспечения информационной безопасности сетей связи общего пользования, обеспечивающих минимизацию рисков и угроз безопасного функционирования сетей связи общего пользования"	02.2019	02.2020	Минкомсвязь России	ПАО "ГИПРОСВЯЗЬ", АО "КОНЦЕРН "АВТОМАТИКА"	Подписан акт об оказанных услугах.
05.02.001.004.003		Разработка и принятие отраслевого нормативного правового акта по результатам исследования по теме: "Разработка комплекса стандартов обеспечения информационной безопасности сетей связи общего пользования, обеспечивающих минимизацию рисков и угроз безопасного функционирования сетей связи общего пользования"	02.2020	12.2021	Минкомсвязь России		Утвержден отраслевой нормативный правовой акт.
05.02.001.004		Разработан и принят комплекс стандартов информационной безопасности, обеспечивающий минимизацию рисков и угроз безопасного функционирования сетей связи общего пользования		12.2021			

			Ожидаемые результаты: 1. Разработаны и приняты национальные стандарты обеспечения информационной безопасности сетей связи общего пользования, обеспечивающие минимизацию рисков и угроз безопасного функционирования сетей связи общего пользования. 2. Разработана система оценки соответствия и механизмов контроля соответствия операторов связи требованиям национальных стандартов обеспечения информационной безопасности сетей связи общего пользования. 3. Принят нормативный отраслевой правовой акт, обязывающий операторов связи выполнять комплекс стандартов информационной безопасности, обеспечивающих минимизацию рисков и угроз безопасного функционирования сетей связи общего пользования						
05.02.001.005.001			Разработка нормативных правовых актов обеспечивающих регулирование вопросов целостного, устойчивого и безопасного функционирования российского сегмента сети Интернет	10.2018	12.2019	Минкомсвязь России			Приняты изменения в Федеральный закон от 07.07.2003 № 126-ФЗ "О связи" и иные федеральные законы
05.02.001.005.002			Разработка программно-технических средств, обеспечивающих сбор и хранение информации об адресах, номерах автономных систем и связей между ними	10.2018	12.2019	Роскомнадзор	ПАО «Ростелеком»		Представлен в Роскомнадзор отчет ПАО «Ростелеком» о реализации программно-технических средств по обеспечению сбора и хранения информации об адресах, номерах автономных систем и связей между ними и обеспечению доступа к этим средствам Роскомнадзора. Размещен в системе электронного взаимодействия участников реализации национальной программы «Цифровая экономика Российской Федерации»
05.02.001.005.003			Разработка программно-аппаратных средств, обеспечивающих мониторинг маршрутов трафика в сети Интернет	02.2019	12.2019	Роскомнадзор	ГРЧЦ		Подписан акт ввода в эксплуатацию
05.02.001.005.004			Разработка программно-аппаратных средств, обеспечивающих устойчивое и безопасное функционирование системы доменных имен	02.2019	02.2020	Роскомнадзор	ПАО «Ростелеком»		Представлен в Роскомнадзор отчет ПАО «Ростелеком» о реализации программно-аппаратных средств по обеспечению устойчивого и безопасного функционирования системы доменных имен в национальном сегменте сети Интернет. Размещен в системе электронного взаимодействия участников реализации национальной программы «Цифровая экономика Российской Федерации»
05.02.001.005.005			Приобретение программно-аппаратных средств обеспечивающих безопасность российского сегмента сети Интернет	01.2019	12.2019	Роскомнадзор	ГРЧЦ		Подписан Акт ввода в эксплуатацию
05.02.001.005.006			Разработка программно-аппаратных средств, обеспечивающих мониторинг и управление сетью связи общего пользования	10.2019	10.2020	Роскомнадзор	ГРЧЦ		Подписан Акт ввода в эксплуатацию
05.02.001.005.007			Обеспечение сбора информации об адресах, номерах автономных систем и связей между ними, маршрутов трафика в сети Интернет, а также управления программно-техническими средствами, обеспечивающими безопасность российского сегмента сети Интернет	10.2018	10.2020	Роскомнадзор, ФСБ России	ГРЧЦ		Правительством Российской Федерации утверждены изменения в постановление от 14.05.2014 №434 «О радиочастотной службе» о наделении полномочиями по обеспечению сбора информации об адресах, номерах автономных систем, связей между ними, маршрутов трафика в сети Интернет, а также обеспечении мониторинга и управления сетью связи общего пользования (постановление в новой редакции).
05.02.001.005.008			Создание национального удостоверяющего центра, для обеспечения устойчивости взаимодействия устройств в российском сегменте сети "Интернет"	10.2018	12.2020	Минкомсвязь России, ФСБ России	ПАО «Ростелеком»		Подписаны Акты сдачи-приемки работ. Приняты правоустанавливающие документы о создании национального удостоверяющего центра.
05.02.001.005.009			Создание распределенной системы управления и мониторинга информационной безопасности в рамках развития российского государственного сегмента сети "Интернет" (RSNet)	01.2019	12.2021	ФСО России, Минкомсвязь России, ФСБ России	Организации, определенные в соответствии с законодательством Российской Федерации		Подписаны акты о создании отдельных компонентов системы
05.02.001.005.010			Разработка целевых значений информационной безопасности функционирования российского сегмента сети "Интернет" с учетом ранее полученных результатов анализа элементов действующей инфраструктуры российского сегмента сети "Интернет" на территории России, включая существующую схему маршрутизации интернет-трафика, проходящего через сети связи иностранных государств/сети иностранных операторов связи, а также определенных на основе анализа подходов по замыканию сетевого трафика на территорию Российской Федерации.	10.2018	03.2019	Минкомсвязь России, ФСБ России, ФСО России			Утверждены целевые значения информационной безопасности функционирования российского сегмента сети "Интернет"

05.02.001.005.011		Проведение ежегодных учений направленных на обеспечение целостности, устойчивости и безопасности функционирования российского сегмента сети Интернет	01.2019	01.2021	Минкомсвязь России, ФСБ России, ФСТЭК России, Роскомнадзор, ФСО России, Минобороны России, МЧС России		Утвержден ежегодный отчет об устранении угроз, выявленных в ходе учений
05.02.001.005		Обеспечено целостное, устойчивое и безопасное функционирование российского сегмента сети Интернет		12.2021			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Созданы программно-технические средства обеспечивающие устойчивое и безопасное функционирование российского сегмента сети Интернет. 2. Обеспечен доступ к информации об адресах, номерах автономных систем и связей между ними для операторов связи и Роскомнадзора 3. Установлены обязанности и ответственность операторов связи и иных юридических лиц использовать программно-аппаратные средства обеспечивающие устойчивое и безопасное функционирование российского сегмента сети Интернет. 4. Разрешение доменных имен в российском сегменте сети Интернет происходит с использованием разработанных программно-технических средств 5. Маршрутизация российского интернет-трафика осуществляется преимущественно по территории Российской Федерации. 6. Для обеспечения устойчивости функционирования взаимодействия устройств в российском сегменте сети "Интернет" введен в эксплуатацию национальный удостоверяющий центр (НУЦ), оснащенный необходимым оборудованием и обеспечивающий создание сертификатов с использованием российских криптографических стандартов. С целью обеспечения работы центра внесены необходимые изменения в нормативные правовые акты Российской Федерации для обеспечения регламентного использования НУЦ в соответствии с разработанной в 2019 году Концепцией. 7. Проводятся ежегодные учения направленные на обеспечение целостности, устойчивости и безопасности функционирования российского сегмента сети Интернет. 8. При Роскомнадзоре создана необходимая организационная структура, обеспечивающая контроль целостности устойчивости и безопасности функционирования российского сегмента сети Интернет. 9. Создана распределенная система управления и мониторинга информационной безопасности в рамках развития российского государственного сегмента сети "Интернет" (RSNet) 					
05.02.001.006.001		Проведение исследования по анализу элементов действующей инфраструктуры российского сегмента сети Интернет на территории России, а также особенностей пропуска трафика в национальном сегменте сети Интернет с целью определения возможностей замыкания Интернет-трафика внутри российского сегмента сети Интернет и определения ресурсов, необходимых для такого замыкания	10.2018	03.2019	Минкомсвязь России	ПАО "ГИПРОСВЯЗЬ"	Подписан акт об оказанных услугах.
05.02.001.006		Проведен анализ элементов действующей инфраструктуры российского сегмента сети "Интернет" на территории России, включая существующую схему маршрутизации интернет-трафика, определены необходимые ресурсы		03.2019			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Разработаны технические меры, направленные на обеспечение преимущественной маршрутизации внутрироссийского Интернет-трафика в пределах территории Российской Федерации. 					
05.02.001.007.001		Внесение изменений в Федеральный закон от 07.07.2003 №126-ФЗ "О связи" в части введения понятия информационной системы обеспечения целостности, устойчивости и безопасности функционирования российского сегмента сети "Интернет", введения понятийного аппарата терминов и определений информационной безопасности в условиях цифровой экономики, сопровождение обсуждения и обеспечение принятия законопроекта	10.2018	06.2019	Минкомсвязь России		Проект изменений в Федеральный закон от 07.07.2003 № 126-ФЗ "О связи"
05.02.001.007		Законодательно закреплён правовой статус российского сегмента сети "Интернет", его инфраструктуры, порядок ее функционирования		06.2019			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Проект изменений в Федеральный закон от 07.07.2003г. № 126-ФЗ "О связи" внесен в Государственную Думу Федерального Собрания Российской Федерации 					
05.02.001.008.001		Разработка требований к устойчивости и безопасности сетей связи и оборудования органов государственной власти (за исключением высших органов государственной власти) и организаций различных организационно-правовых форм	10.2018	06.2019	Минкомсвязь России, ФСТЭК России, ФСБ России	ПАО "ГИПРОСВЯЗЬ", ФГУП ЦНИИС, Фонд "Сколково"	Утверждены требования к устойчивости и безопасности сетей связи и оборудования органов государственной власти.
05.02.001.008		Законодательно приняты требования к устойчивости и безопасности сетей связи и оборудования органов государственной власти и организаций различных организационно-правовых форм и обеспечен контроль (надзор) за их соблюдением.		06.2019			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Утверждены требования к устойчивости и безопасности сетей связи и оборудования органов государственной власти и организаций различных организационно-правовых форм. 2. Обеспечен контроль за соблюдением требований 					

05.02.001.009.001		Проведение исследований по оценке уязвимости web-приложений, размещенных в российском сегменте сети "Интернет"	10.2018	03.2019	Минкомсвязь России, ФСБ России, ФСТЭК России, ФСО России, Банк России		Подписан Акт выполненных работ.
05.02.001.009.002		Разработка предложений по функционалу, архитектуре, форматам взаимодействия и регламентам обмена данными и функционирования отечественного ресурса проверки угроз уровня web-приложений. Согласование их с головным подразделением ГосСОПКА и Банка данных угроз ФСТЭК России	10.2018	09.2019	Минкомсвязь России, ФСБ России, ФСТЭК России, Банк России		Подписан Акт выполненных работ.
05.02.001.009.003		Разработка отечественного ресурса информирования и проверки угроз уровня web-приложений, согласованный с головным подразделением ГосСОПКА и Банка данных угроз ФСТЭК России	10.2019	12.2020	Минкомсвязь России, Банк России, ФСТЭК России	АО "КОНЦЕРН "АВТОМАТИКА"	Доклад в Президиум Правительственной комиссии по цифровому развитию, использовано информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности.
05.02.001.009.004		Создание корпоративных центров ГосСОПКА, обеспечивающих оказание услуг в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты для физических лиц, индивидуальных предпринимателей и малого бизнеса, в том числе не относящимся к субъектам КИИ.	11.2018	12.2020	ФСБ России, ФСТЭК России, Минкомсвязь России, Минэнерго России, Банк России	ООО «Бизон», ПАО Сбербанк	Подписаны соглашения о взаимодействии с корпоративными центрами ГосСОПКА.
05.02.001.009.005		Создание стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ	02.2019	12.2021	Минкомсвязь России	АО "КОНЦЕРН "АВТОМАТИКА"	Перечень решений сформирован (актуализирован) и утверждён в 2019, 2020, 2021 гг.
05.02.001.009.006		Создание номенклатуры стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ	02.2019	12.2021	Минкомсвязь России	АО "КОНЦЕРН "АВТОМАТИКА"	Номенклатура сформирована (актуализирована) и утверждена в 2019, 2020, 2021 гг.
05.02.001.009.007		Оказание мер финансовой поддержки органам государственной власти субъектов Российской Федерации по реализации требований Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	11.2019	12.2021	Минкомсвязь России		Утвержден ежегодный план по реализации мероприятий в отобранных пилотных субъектах Российской Федерации. Утвержден ежегодный отчет о предоставлении мер финансовой поддержки государственных органов для отобранных пилотных субъектов Российской Федерации.
05.02.001.009		Определение функционала и архитектуры ресурса информирования и проверки угроз уровня web-приложений, создание корпоративных и отраслевых центров ГосСОПКА, оказание мер поддержки органам государственной власти субъектов по реализации требований Федерального закона от 26.07.2017 №187-ФЗ и созданию решений для типовых объектов КИИ		12.2021			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> Создан отечественный ресурс информирования и проверки угроз уровня web-приложений, согласованный с головным подразделением ГосСОПКА и Банка данных угроз ФСТЭК России. Реализована инициатива по формированию системы автоматизированного обмена информацией об киберугрозах. Эффекты от реализации: снижение ущерба для бизнеса от действий киберпреступников; сокращение времени реагирования бизнеса на инциденты кибербезопасности и повышение качества их устранения. Подписаны соглашения о взаимодействии с корпоративными центрами ГосСОПКА. Разработаны и утверждены планы реализации мероприятий финансовой поддержки органам государственной власти субъектов Российской Федерации по реализации требований Федерального закона от 26.07.2017 №187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" и по созданию стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ Утверждена номенклатура стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ Оказана финансовая поддержка органам государственной власти субъектов Российской Федерации по реализации требований №187-ФЗ "О безопасности критической информационной инфраструктуры" в не менее, чем в одном пилотном субъекте. 					
05.02.001.010.001		Регламентирован и организован обмен сведениями о компьютерных инцидентах и угрозах безопасности информации между операторами больших массивов данных и Национальным координационным центром по компьютерным инцидентам (НКЦКИ)	02.2019	03.2020	Минкомсвязь России, ФСБ России, ФСТЭК России, Банк России	АО "КОНЦЕРН "АВТОМАТИКА"	Утверждено заключение по экспертизе результатов проектно-исследовательских работ.
05.02.001.010		Обеспечен обмен сведениями между операторами больших массивов данных и НКЦКИ		03.2020			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> Регламентирован обмен сведениями о компьютерных инцидентах и угрозах безопасности информации Организован обмен сведениями о компьютерных инцидентах и угрозах безопасности информации между операторами больших массивов данных и Национальным координационным центром по компьютерным инцидентам (НКЦКИ). 					
05.02.001.011.001		Анализ перспектив развития информационных систем, выявление потребностей в недостающих средствах защиты информации	02.2019	09.2019	Минкомсвязь России, ФСБ России, ФСТЭК России	АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден отчет.

05.02.001.011.002			Создание независимых центров по техническому тестированию программного и аппаратного обеспечения, в том числе средств обеспечения безопасности информации (за исключением тестирования реализованных в них механизмов защиты информации), позволяющего компаниям получить доступ к аналитической информации и результатам независимого тестирования предлагаемых на рынке решений	02.2019	12.2021	Минкомсвязь России, ФСБ России, МВД России, ФСТЭК России	Фонд "Сколково", АНО «Центр компетенций по импортозамещению в сфере ИКТ», ООО "Бизон", ООО "АльтЭль", АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет о создании независимых центров по техническому тестированию программного и аппаратного обеспечения, включая результаты проделанной ими работы за прошедший период.	
05.02.001.011.003			Разработка отечественных технологических решений, обеспечивающих возможность анализа сетевого трафика и поведенческого анализа, с целью выявления фактов заражения абонентов вредоносными программами и пересылке вредоносных вложений	02.2019	12.2021	Минкомсвязь России	ООО "Группа АйБи ТДС", ПАО "Ростелеком", АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет о технических решениях, включенных за отчетный период в реестр отечественного программного обеспечения.	
05.02.001.011			Проведен анализ существующих и перспективных средств защиты информации, созданы независимые центры технического тестирования программного и аппаратного обеспечения для целей цифровой экономики		12.2021				
			<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Утвержден перечень используемых средств защиты информации 2. Утвержден перечень недостающих средств защиты информации 3. Проведена оценка затрат на средства защиты 4. Функционирует независимый центр тестирования по техническому тестированию программного и аппаратного обеспечения, в том числе средств обеспечения безопасности информации (за исключением тестирования реализованных в них механизмов защиты информации), позволяющий компаниям получить доступ к аналитической информации и результатам независимого тестирования предлагаемых на рынке решений 5. Разработаны отечественные технологические решения, обеспечивающие возможность анализа сетевого трафика и поведенческого анализа, с целью выявления фактов заражения абонентов вредоносными программами и пересылке вредоносных вложений 6. Ведется пилотная эксплуатация отечественных технологических решений на сети ПАО "Ростелеком" 						
05.02.001.012.001			Проведение исследований рынка отечественного оборудования телерадиовещания, определение потребностей российских компаний в сфере телерадиовещания в указанном оборудовании	02.2019	05.2019	Минкомсвязь России, Минпромторг России		Подписан акт	
05.02.001.012.002			Оказание мер стимулирования развития и модернизации отечественного производственного комплекса оборудования в сфере телерадиовещания	06.2019	12.2021	Минкомсвязь России, Минпромторг России		Утвержден ежегодный отчет об оказанных мерах стимулирования развития и модернизации отечественного производственного комплекса оборудования в сфере телерадиовещания	
05.02.001.012.003			Разработка и модернизация программно-аппаратных решений по повышению устойчивости и безопасности функционирования отечественной инфраструктуры телерадиовещания	02.2019	12.2021	Минкомсвязь России, Минпромторг России	АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет о разработанных и модернизированных программно-аппаратных решениях	
05.02.001.012			Развитие отечественной инфраструктуры телерадиовещания и обеспечение безопасности ее функционирования		12.2021				
			<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Определена потребность российских компаний в сфере телерадиовещания в оборудовании (поддерживающим технологию 4K / IP), сформирован перечень отечественных производителей оборудования в сфере телерадиовещания, рассчитан потенциал рынка отечественного оборудования в сфере телерадиовещания на перспективу до 2024 года; 2. Отечественный производственный комплекс оборудования в сфере телерадиовещания модернизирован, потребность российских компаний в сфере телерадиовещания в указанном оборудовании (поддерживающего технологию 4K / IP) удовлетворена; 3. Разработаны и протестированы программно-аппаратные решения по повышению устойчивости и безопасности функционирования отечественной инфраструктуры телерадиовещания 						

05.02.001.013.001		Разработка предложений, направленных на использование отечественных решений в области информационной безопасности по направлению "Умный город"	02.2019	12.2019	Минстрой России, Минкомсвязь России, ФСБ России, Роскомнадзор, МЧС России, Банк России, Минпромторг России	ВЭБ.РФ	Доклад в Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности.
05.02.001.013		Разработаны предложения по продвижению отечественных решений в области информационной безопасности по направлению «Умный город»		12.2019			
		Ожидаемые результаты: 1. Одобрены предложения по продвижению отечественных решений в области информационной безопасности по направлению "Умный город"					
05.02.001.014.001		Разработка стандартов обеспечения информационной безопасности микропроцессорных систем управления, расположенных на транспортных средствах и объектах транспортной инфраструктуры, для автомобильного, железнодорожного и воздушного транспорта	02.2020	12.2021	Минтранс России, Минпромторг России, ФСТЭК России, ФСБ России, Росстандарт	ОАО "РЖД", организация отобранная по конкурсу	Утвержден ежегодный отчет об утвержденных за отчетный период стандартах обеспечения информационной безопасности на транспортных средствах и объектах транспортной инфраструктуры.
05.02.001.014.002		Разработка концепции создания единой среды мониторинга защищенности транспортных средств и грузов от деструктивных воздействий	02.2020	10.2020	Минтранс России	ОАО "РЖД", организация отобранная по конкурсу	Утверждена концепция создания единой среды мониторинга.
05.02.001.014.003		Реализация пилотных проектов в сфере железнодорожного транспорта в рамках разработки концепции создания единой среды мониторинга защищенности транспортных средств и грузов от деструктивных воздействий	11.2020	12.2021	Минтранс России	ОАО "РЖД"	Утвержден отчет о реализации пилотных проектов.
05.02.001.014		Разработаны технологические решения по защите аппаратно-программных комплексов транспортной инфраструктуры		12.2021			
		Ожидаемые результаты: 1. Установлены единые технические требования по обеспечению кибербезопасности микропроцессорных систем управления, учитывающие специфику архитектуры и условий функционирования таких систем, используемых на различных видах транспорта, что позволит сократить временные и финансовые затраты на их разработку и создание. Мероприятие реализуется в целях обеспечения гарантированного уровня защищенности микропроцессорных систем управления при условии соответствия их указанным стандартам. 2. Обеспечен непрерывный процесс мониторинга защищенности транспортных средств и грузов (бортовые датчики/агрегаты, запорно-пломбировочные устройства и другое дооснащаемое оборудование) от деструктивных воздействий (поломка, кража, искажение передаваемых данных и др.) за счет использования средств сбора и передачи телеметрической информации и систем транспортной телематики, что позволит снизить затраты на техническое обслуживание транспортных средств и минимизировать финансовые потери участников перевозочного процесса.					
05.02.001.015.001		Разработка концепции защищенной цифровой среды взаимодействия двойного назначения на базе отечественных технологий для нужд МВД России, МЧС России, Росгвардии	02.2019	07.2019	Минкомсвязь России, Минпромторг России, МВД России, МЧС России, ФСБ России, Росгвардия	ПАО "Ростелеком", ФГУП «Российская телевизионная и радиовещательная сеть», АО "КОНЦЕРН "АВТОМАТИКА"	Утверждена концепция.
05.02.001.015.002		Создание номенклатуры и требований к пользовательскому оборудованию двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 для нужд МВД России, МЧС России, Росгвардии	08.2019	12.2021	Минкомсвязь России, Минпромторг России, МВД России, МЧС России, ФСБ России, Росгвардия	ФГУП «Российская телевизионная и радиовещательная сеть», АО "КОНЦЕРН "АВТОМАТИКА"	Номенклатура и требования сформированы (актуализированы) и утверждены в 2019, 2020, 2021 гг.
05.02.001.015.003		Разработка и реализация мер поддержки потребителей пользовательского оборудования двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 для нужд МВД России, МЧС России, Росгвардии	11.2019	12.2021	Минкомсвязь России, Минпромторг России, МВД России, МЧС России, ФСБ России, Росгвардия	ФГУП «Российская телевизионная и радиовещательная сеть», АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет о мерах поддержки потребителей пользовательского оборудования.
05.02.001.015		Создана защищенная цифровая среда взаимодействия двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 для нужд МВД России, МЧС России, Росгвардии		12.2021			
		Ожидаемые результаты: 1. Разработана концепция защищенной цифровой среды взаимодействия двойного назначения на базе отечественных технологий для нужд МВД России, МЧС России, Росгвардии. Концепция определяет защищенные способы обеспечения связи территорий Российской Федерации, в которых в настоящее время связь отсутствует. Концепция согласована со всеми заинтересованными органами. 2. Утверждены номенклатура и требования к оборудованию двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 3. Приняты и реализуются меры поддержки потребителей пользовательского оборудования двойного назначения на базе отечественных технологий для работы в стандарте LTE-450					
05.02.002		Обеспечена защита прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики					

05.02.002.001.001			Разработка стандартов для обеспечения надлежащего уровня обеспечения безопасности для систем, реализующих облачные, туманные, квантовые технологии, систем дополненной реальности, а также систем, реализующих функционал искусственного интеллекта	03.2019	12.2021	Росстандарт, Минкомсвязь России, ФСБ России, Минпромторг России, Банк России, заинтересованные федеральные органы исполнительной власти	Московский Государственный Университет, Фонд "Сколково"	1. Утверждён ежегодный отчёт. 2. Приказы Росстандарта об утверждении национальных стандартов. 3. Приказ Росстандарта об утверждении Программы национальной стандартизации
05.02.002.001.002			Разработка недостающих/ гармонизация существующих стандартов, определяющих целевое гармонизированное регулирование процессов жизненного цикла разработки программного обеспечения, в которых формируется его качество	03.2019	12.2021	Росстандарт, Минкомсвязь России, ФСБ России, ФСТЭК России, Минпромторг России, Банк России, заинтересованные федеральные органы исполнительной власти	Московский Государственный Университет, Фонд "Сколково"	1. Утверждён ежегодный отчёт. 2. Приказы Росстандарта об утверждении национальных стандартов. 3. Приказ Росстандарта об утверждении Программы национальной стандартизации
05.02.002.001.003			Разработка проектов стандартов по безопасной разработке отечественного программного обеспечения	03.2019	12.2021	Росстандарт, Минкомсвязь России, ФСБ России, ФСТЭК России, Минпромторг России, МЧС России, Банк России, заинтересованные федеральные органы исполнительной власти	Московский Государственный Университет, Фонд "Сколково"	1. Утверждён ежегодный отчёт. 2. Приказы Росстандарта об утверждении национальных стандартов. 3. Приказ Росстандарта об утверждении Программы национальной стандартизации
05.02.002.001.004			Утверждение новых межгосударственных стандартов и изменений в действующие стандарты в сфере информационной безопасности для стран ЕАЭС	03.2019	12.2021	Росстандарт, Минкомсвязь России, ФСБ России, ФСТЭК России, Минпромторг России, Банк России, заинтересованные федеральные органы исполнительной власти	Московский Государственный Университет, Фонд "Сколково"	1. Утверждён ежегодный отчёт. 2. Приказы Росстандарта об утверждении национальных стандартов. 3. Приказ Росстандарта об утверждении Программы национальной стандартизации
05.02.002.001.005			Разработка информационно-справочной системы, позволяющей бизнесу определять свое соответствие требованиям российского и международного законодательства, а также отраслевым, национальным и международным стандартам в области информационной безопасности	02.2019	12.2020	Минкомсвязь России, ФСБ России, МВД России, Банк России	ПАО "Сбербанк", Фонд "Сколково"	Подписан Акт ввода в эксплуатацию.
05.02.002.001.006			Разработка защищенных программно-аппаратных комплексов, реализующих технологии распознавания образов (компьютерного зрения), для использования на беспилотных транспортных средствах	02.2020	12.2021	Минтранс России	ОАО "РЖД", организация отобранная по конкурсу	Подписан акт.
05.02.002.001			Разработаны, приняты, гармонизированы и реализованы стандарты информационной безопасности в системах, реализующих облачные, туманные, квантовые технологии, в системах виртуальной и дополненной реальности, и технологий искусственного интеллекта.		12.2021			

		<p>Ожидаемые результаты:</p> <p>1. Утверждено 20 стандартов в области обеспечения безопасности облачных, туманных, квантовых технологий, систем дополненной реальности, а также систем, реализующих функционал искусственного интеллекта. Расширены возможности для использования российских технологических разработок и спектра их применения – уровень безопасности комплексных систем поднят на принципиально иной уровень.</p> <p>2. Утверждено 10 стандартов, определяющих целевое гармонизированное регулирование процессов жизненного цикла разработки программного обеспечения. Сформирован пул стандартов для реализации единой технической политики в части разработки программного обеспечения. Обеспечена взаимозаменяемость установленных стандартами технических решений для всего жизненного цикла программного обеспечения. Снижена себестоимость разработки за счет применения стандартизованных решений и повышено качество и надежность программного обеспечения.</p> <p>3. Утверждено 15 стандартов по безопасной разработке отечественного программного обеспечения. Минимизирован риск появления уязвимостей в разрабатываемом ПО, повышено качество защиты данных за счет применения стандартизованных решений.</p> <p>4. Утверждено 20 межгосударственных стандартов и изменений в действующие стандарты в сфере информационной безопасности. Утверждение стандартов позволит выработать общий подход при межгосударственном информационном взаимодействии, повысить уровень интеграции при разработке информационных систем в рамках ЕАЭС, а также будет стимулировать развитие рынка информационной безопасности в странах ЕАЭС.</p>					
05.02.002.002.001		Проведение исследования по идентификации рисков и угроз информационной безопасности при обработке массивов больших данных, анализу адекватности существующих стандартов обработки массивов больших данных выявленным рискам и угрозам информационной безопасности в разрезе отраслей экономики	02.2019	12.2021	Минкомсвязь России, Роскомнадзор	АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет по результатам исследования.
05.02.002.002.002		Разработка проектов стандартов безопасности обработки массивов больших данных	02.2019	12.2021	Минкомсвязь России, ФСБ России, Банк России, Роскомнадзор, Росстандарт	Фонд "Сколково"	Утвержден ежегодный отчет. Приказы Росстандарта об утверждении стандартов.
05.02.002.002		Созданы национальные стандарты обработки массивов больших данных		12.2021			
		<p>Ожидаемые результаты:</p> <p>1. Приняты и используются национальные стандарты безопасности обработки массивов больших данных</p>					
05.02.002.003.001		Проведение анализа потребностей рынка в регулировании деятельности операторов связи промышленного Интернета. По результатам анализа разработать требования к операторам промышленного Интернета	05.2019	12.2021	Минкомсвязь России	Фонд "Сколково", АО «Лаборатория Касперского», АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет.
05.02.002.003.002		Проведение анализа и оценки адекватности рискам и угрозам информационной безопасности существующих стандартов киберфизических систем, включая "Интернет вещей". По результатам разработаны проекты стандартов безопасности для киберфизических систем, включая "Интернет вещей", а также - требования и методики проверки киберфизических систем, включая "Интернет вещей"	05.2019	12.2021	Минкомсвязь России, ФСБ России, Роскомнадзор, Росстандарт, Банк России	Фонд "Сколково", АО «Лаборатория Касперского», АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет.
05.02.002.003.003		Разработка системы управления охраняемыми услугами с учётом современных требований информационной безопасности на базе отечественного программного обеспечения.	01.2020	12.2021	Росгвардия	Организация, отобранная по конкурсу	Подписаны акты ввода в эксплуатацию
05.02.002.003.004		Создание информационного ресурса, предоставляющего физическим и юридическим лицам дистанционный доступ к сервисам оказания охраняемых услуг.	01.2020	12.2021	Росгвардия	Организация, отобранная по конкурсу	Подписан акт об оказанных услугах.
05.02.002.003.005		Создание отечественной защищённой платформы для обработки больших массивов данных. Реализация пилотного проекта по модернизации существующей системы информационного обеспечения централизованного учёта оружия, контроля за соблюдением законодательства Российской Федерации в области оборота оружия и в области частной охранной деятельности Росгвардии на разработанной программно-аппаратной платформе.	02.2019	12.2021	Росгвардия, Минкомсвязь России	Организация, отобранная по конкурсу	Утверждены методические рекомендации. Утверждена документация.
05.02.002.003		Разработаны требования к операторам промышленного Интернета, требования и методики проверки киберфизических систем, проекты стандартов безопасности для киберфизических систем, включая "Интернет вещей"		12.2021			

		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Разработаны стандарты безопасности для киберфизических систем. 2. Разработаны требования или правила регулирования информационной безопасности для операторов связи промышленного Интернета (беспилотных систем и т.д.) 3. Разработаны требования и методики проверки киберфизических систем, включая "Интернет вещей" на соответствие закону "О безопасности критической информационной инфраструктуры Российской Федерации" другим требованиям безопасности. 4. Снижение размеров материального ущерба имуществу юридических и физических лиц на территории субъектов Российской Федерации за счёт использования современных цифровых решений и технологий информационной безопасности, в том числе - повышение эффективности сбора, обработки и передачи служебной информации при оказании охранных услуг, создания единой централизованной системы мониторинга и позиционирования, с использованием современных каналов связи передачи информации, внедрения видео регистрирующей аппаратуры для фиксации событий при обработке служебной информации. 5. Повышение уровня защищённости граждан и юридических лиц за счёт организации доступа к комплексу охранных услуг со всех компьютерных устройств, подключённых к отечественному сегменту сети "Интернет". 6. Разработаны методические рекомендации по адаптации информационных систем, построенных на базе отечественного программного обеспечения в ИТ-панельные платёжному на импортных программных продуктах. 						
05.02.002.004.001		Исследование по формированию базовых требований к отечественным или доверенным операционным системам для киберфизических систем, включая "Интернет вещей"	02.2019	12.2020	Минкомсвязь России, Минпромторг России, ФСТЭК России, ФСБ России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", АО «Лаборатория Касперского», АО "КОНЦЕРН "АВТОМАТИКА"	Подписан акт.	
05.02.002.004.002		Разработка нормативных правовых актов по регулированию вопросов использования отечественных или доверенных операционных систем для киберфизических систем и "Интернета вещей"	01.2019	06.2020	Минкомсвязь России, Минпромторг России, ФСТЭК России, ФСБ России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", АО «Лаборатория Касперского», Фонд "Сколково", АО «НПО РусБИТех», АО "КОНЦЕРН "АВТОМАТИКА"	Утверждены нормативно-правовые акты.	
05.02.002.004		Создана система отраслевого регулирования использования киберфизических систем, включая "Интернет вещей"		12.2020				
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Разработаны критерии оценки на предмет соответствия операционных систем отечественным или доверенным, в том числе на базе отечественных процессорных платформ. 2. Утверждены нормативные правовые акты. 						
05.02.002.005.001		Комплексный анализ и оценка потенциальных уязвимостей, угроз и рисков информационной безопасности, характерных для систем, реализованных на технологиях облачных, туманных, квантовых, виртуальных, искусственного интеллекта, дополненной реальности и распределенных реестров, а также сравнительная оценка экономического эффекта от внедрения облачных, туманных, квантовых технологий, систем виртуальной и дополненной реальности, технологий искусственного интеллекта и распределенных реестров.	10.2018	03.2019	Минкомсвязь России, ФСБ России, Банк России	Организация отобранная по конкурсу	Утвержден отчет.	
05.02.002.005.002		Разработка Концепции реализации единых политик и процессов автоматизации фондов алгоритмов и программ для заказных разработок, в том числе с применением методов искусственного интеллекта для раннего выявления уязвимостей на уровне исходного кода	02.2019	12.2021	Минкомсвязь России, Минтранс России, ФСБ России, МВД России, ФСТЭК России	ОАО "РЖД", АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет. Утверждена концепция.	
05.02.002.005.003		Разработка технологических решений и проведение пилотных проектов по созданию федеральных и региональных государственных информационных ресурсов на основе перспективных систем обработки и хранения информации.	02.2019	12.2021	Минкомсвязь России, ФСБ России, Роскомнадзор, Банк России	ООО «ВЭБ-Инновации», ООО "Яндекс", АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден ежегодный отчет о реализованных пилотных проектах на основе разработанных технологических решений.	
05.02.002.005.004		Обеспечение развития технологий отечественных систем "Интернета вещей", включая телекоммуникационную инфраструктуру и пользовательское оборудование, с учётом требований информационной безопасности	02.2019	12.2021	Минкомсвязь России, ФСБ России, Минпромторг России, Банк России	АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден план-график разработки нормативных актов. Утвержден ежегодный отчет о реализованных мерах развития отечественных систем "Интернета вещей"	

05.02.002.005		Проведены анализ и оценка потенциальных уязвимостей, угроз и рисков информационной безопасности в системах, реализованных на облачных, туманных, квантовых, виртуальных технологиях, технологиях искусственного интеллекта и дополненной реальности, технологиях распределённого реестра, определен перечень необходимых стандартов, ресурсное обеспечение. Разработаны технологические решения и реализованы пилотные проекты с использованием технологии распределённых реестров, внедрение методов и технологий искусственного интеллекта анализа данных, а также "Интернета вещей"		12.2021			
		Ожидаемые результаты: 1. Проведены анализ и оценка потенциальных уязвимостей, угроз и рисков информационной безопасности, характерных для систем, реализованных на технологиях облачных, туманных, квантовых, виртуальных, искусственного интеллекта, дополненной реальности и распределённых реестров, а также произведена сравнительная оценка экономического эффекта от внедрения облачных, туманных, квантовых технологий, систем виртуальной и дополненной реальности, технологий искусственного интеллекта и распределённых реестров. 2. Разработана и утверждена концепция реализации единых политик и процессов автоматизации фондов алгоритмов и программ для заказных разработок, в том числе с применением методов искусственного интеллекта для раннего выявления уязвимостей на уровне исходного кода 3. Разработаны и применяются технологические решения, проведены пилотные проекты по созданию федеральных и региональных государственных информационных ресурсов на основе перспективных систем обработки и хранения информации. 4. Исполняются меры по развитию технологий отечественных систем "Интернета вещей", включая телекоммуникационную инфраструктуру и пользовательское оборудование, с учётом требований информационной безопасности.					
05.02.002.006.001		Создание ресурса по дистанционной регистрации юридических лиц и индивидуальных предпринимателей и открытия им счетов в кредитных организациях с использованием технологии, защищенной с использованием криптографических средств, на основе документов нового образца, содержащих персональные данные гражданина, включая биометрические, а также - усиленную квалифицированную электронную подпись указанных данных	02.2019	12.2020	Минкомсвязь России, Минэкономразвития России, ФСБ России, ФСТЭК России, МВД России, Банк России, ФНС России	ПАО "Сбербанк", ФГБУ НИИ Восход, Госзнак	Подписан Акт ввода в эксплуатацию.
05.02.002.006.002		Создание инфраструктуры сбора биометрических данных граждан и выдачи документов нового образца содержащих усиленную квалифицированную электронную подпись и биометрические данные гражданина на территории всех субъектов РФ.	02.2019	12.2021	Минкомсвязь России, Минэкономразвития России, МВД России, ФСБ России, ФСТЭК России, Банк России	ПАО "Сбербанк", Госзнак, ФГБУ НИИ Восход	Утверждён ежегодный отчёт. Подписаны акты ввода в эксплуатацию.
05.02.002.006		Обеспечено развитие перспективных технологий идентификации участников информационного взаимодействия, включая технологии биометрической идентификации, многофакторной идентификации, методов криптографической аутентификации и иных технологий идентификации		12.2021			
		Ожидаемые результаты: 1. Создана и функционирует система, позволяющая выполнять дистанционную регистрацию ЮЛ и ИП и открытия им счетов в кредитных организациях с использованием технологии, защищенной с использованием криптографических средств, на основе документов нового образца содержащих усиленную квалифицированную электронную подпись и биометрические данные гражданина 2. Проведена проверка компонент системы на соответствие требованиям по информационной безопасности, установленным законодательством Российской Федерации. 3. В многофункциональных центрах предоставления государственных и муниципальных услуг на территории всех субъектов РФ создана инфраструктура сбора биометрических данных граждан и выдачи документов нового образца, содержащих усиленную квалифицированную электронную подпись и биометрические данные гражданина					
05.02.002.007.001		Проведение исследования с целью определения способов идентификации пользователей коммуникационных и иных сервисов участников информационного взаимодействия, а также идентификации пользовательского "Интернета вещей", анализ потребностей рынка в регулировании указанных видов идентификации	02.2019	01.2020	Минкомсвязь России, ФСБ России	Фонд "Сколково"	Утвержден отчет.
05.02.002.007.002		Разработка проекта нормативного правового акта об идентификации пользователей коммуникационных и иных сервисов участников информационного взаимодействия, а также идентификации пользовательского "Интернета вещей"	04.2019	05.2020	Минкомсвязь России, ФСБ России, Банк России	Фонд "Сколково"	Утверждён нормативный правовой акт.
05.02.002.007		Законодательно установлены требования по идентификации пользователей коммуникационных и иных сервисов участников информационного взаимодействия, а также идентификации пользовательского "Интернета вещей"		05.2020			

			Ожидаемые результаты: 1. Подготовлен аналитический отчет по вопросам идентификации пользователей коммуникационных и иных сервисов участников информационного взаимодействия, а также идентификации пользовательского "Интернета вещей", с описанием потребностей рынка в регулировании указанных видов идентификации. 2. Разработан и утвержден нормативный правовой акт об идентификации пользователей коммуникационных и иных сервисов участников информационного взаимодействия, а также идентификации пользовательского "Интернета вещей".				
05.02.002.008.001		Разработка и утверждение регламента государственного контроля обработки и доступа к большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации.	09.2019	02.2021	Роскомнадзор, Минкомсвязь России	Фонд "Сколково"	Утвержден регламент.
05.02.002.008		Обеспечен контроль обработки и доступа к большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации		02.2021			
		Ожидаемые результаты: 1. Утверждение регламента контроля обработки и доступа к большим пользовательским данным при условии закрепления в законодательстве Российской Федерации понятия «большие пользовательские данные» и возложения на Роскомнадзор полномочий по осуществлению контроля за их обработкой. 2. Обеспечено соблюдение нормативных правовых актов об информационном взаимодействии при обработке больших пользовательских данных, в том числе в социальных сетях и прочих средствах социальной коммуникации.					
05.02.002.009.001		Формирование концепции по реализации архитектуры и функционалу специализированного ресурса. При необходимости, подготовка требований по изменению законодательства. Подготовка технических требований	02.2019	06.2019	МВД России, Роскомнадзор, ФСТЭК России, ФСБ России, Банк России		Утверждена концепция. Подготовлены и утверждены технические требования.
05.02.002.009.002		Создание прототипа специализированного ресурса	07.2019	06.2020	МВД России, Роскомнадзор, ФСТЭК России, ФСБ России, Банк России		Подписан акт ввода в опытную эксплуатацию.
05.02.002.009		Создан специализированный ресурс, предназначенный для взаимодействия с уполномоченными органами в части оперативной передачи данных о признаках противоправных действий в области информационных технологий (компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем) в целях противодействия компьютерной преступности, в том числе в финансовой сфере, а также иных случаев криминального и противоправного использования информационных технологий		06.2020			
		Ожидаемые результаты: 1. Разработан специализированный ресурс. 2. Участники информационного взаимодействия осуществляют обмен данными с использованием специализированного ресурса. 3. Определены эксплуатационные потребности при вводе специализированного ресурса в промышленную эксплуатацию. Разработана эксплуатационная документация. 4. Налажено взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ).					
05.02.002.010.001		Разработана архитектура и прототип ресурса антивирусного мультисканера для проверки на наличие признаков вредоносной активности, определены необходимые ресурсы, проведена его опытная эксплуатация. Дана оценка целесообразности создания полнофункционального общедоступного антивирусного мультисканера для проверки на наличие признаков вредоносной активности.	02.2019	12.2021	ФСБ России, ФСТЭК России, Минкомсвязь России		Утверждены отчеты о ходе выполнения работ в 2019 г., 2020 г., 2021 г. Подписан акт ввода в опытную эксплуатацию
05.02.002.010		Создан прототип общедоступного антивирусного мультисканера для проверки на наличие признаков вредоносной активности, определены необходимые ресурсы		12.2021			
		Ожидаемые результаты: 1. Оценена целесообразность создания общедоступного антивирусного мультисканера для прекращения практики проверки фалов на вредоносность персоналом информационных ресурсов Российской Федерации с использованием иностранных решений.					

05.02.002.011.001		Анализ зарубежного и отечественного опыта. Уточнение потребностей пользователей ресурса и участников информационного взаимодействия. Формирование замысла и обсуждение его с заинтересованными сторонами. Разработка концепции системы фильтрации интернет-трафика при использовании информационных ресурсов детьми. Разработка приложения, предоставляющее доступ к безопасным для детей интернет-ресурсам ("белый" перечень интернет-ресурсов)	03.2019	12.2019	Роскомнадзор, Минкомсвязь России, МВД России, ФСБ России		Разработана концепция системы. Представлено на согласование предложение по изменению законодательства РФ. Акт приемки-передачи приложения.
05.02.002.011.002		Создание системы фильтрации интернет-трафика при использовании информационных ресурсов детьми	02.2020	12.2021	Роскомнадзор, Минкомсвязь России, МВД России, ФСБ России		Подписан акт ввода в эксплуатацию.
05.02.002.011		Введена в эксплуатацию система фильтрации интернет-трафика при использовании информационных ресурсов детьми		12.2021			
		Ожидаемые результаты: 1. Создана система фильтрации интернет-трафика при использовании информационных ресурсов детьми. 2. Разработано приложение, предоставляющее доступ к безопасным для детей интернет-ресурсам ("белый" перечень интернет-ресурсов) 3. Проведена опытная эксплуатация системы. 4. Система введена в промышленную эксплуатацию.					
05.02.002.012.001		Анализ предметной области. Определение архитектуры, функционала и технических требований к государственной информационной системе национальной базы знаний индикаторов вредоносной активности (далее – База). Разработка предложений по источникам наполнения, порядку использования Базы и необходимому обеспечению. Разработка технико-экономического обоснования потребностей на эксплуатацию. Разработка технического задания. Выработка предложений по взаиморасчету с контрагентами материалами из базы знаний.	04.2019	03.2020	ФСБ России	Организация отобранная по конкурсу	Подписан акт приёмки работ.
05.02.002.012.002		Разработка первой очереди Базы. Выбор исполнителя. Проведение опытной эксплуатации.	05.2020	12.2021	ФСБ России	Организация отобранная по конкурсу	Подписаны акты приемки опытного образца базы.
05.02.002.012.003		Разработка постановления Правительства Российской Федерации, определяющего порядок создания, эксплуатации и финансирования государственной информационной системы национальной базы знаний индикаторной вредоносной активности.	07.2021	12.2021	ФСБ России, Минкомсвязь России		Выпущено постановление Правительства Российской Федерации.
05.02.002.012		Создана первая очередь национальной базы знаний индикаторов вредоносной активности		12.2021			
		Ожидаемые результаты: 1. Разработана концепция построения национальной базы знаний индикаторов вредоносной активности, а также предложения по источникам её наполнения и порядку использования. Разработано техническое задание на создание первой очереди Базы. 2. Разработана и проведена опытная эксплуатация первой очереди Базы. Уточнены требования к функционалу Базы. Уточнены требования к составу и функциональным характеристикам КТС. 3. Выпущено постановление Правительства Российской Федерации, определяющее порядок создания, эксплуатации и финансирования Базы.					
05.02.002.013.001		Разработка специализированного ресурса, обеспечивающего гражданам России доступ к информации о случаях использования их персональных данных, а также возможность отказа от такого использования	02.2020	12.2021	Роскомнадзор, Минкомсвязь России, МВД России, ФСБ России, ФСТЭК России		Акт ввода в эксплуатацию.
05.02.002.013		Создан специализированный ресурс, обеспечивающий гражданам России доступ к информации о случаях использования их персональных данных, а также возможность отказа от такого использования		12.2021			
		Ожидаемые результаты: 1. Разработана полнофункциональная версия ресурса. 2. Проведена опытная эксплуатация. Доработана эксплуатационная документация. Проведена оценка эксплуатационных расходов при запуске в промышленную эксплуатацию. 3. Ресурс введен в промышленную эксплуатацию.					
05.02.002.014.001		Разработка предложений по популяризации добровольного страхования рисков ИБ. Проработка возможности введения налоговых льгот при страховании рисков ИБ. В том числе, возможность отнесения на себестоимость в бухгалтерском учете.	02.2020	02.2021	Минфин России, Банк России, Минкомсвязь России	Всероссийский Союз Страховщиков, Фонд "Сколково"	Доклад в Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности о наличии/отсутствии административных барьеров.

05.02.002.014.002		Развитие подходов повышения грамотности и практико-ориентированной подготовки в области кибербезопасности для представителей бизнеса и государства на базе опыта ведущих компаний цифровой экономики	02.2019	12.2021	Минкомсвязь России, ФСБ России, ФСТЭК России, МВД России, Банк России	ПАО Сбербанк, АО "Лаборатория Касперского" (научно-образовательные центры), РТУ МИРЭА, АНО "Агентство стратегических инициатив по продвижению новых проектов"	Утвержден ежегодный отчет.
05.02.002.014.003		Создание киберполигона, реализованного в том числе с использованием облачных технологий, для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ, современным практикам обеспечения безопасности	02.2019	12.2019	Минкомсвязь России, МВД России, ФСТЭК России, ФСБ России, Банк России, Минобрнауки России	Фонд "Сколково", ПАО Сбербанк, ООО "Бизон", ООО "АльтЭль"	Подписан акт ввода в эксплуатацию.
05.02.002.014		Разработаны предложения по популяризации добровольного страхования рисков ИБ и повышению киберкультуры		12.2021			
		<p>Ожидаемые результаты:</p> <p>1. Разработаны предложения по введению налоговых льгот по страхованию рисков ИБ. Внесены соответствующие законопроекты.</p> <p>2. Разработаны предложения по популяризации добровольного страхования рисков ИБ.</p> <p>3. Реализована система повышения грамотности в области информационной безопасности, в том числе разработано не менее 10 учебных курсов по 4 направлениям, связанным с ИБ; введена в эксплуатацию платформа управления обучением, включающая разработанные учебные курсы по ИБ; подготовлено не менее 10 специальных практических комплексов для проведения семинаров и практикумов; проведено не менее 100 образовательных мероприятий (лекций, семинаров, вебинаров и пр.) для слушателей, включая представителей МВД России, Следственного комитета, Генпрокуратуры и бизнес-структур; для организации обучения привлечено не менее 3 ведущих отечественных компаний в сфере информационной безопасности.</p> <p>4. Введен в эксплуатацию киберполигон для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ современным практикам обеспечения безопасности</p>					
05.02.002.015.001		Анализ норм и практики правоприменения привлечения к ответственности за правонарушения в области информационных технологий	03.2019	08.2019	МВД России, Минкомсвязь России, Минэкономразвития России, Банк России, МЧС России		Подписан акт приемки результатов анализа.
05.02.002.015.002		Разработка проектов актов о внесении изменений в действующее законодательство по новым составам и квалифицирующим признакам правонарушений, совершенных с использованием информационных технологий	08.2019	06.2020	МВД России, Минкомсвязь России, Минэкономразвития России, Банк России	ПАО "Сбербанк", Фонд "Сколково"	Проект закона внесен в Правительство Российской Федерации.
05.02.002.015		Внесены изменения в Уголовный кодекс Российской Федерации, касающиеся расширения криминализации новых типов деяний, совершенных с использованием информационных технологий		06.2020			
		<p>Ожидаемые результаты:</p> <p>1. Предложения по ужесточению ответственности за преступления в области информационных технологий</p> <p>2. Законопроект вынесен для утверждения</p> <p>3. В Уголовный кодекс внесены изменения, определяющие ответственность за новые типы деяний, совершенных с использованием информационных технологий</p>					
05.02.002.016.001		Разработан проект федерального закона об основах государственного регулирования криптографической деятельности в Российской Федерации	03.2019	12.2021	ФСБ России	Организация отобранная по конкурсу	Проект федерального закона согласован с заинтересованными федеральными органами исполнительной власти. Утвержден ежегодный отчет о ходе реализации мероприятия.
05.02.002.016.002		Разработка проекта плана мероприятий ("дорожная карта") «Российская криптография в российском сегменте Интернет»	10.2018	03.2019	Минкомсвязь России, ФСБ России, Росстандарт	Лицензиаты ФСБ России	План мероприятий утвержден.
05.02.002.016		Сформированы условия для эффективного применения шифровальных (криптографических) средств защиты информации в условиях цифровой экономики		12.2021			
		<p>Ожидаемые результаты:</p> <p>1. Проект федерального закона направлен на согласование в заинтересованные федеральные органы исполнительной власти.</p> <p>2. Разработан, согласован с соответствующими органами план мероприятий ("дорожная карта") "Российская криптография в российском сегменте Интернет"</p>					

05.02.002.017.001			Разработка и поддержание в актуальном состоянии технологических карт осуществления переводов денежных средств, описывающих криптографические алгоритмы с указанием применяемых криптографических примитивов с учетом деятельности международных платежных систем.	01.2020	07.2020	Банк России	АО НСПК, ПАО Сбербанк, ПАО Банк ВТБ, АО «Газпромбанк», АО «Альфа-Банк», технический комитет по стандартизации ТК 122 «Стандарты финансовых операций»	Доклад в Правительство Российской Федерации.
05.02.002.017.002			Формирование «дорожной карты» по дальнейшей разработке криптографических алгоритмов, предназначенных для использования в СКЗИ значимых платежных систем, с учетом криптографических алгоритмов, определяемых документами национальной системы стандартизации Российской Федерации	10.2018	12.2019	ФСБ России, Банк России	АО "НСПК"	"Дорожная карта" утверждена Правительством Российской Федерации.
05.02.002.017.003			Определение порядка разработки, ответственных за поддержание в актуальном состоянии, а также разработка и опубликование функционально-технических требований к техническим средствам и программному обеспечению, реализующим СКЗИ (включая функциональные и эксплуатационные требования): аппаратный модуль безопасности (HSM-модули); платежные устройства с терминальным ядром; платежные карты (крипто модуль, приложение); интернет-браузеры и стандартные операционные системы и т.д.	10.2018	12.2019	Банк России	Ассоциация банков России, АО НСПК, ПАО Сбербанк, ПАО Банк ВТБ, АО «Газпромбанк», АО «Альфа-Банк», ООО «Платежная система «Виза», ООО «МастерКард»	Разработаны в соответствии с порядком функционально-технические требования к техническим средствам и программному обеспечению, реализующим СКЗИ (включая функциональные и эксплуатационные требования) . Определены ответственные за поддержание в актуальном состоянии разработанных функциональных требований. Требования и ответственные опубликованы на сайте Банка России.
05.02.002.017.004			Разработка и опубликование требований к СКЗИ, указанных в пункте 2.20 указания Банка России от 9 июня 2012 г. № 382-П (в редакции указания Банка России от 7 мая 2018 г. № 4793-У).	10.2018	12.2019	ФСБ России, Банк России		Разработаны требования к СКЗИ, указанные в пункте 2.20 указания Банка России от 9 июня 2012 г. № 382-П. Требования опубликованы на сайте Банка России.
05.02.002.017.005			Формирование «дорожной карты» по разработке сертифицированных ФСБ России программных средств, реализующих СКЗИ, в соответствии с требованиями, разработанными в результате выполнения пунктов 05.02.002.017.003, 05.02.002.017.004.	01.2020	12.2020	Минкомсвязь России, ФСБ России, Банк России		"Дорожная карта" утверждена Правительством Российской Федерации.
05.02.002.017.006			Формирование «дорожной карты» по разработке сертифицированных ФСБ России технических средств, реализующих СКЗИ, в соответствии с требованиями, разработанными в результате выполнения пунктов 05.02.002.017.003, 05.02.002.017.004.	01.2020	12.2020	Минпромторг России, Минкомсвязь России, ФСБ России, Банк России		"Дорожная карта" утверждена Правительством Российской Федерации.
05.02.002.017.007			Формирование «дорожной карты» по сертификации на соответствие требованиям международных платежных систем программных и технических средств, разработанных в соответствии с "дорожными картами", утвержденными в результате выполнения пунктов 05.02.002.017.005, 05.02.002.017.006.	01.2020	06.2021	Банк России, Минпромторг России, Минкомсвязь России, ФСБ России	ООО «Платежная система «Виза», ООО «МастерКард», АО НСПК	"Дорожная карта" утверждена Правительством Российской Федерации.
05.02.002.017.008			Создание и обеспечение функционирования центра тестирования технических средств и программного обеспечения на соответствие функционально-техническим требованиям, включая разработку регламента и методики тестирования.	01.2021	10.2021	Минкомсвязь России, Банк России, ФСБ России, Минпромторг России	АО НСПК, ООО «Платежная система «Виза», ООО «МастерКард»	Утверждены регламент, методика тестирования, акт ввода в эксплуатацию центра тестирования технических средств и программного обеспечения.
05.02.002.017.009			Подготовка системного проекта по созданию реестра данных (на базе технической платформы оперативного обмена данными), содержащего идентификационные сведения платежных карт, предусматривающего в том числе определение состава сведений которые будут храниться в реестре, определение порядка ведения реестра, определение оператора реестра, определение круга лиц, обладающих правом получения из реестра информации	02.2019	12.2019	Банк России, Минфин России, ФСБ России, МВД России, Росфинмониторинг, Минкомсвязь России	ООО «Платежная система «Виза», ООО «МастерКард», АО НСПК	Доклад в Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности с анализом результатов проделанной работы.
05.02.002.017.010			Создание (на базе технической платформы оперативного обмена данными) и обеспечение функционирования реестра данных, содержащего идентификационные сведения платежных карт	01.2020	07.2021	Банк России, Минфин России, ФСБ России, МВД России, Росфинмониторинг, Минкомсвязь России	АО НСПК, ООО «Платежная система «Виза», ООО «МастерКард»	Подписан Акт ввода в эксплуатацию.

05.02.002.017		Обеспечено развитие значимых платежных систем и обеспечение их информационной безопасности, в том числе в части использования в них российских криптографических средств.		10.2021			
		<p>Ожидаемые результаты:</p> <p>1. Поддержка в актуальном состоянии технологических карт осуществления переводов денежных средств, описывающих криптографические алгоритмы с указанием применяемых криптографических примитивов с учетом деятельности международных платежных систем.</p> <p>2. Создан и функционирует центр тестирования технических средств и программного обеспечения на соответствие функционально-техническим требованиям, включая разработку регламента и методики тестирования.</p> <p>3. Обеспечено развитие значимых платежных систем.</p> <p>4. Обеспечены информационная безопасность значимых платежных систем, в том числе в части использования в них российских криптографических средств.</p> <p>5. Доклад Президенту Российской Федерации (ежегодно до 1 июня, начиная с 2020 года).</p>					
05.02.002.018.001		Разработка механизмов координации работ по реализации мероприятий по развитию профессионального образования в сфере информационной безопасности	10.2020	12.2021	Минобрнауки России, Минпросвещения России	ФУМО ВО ИБ, ФУМО СПО ИБ.	Приказ Минобрнауки России. Аналитическая справка, утвержденная Минобрнауки направлена в Межведомственную комиссию по информационной безопасности при Совете Безопасности Российской Федерации (далее - МВК ИБ СБ РФ)
05.02.002.018.002		Формирование общего объема контрольных цифр приема по специальностям и направлениям подготовки в области информационной безопасности для обучения в образовательных организациях за счет бюджетных ассигнований федерального бюджета.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России, ФСТЭК России, МЧС России, Банк России, заинтересованные субъекты Российской Федерации	Организации, определённые в соответствии с законодательством Российской Федерации	Подписан акт сдачи-приемки. Приказ Минобрнауки России.
05.02.002.018.003		Определение потребностей в кадрах в области информационной безопасности	02.2019	12.2021	Минтруд России, Минобрнауки России, Министерство просвещения РФ, Минпромторг России, Минкомсвязь России, ФСТЭК России, МЧС России, Банк России, заинтересованные государственные органы и субъекты Российской Федерации	ФГБУ "ВНИИ труда" Минтруда России, АНО "Агентство стратегических инициатив по продвижению новых проектов"	Утверждён ежегодный аналитический отчет
05.02.002.018.004		Анализ состояния реализации образовательных программ в области ИБ, в том числе анализ материально-технической базы, в образовательных организациях высшего образования и среднего профессионального образования.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России	ФУМО ВО ИБ, ФУМО СПО ИБ, организации, определённые в соответствии с законодательством Российской Федерации	Подписан акт сдачи-приемки. Направлена в МВК ИБ СБ РФ аналитическая ежегодная справка.

05.02.002.018.005		Разработка проекта ведомственной целевой программы "Подготовка кадров в области информационной безопасности на 2022 – 2028 годы" и последующая синхронизация и развитие с федеральными проектами "Информационная безопасность" и "Кадры для цифровой экономики" национальной программы "Цифровая экономика РФ", "Концепцией развития кадрового обеспечения в области информационной безопасности в РФ на долгосрочную перспективу".	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России, МЧС России, Банк России, заинтересованные субъекты Российской Федерации		Приказ Минобрнауки России.
05.02.002.018		Проведен анализ существующей системы образования в области информационной безопасности, сформировано целевое состояние такой системы, определены ресурсы.		12.2021			
		<p>Ожидаемые результаты:</p> <p>1. Новый состав Координационного совета Минобрнауки России по подготовке, профессиональной переподготовке и повышению квалификации в области ИБ (далее - КС ИБ), утвержден и приступил к работе, разработано Положение о КС ИБ с возложением на него функций головного координирующего органа в системах высшего образования (далее-ВО), среднего профессионального образования (далее-СПО) и дополнительного профессионального образования (далее-ДПО) по выполнению мероприятий по развитию профессионального образования в области информационной безопасности в рамках федерального проекта "Информационная безопасность". Определение Минобрнауки России образовательной организации, обеспечивающей деятельность КС ИБ.</p> <p>2. Прогноз по количеству специалистов с разным уровнем образования (разного уровня квалификации: с высшим образованием, со средним профессиональным образованием) в целом и по субъектам Российской Федерации на трехлетний период, утвержден на КС ИБ. Прогноз составлен с учетом предложений государственных органов, профильных работодателей, бизнес сообщества и обеспечивает нужды цифровой экономики, ежегодно корректируется.</p> <p>3. Контрольные цифры приема по специальностям и направлениям подготовки в области информационной безопасности соответствуют требованиям цифровой экономики. Количество принятых на обучение по программам: высшего образования в области ИБ не менее 9 тыс. студентов на 2022/2023 год, на 2023/2024 год - не менее 10 тыс., далее увеличение КЦП ежегодно до 1000 чел.; по программам СПО в области ИБ не менее 2500 чел. на 2020 год, далее ежегодное увеличение до 1000 чел., ежегодная коррекция КЦП с учетом потребности развития цифровой экономики.</p> <p>4. Паспорт Программы "Подготовка кадров в области информационной безопасности" на 2022 – 2028 годы разработан, согласован с Минпросвещения России в целях реализации "Концепции развития кадрового обеспечения в области информационной безопасности в РФ на долгосрочную перспективу", утв. Правительством РФ.</p> <p>5. Анализ материально-технической базы образовательных организаций проведен, подготовлен отчет для рассмотрения на заседании КС ИБ, разработаны показатели для развития и совершенствования МТБ в целях повышения качества подготовки кадров, ежегодная коррекция уровня оснащенности МТБ образовательных организаций.</p> <p>6. Разработаны типовые комплексы учебно-тренировочных средств и компьютерных полигонов и современные лабораторные практикумы, внедрены в учебный процесс не менее чем в 60 образовательных организациях ВО и СПО, что создает условия требуемого качества подготовки кадров, в т.ч. на основе отечественных продуктов в области ИБ.</p>					
05.02.002.019.001		Разработка и апробация программ повышения квалификации педагогических работников образовательных организаций, осуществляющих подготовку специалистов по защите информации для задач цифровой экономики.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России	ФУМО ВО ИБ, ФУМО СПО ИБ, организация отобранная по конкурсу	Подписан акт сдачи-приемки о проведенном исследовании. Программы согласованы письмом Минобрнауки России.
05.02.002.019.002		Формирование и реализация проектов с государственной поддержкой по профессиональной переподготовке, повышению квалификации и стажировке научно-педагогических и педагогических работников, реализующих образовательные программы в области информационной безопасности.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России, МЧС России, ФСО России, заинтересованные субъекты Российской Федерации	ФУМО ВО ИБ, ФУМО СПО ИБ, организация отобранная по конкурсу	Утверждён перечень мероприятий. Утвержден распорядительный документ по выделению средств на повышение квалификации и проведение научно-образовательных и проектных мероприятий. Подписаны акты об оказании услуг.
05.02.002.019.003		Разработка мер стимулирования научных школ по подготовке научно-педагогических кадров в аспирантуре в области информационной безопасности для задач цифровой экономики.	02.2020	12.2021	Минобрнауки России, Минкомсвязь России, ФСО России	Организация отобранная по конкурсу	Утверждён приказ по созданию диссертационных советов. Утвержден нормативный правовой акт (распорядительный документ) о выделении грантов аспирантам и молодым ученым. Подписаны акты об оказании услуг по проведению научно-образовательных и проектных мероприятий

05.02.002.019.004			Разработка методического аппарата оценки степени подготовленности государственных гражданских служащих	02.2019	12.2021	Минтруд России, Минобрнауки России, Минпросвещения России, Минкомсвязь России, заинтересованные федеральные органы исполнительной власти	ФГБУ "ВНИИ труда" Минтруда России, МОО «Ассоциация защиты информации», АНО "Агентство стратегических инициатив по продвижению новых проектов"	Представлен ежегодный отчет.
05.02.002.019.005			Разработка и реализация пилотных проектов по формированию культуры информационной безопасности у обучающихся общеобразовательных организаций.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России, Банк России, субъекты Российской Федерации	ФУМО ВО ИБ, ФУМО СПО ИБ, организация отобранная по конкурсу	Концепция утверждена протоколом КС ИБ. Утверждены приказы Минобрнауки России, Минпросвещения России об утверждении планов мероприятий. Утверждены распорядительные документы по выделению средств по реализации мероприятий планов. Подписаны акты об оказании услуг.
05.02.002.019.006			Реализация дополнительных мер по привлечению молодежи и иных категорий граждан к участию в олимпиадах школьников и интеллектуальным соревнованиям в области информационной безопасности, в том числе с использованием возможностей государственной поддержки талантливой молодежи, ориентированной на деятельность в данной области.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, ФСО России	ФУМО ВО ИБ, ФУМО СПО ИБ, организация отобранная по конкурсу	Утверждены регламенты проведения интеллектуальных соревнований в области информационной безопасности. Утверждены распорядительные документы по выделению средств на проведение олимпиад и иных интеллектуальных соревнований. Подписаны акты об оказании услуг.
05.02.002.019			Созданы условия для развития образования в области информационной безопасности в интересах реализации задач цифровой экономики.		12.2021			
			<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Программы повышения квалификации педагогических работников разработаны (не менее 15), внедрены в образовательный процесс в целях повышения профессиональной компетентности педагогических работников в области ИБ. 2. Оказывается государственная поддержка проектов по профессиональной переподготовке, повышению квалификации и стажировке педагогических работников. Повышение квалификации и переподготовку по компетенциям в области информационной безопасности прошли не менее 800 педагогических работников. 3. Сформированы диссертационные советы (не менее одного в федеральном округе). Увеличены КЦП по направлению подготовки кадров высшей квалификации 10.06.01 "Информационная безопасность" не менее чем в два раза. Утвержден нормативный правовой акт (распорядительный документ) о выделении грантов аспирантам и молодым ученым, количество защитившихся по научной специальности 05.13.19 « Методы и средства защиты информации, ИБ» к 2025 году не менее 100 чел. 4. Разработаны и внедрены методики оценки и оценочные задания для определения уровня подготовленности государственных гражданских служащих к решению профессиональных задач в сфере обеспечения ИБ. 5. Реализованы дополнительные меры по привлечению молодежи и иных категорий граждан к участию в олимпиадах школьников и к иным интеллектуальным соревнованиям в области информационной безопасности. Олимпиадами и иными интеллектуальными соревнованиями охвачены не менее 8000 школьников ежегодно, из них не менее 300 победителей по результатам олимпиад получают льготы при поступлении в образовательные организации высшего образования. 6. Олимпиадами и иными интеллектуальными соревнованиями ежегодно охвачены не менее 10 % студентов образовательных организаций ВО и СПО, реализующих программы в области ИБ в целях повышения профессионального мастерства. 7. Охват не менее 20 % школьников в не менее чем 6-ти пилотных субъектах Российской Федерации мероприятиями по формированию культуры информационной безопасности. 8. Повышение квалификации и переподготовку по компетенциям в области информационной безопасности прошли не менее 12000 специалистов по защите информации. 					
05.02.002.020.001			Актуализация существующих и разработка новых профессиональных стандартов	02.2020	12.2021	Минтруд России, Минкомсвязь России, ФСТЭК России, Банк России	ФГБУ "ВНИИ труда" Минтруда России, МОО «Ассоциация Защиты Информации», АНО "Агентство стратегических инициатив по продвижению новых проектов"	Утверждены приказами Минтруда России профессиональные стандарты в части учета компетенций в области информационной безопасности

05.02.002.020.002			Внесение изменений в Федеральные государственные образовательные стандарты и примерные основные образовательные программы, отражающие требования к формированию компетенций в сфере информационной безопасности для всех уровней профессионального образования.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России, Банк России	ФУМО ВО ИБ, ФУМО СПО ИБ, организация отобранная по конкурсу	Утверждены приказы Минобрнауки России, Минпросвещения России о внесении изменений в ФГОС ВО и ФГОС СПО. Исходящим письмом ФУМО ВО ИБ, ФУМО СПО ИБ актуализированные примерные основные образовательные программы включены в реестр примерных ООП.
05.02.002.020.003			Разработка актуальных примерных основных профессиональных образовательных программ всех уровней профессионального образования в области информационной безопасности, отвечающих целям и задачам цифровой экономики, и их корректировка.	02.2020	12.2021	Минобрнауки России, Минпросвещения России, Минкомсвязь России, ФСТЭК России, Банк России, МЧС России	ФУМО ВО ИБ, ФУМО СПО ИБ, организация отобранная по конкурсу	Подписан акт сдачи-приемки о проведенном исследовании. Исходящим письмом ФУМО ВО ИБ, ФУМО СПО ИБ примерные основные образовательные программы включены в реестр примерных ООП. Утверждён ежегодный отчёт об актуализированных примерных программах.
05.02.002.020.004			Разработка на конкурсной основе актуальных магистерских программ по перспективным направлениям индустрии информационной безопасности, реализуемых с участием работодателей, проведение их апробации и внедрение.	02.2020	12.2021	Минобрнауки России, Минкомсвязь России, Банк России	ФУМО ВО ИБ, организация отобранная по конкурсу	Подписан акт сдачи-приемки о проведенном исследовании. Исходящим письмом ФУМО ВО ИБ программы включены в реестр примерных ООП.
05.02.002.020.005			Разработка оценочных средств для проведения промежуточной и государственной аттестации по образовательным программам высшего образования в области информационной безопасности.	02.2020	12.2021	Минобрнауки России, Минкомсвязь России	ФУМО ВО ИБ, организация отобранная по конкурсу	Подписан акт сдачи-приемки о проведенном исследовании. Исходящим письмом ФУМО ВО ИБ оценочные средства включены в реестр примерных ООП.
05.02.002.020.006			Разработка с участием работодателей актуальных программ проведения демонстрационного экзамена с учетом отечественных продуктов в области защиты информации, проведение апробации и внедрение программ в образовательный процесс.	02.2020	12.2021	Минпросвещения России, Минобрнауки России, Минкомсвязь России	ФУМО СПО ИБ, организация отобранная по конкурсу	Подписан акт сдачи-приемки о проведенном исследовании. Исходящим письмом ФУМО ВО ИБ программы включены в реестр примерных ООП.
05.02.002.020			Система профессионального образования в области информационной безопасности работает в объеме достаточном для нужд рынков цифровой экономики.		12.2021			
			<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Определен перечень профессиональных стандартов, в которые внесены изменения в части требований по информационной безопасности в целях повышения профессиональной компетентности работников в сфере ИБ. 2. Актуализированы существующие и разработаны новые профессиональные стандарты в области информационной безопасности с учетом развития индустрии информационной безопасности и реализации задач цифровой экономики. 3. Внесены изменения в Федеральные государственные образовательные стандарты и примерные основные образовательные программы для всех уровней профессионального образования в целях повышения профессиональной компетентности в области информационной безопасности выпускников систем ВО и СПО. 4. Примерные основные образовательные программы в области ИБ утверждены (актуализированы) в установленном порядке, включены в реестр примерных программ для реализации в более 180 образовательных организациях ВО и СПО. 5. Разработано и внедрено не менее 10 пилотных магистерских программ по перспективным направлениям индустрии информационной безопасности. 6. Совместно с работодателями разработаны фонды оценочных средств (не менее одного) для 6 образовательных программ ВО в области ИБ в целях контроля качества образования. 7. Разработаны совместно с работодателями программы проведения демонстрационного экзамена (не менее 2) с учетом использования отечественных продуктов в области защиты информации. 					
05.03	Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями							
05.03.001	Обеспечено использование отечественных разработок и технологий при передаче, обработке и хранении данных							
05.03.001.001.001			Создание механизма поддержки функционирования Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий	10.2018	12.2021	Минкомсвязь России		Выпущен нормативный правовой акт (ведомственный акт), определяющий механизм финансирования Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий. Утверждён ежегодный отчёт о деятельности Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий
05.03.001.001			Обеспечено функционирование Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий		12.2021			

		Ожидаемые результаты: 1. Введено в действие Положение о Центре компетенций по импортозамещению в сфере информационно-коммуникационных технологий. Положение учитывает статус организации, полномочия, методики взаимодействия с потенциальными обращениями, определены технические методики по испытаниям отечественного оборудования, включая тесты на совместимость и т.п. Разработан и утвержден механизм поддержки функционирования Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий.						
05.03.001.002.001		Комплексный анализ мировых тенденций и долгосрочный прогноз развития информационных технологий в области информационной безопасности, разработка "дорожной карты" с учетом полученных результатов	10.2018	03.2019	Минкомсвязь России, ФСБ России, ФСТЭК России	АРПП «Отечественный софт», АО "КОНЦЕРН "АВТОМАТИКА"	Утверждена "Дорожная карта" научно-технического и технологического развития Российской Федерации в части перспективных информационных технологий в области информационной безопасности.	
05.03.001.002		Определен перечень перспективных информационных технологий в области информационной безопасности (в том числе средств обеспечения информационной безопасности) для их инвестиционной поддержки		03.2019				
		Ожидаемые результаты: 1. Определены приоритетные потребности страны в научных и технических достижениях, технологиях обеспечивающих решение задач национальной обороноспособности и безопасности, конкурентоспособности и мирового лидерства в области технологий информационной безопасности, исходя из стратегических целей социально-экономического и оборонного строительства. Обеспечено стимулирование развития высокотехнологичных и конкурентоспособных технологий и производств в рассматриваемой сфере за счет средств федерального бюджета и внебюджетных источников в целях обеспечения национальной обороноспособности и безопасности, конкурентоспособности и мирового лидерства.						
05.03.001.003.001		Разработка и реализация мер по обеспечению надлежащего применения субъектами национальной экономики кодов группировок Общероссийского классификатора видов экономической деятельности (ОКВЭД2) и Общероссийского классификатора продукции по видам экономической деятельности (ОКПД2), в части закупок отечественного программного обеспечения и средств защиты информации органами государственной власти и местного самоуправления, государственными корпорациями, компаниями с государственным участием	10.2018	06.2019	Минфин России, Минкомсвязь России, Минэкономразвития России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Утвержден План по реализации мероприятий.	
05.03.001.003.002		Разработка и реализация системных, организационных и технических мер по развитию возможностей единой информационной системы в сфере закупок в части мониторинга закупок отечественного и иностранного программного обеспечения, осуществляемого органами государственной власти и местного самоуправления, государственными корпорациями, компаниями с государственным участием	12.2018	06.2019	Минфин России, Минкомсвязь России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Утвержден План по реализации системных, организационных и технических мер.	
05.03.001.003.003		Осуществление мониторинга и оценки закупок отечественного и иностранного программного обеспечения органами государственной власти и местного самоуправления, государственными корпорациями, компаниями с государственным участием, экономических показателей, характеристики изменения факторов и тенденций, макроэкономический анализ в этой сфере	06.2019	12.2020	Минфин России, Минкомсвязь России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Регулярный доклад в Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности с анализом результатов проделанной работы.	
05.03.001.003		Обеспечение на постоянной основе мониторинга и контроля текущей ситуации с закупками отечественного программного обеспечения органами государственной власти и местного самоуправления, государственными корпорациями, компаниями с государственным участием, определены необходимые ресурсы		12.2020				
		Ожидаемые результаты: 1. Обеспечены условия для государственного статистического наблюдения за субъектами национальной экономики, деятельностью, связанной с закупками отечественного и иностранного программного обеспечения 2. Обеспечена системная, организационная, техническая поддержка реализации потребности органов государственной власти в информации при решении аналитических задач, в том числе необходимых для нормативного правового регулирования деятельности, связанной с закупками отечественного и иностранного программного обеспечения органами государственной власти и местного самоуправления, государственными корпорациями, компаниями с государственным участием 3. Регулярный доклад в Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности с анализом результатов проделанной работы						
05.03.001.004.001		Создание испытательных лабораторий для обеспечения информационной безопасности национальных сетей связи с использованием квантовых криптографических технологий	02.2019	12.2021	ФСБ России, Минкомсвязь России	Московский Государственный Университет, ИТМО, АО "Смартс"	Подписан Акт ввода в эксплуатацию. Утвержден ежегодный отчет о ходе реализации мероприятия.	

05.03.001.004		Обеспечение информационной безопасности национальных волоконно-оптических сетей связи с применением квантовых технологий		12.2021			
		Ожидаемые результаты: 1. Созданы испытательные лаборатории для квантовых технологий защиты. 2. Обеспечивается безопасность национальных волоконно-оптических сетей связи с применением квантовых технологий					
05.03.001.005.001		Определение показателей развития информационно-телекоммуникационных технологий, включая их целевые значения, и разработка методики их оценки	10.2018	03.2019	Минкомсвязь России, Минпромторг России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Утверждены перечень показателей и методика их расчета.
05.03.001.005.002		Расчет текущих показателей развития информационно-телекоммуникационных технологий и радиоэлектронной отрасли	10.2018	03.2019	Минкомсвязь России, Минпромторг России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Утвержден отчет о выполнении показателей.
05.03.001.005		Определение методик оценки показателей развития информационно-телекоммуникационных технологий и радиоэлектронной отрасли, их текущих и целевых значений		03.2019			
		Ожидаемые результаты: 1. Утвержден перечень показателей развития информационно-телекоммуникационных технологий и радиоэлектронной отрасли. 2. Утверждена методика оценки показателей развития информационно-телекоммуникационных технологий и радиоэлектронной отрасли. 3. Определены текущие значения показателей развития информационно-телекоммуникационных технологий и радиоэлектронной отрасли.					
05.03.001.006.001		Разработка предложений по актуализации федерального законодательства о закупках и смежных нормативных правовых актов	11.2018	06.2019	Минпромторг России, Минкомсвязь России, Минэкономразвития России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", Фонд "Сколково"	Утвержден список предложений по актуализации федерального законодательства о закупках и смежных нормативных правовых актов. Подготовлены проекты нормативных актов.
05.03.001.006.002		Модернизация системы критериев для определения телекоммуникационного, компьютерного и серверного оборудования российского происхождения (ТОРП) и программного обеспечения (ПО). Разработка предложений по актуализации федерального законодательства о закупках и смежных нормативных правовых актов	11.2018	03.2019	Минпромторг России, Минкомсвязь России, Минэкономразвития России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Представлен проект актуализированных критериев и методики. Утвержден список предложений по актуализации федерального законодательства о закупках и смежных нормативных правовых актов.
05.03.001.006		Законодательное закрепление норм, обеспечивающих преференции для компьютерного, серверного и телекоммуникационного оборудования и ПО отечественного производства при осуществлении закупок для государственных и муниципальных нужд, а также при предоставлении различных форм государственной поддержки		06.2019			
		Ожидаемые результаты: 1. Методика присвоения статуса ТОРП актуализирована 2. Утвержден пакет нормативных правовых актов, обеспечивающих преференции для компьютерного, серверного и телекоммуникационного оборудования и ПО отечественного происхождения при осуществлении закупок для государственных и муниципальных нужд, а также при предоставлении различных форм государственной поддержки					
05.03.001.007.001		Формирование описания типовых объектов закупок телекоммуникационного оборудования и отдельных видов радиоэлектронной продукции, закупаемых органами государственной и муниципальной власти, а также компаниями с государственным участием	03.2019	06.2019	Минкомсвязь России, Минпромторг России, Минфин России, Минэкономразвития России		Утвержден отчет. Подготовлены проекты нормативных правовых актов для дальнейшего согласования с заинтересованными ведомствами.
05.03.001.007.002		Формирование описания типовых объектов закупок программного обеспечения органами государственной власти, компаниями с государственным участием, в том числе, рекомендуемых функциональных, технических и других характеристик	10.2018	02.2019	Минкомсвязь России, Минфин России, Минэкономразвития России, ФСТЭК России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", Фонд "Сколково", АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден отчет. Подготовлены проекты нормативных правовых актов.
05.03.001.007		Принятие нормативных правовых актов, определяющих описание типовых объектов закупок компьютерного, серверного и телекоммуникационного оборудования, а также программного обеспечения		06.2019			

			Ожидаемые результаты: 1. Определены типовые объекты закупок телекоммуникационного оборудования и отдельных видов радиоэлектронной продукции 2. Определены типовые объекты закупок программного обеспечения				
05.03.001.008.001		Разработка требований по использованию преимущественно отечественного компьютерного, серверного и телекоммуникационного оборудования на объектах инфраструктуры обработки данных	10.2018	03.2019	Минкомсвязь России, Минпромторг России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", Фонд "Сколково", АО "КОНЦЕРН "АВТОМАТИКА"	Утверждены требования.
05.03.001.008.002		Определение потребностей использования на территории России компьютерного, серверного и телекоммуникационного оборудования российского производства, проведение анализа возможностей отечественных производителей оборудования и электронных компонентов, определение необходимых ресурсов	02.2019	06.2019	Минкомсвязь России, Минпромторг России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", АО "КОНЦЕРН "АВТОМАТИКА"	Утвержден отчет о выполнении показателей. Утвержден перечень гражданской радиоэлектронной продукции, производимой на территории Российской Федерации с учётом отечественной ЭКБ.
05.03.001.008		Законодательно установлены требования к использованию отечественного компьютерного, серверного и телекоммуникационного оборудования на объектах инфраструктуры обработки данных		06.2019			
		Ожидаемые результаты: 1. Приняты требования по использованию преимущественно отечественного компьютерного, серверного и телекоммуникационного оборудования на объектах инфраструктуры обработки данных. 2. Утвержден перечень гражданской радиоэлектронной продукции, производимой на территории Российской Федерации с учётом отечественной ЭКБ, для реализации мероприятий плана развития микроэлектронной промышленности Российской Федерации					
05.03.001.009.001		Проведение исследования по анализу международного опыта поддержки производителей электронной компонентной базы	10.2018	03.2019	Минпромторг России, Минкомсвязь России		Утвержден отчет по проведенному исследованию.
05.03.001.009.002		Мониторинг использования российскими компаниями - производителями компьютерного, серверного и телекоммуникационного оборудования отечественных комплектующих, включая электронную компонентную базу (ЭКБ)	10.2018	12.2021	Минпромторг России, Минкомсвязь России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", организация отобранная по конкурсу	Утвержден ежегодный отчет.
05.03.001.009.003		Мониторинг использования на объектах информационной инфраструктуры Российской Федерации, включая инфраструктуру обработки данных, преимущественно отечественного компьютерного, серверного и телекоммуникационного оборудования.	10.2018	06.2019	Минкомсвязь России, Минпромторг России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Утвержден отчет.
05.03.001.009		Создана система стимулов для развития отечественных организаций, обеспечивающих потребности отраслей экономики в электронной компонентной базе, и использования отечественных комплектующих компаниями-производителями компьютерного, серверного и телекоммуникационного оборудования		12.2021			
		Ожидаемые результаты: 1. Утвержден отчет о проведении исследования по анализу международного опыта поддержки производителей электронной компонентной базы 2. Выработаны и реализуются меры, обеспечивающие равные конкурентные условия для отечественных производителей ТКО в сравнении с зарубежными производителями 3. Проводится мониторинг.					
05.03.001.010.001		Разработка предложений по стимулированию приобретения и использования оборудования российского производства	10.2018	03.2019	Минпромторг России, Минкомсвязь России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Утверждены предложения по стимулированию приобретения и использования оборудования российского производства.

05.03.001.010.002		Разработка мер предоставления льгот российским организациям и индивидуальным предпринимателям, закупающим и использующим отечественные продукты по ИБ (товары и услуги), в части начисления амортизации, налога на добавленную стоимость и налога на прибыль	02.2019	10.2019	Минкомсвязь России, Минэкономразвития России, Минфин России, ФСТЭК России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", Фонд "Сколково"	Утверждён перечень мер по поддержке организаций, закупающих отечественные продукты по ИБ.
05.03.001.010		Создана система стимулов для приобретения и использования компьютерного, серверного и телекоммуникационного оборудования отечественного производства		10.2019			
		Ожидаемые результаты: 1. Внесены изменения в нормативные правовые акты, создающие систему стимулирования приобретения и использования оборудования отечественного производства.					
05.03.001.011.001		<ul style="list-style-type: none"> - Проведение исследования по определению приоритетных направлений и объемов поддержки разработки отечественного программного обеспечения, включая разработчиков средств защиты информации и увеличения его доли в условиях цифровой экономики институтами развития - Осуществляется финансовая поддержка разработчиков отечественного офисного программного обеспечения и отечественного программного обеспечения в сфере информационной безопасности для обеспечения совершенствования программного обеспечения в целях его соответствия требованиям заказчиков к функциональным, техническим и эксплуатационным характеристикам. - Осуществляется финансовая поддержка механизмов стимулирования замещения используемых на критически важных объектах автоматизированных систем управления предприятиями и технологическими процессами, инженерного программного обеспечения, оборудования для систем безопасности иностранного производства на отечественные аналоги. - Осуществляется акселерация (обучение, поддержка, возвращение) команд-разработчиков отечественного программного обеспечения, включая разработчиков средств защиты информации. - Осуществляется грантовая поддержка малых инновационных предприятий по разработке отечественного программного обеспечения, включая разработчиков средств защиты информации - Реализуются программы соинвестирования и инвестирования в уставной капитал разработчиков отечественного программного обеспечения, включая разработчиков средств защиты информации 	02.2019	12.2021	Минкомсвязь России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", ВЭБ.РФ, Фонд развития интернет-инициатив (ФРИИ) ООО "ВЭБ Инновации" Фонд содействия развитию малых форм предприятий в научно-технической сфере	Утвержден ежегодный отчет об оказанных мерах финансовой поддержки разработчиков отечественного программного обеспечения. Регулярный доклад в Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности с анализом результатов проделанной работы.
05.03.001.011.002		Созданы венчурные фонды для финансирования разработки программного обеспечения, включая разработчиков средств защиты информации	02.2019	12.2021	Минкомсвязь России	АО "Российская венчурная компания", ООО "ВЭБ Инновации"	Утверждён ежегодный отчет.
05.03.001.011.003		<p>Осуществляется льготное кредитование разработчиков программного обеспечения, включая разработчиков средств защиты информации</p> <p>Осуществляется поддержка инновационных отечественных разработок программного обеспечения, ориентированных на новые рынки, включая разработчиков средств защиты информации</p> <p>Обеспечение координации и мониторинга выделения инвестиций по приоритетным направлениям разработки программного обеспечения, включая разработчиков средств защиты информации</p> <p>Организована выдача денежных премий (призов) за найденные уязвимости в программном и программно-аппаратном обеспечении</p> <p>Создание механизма коммерциализации продуктов, созданных на основе новых отечественных ИТ</p>	02.2019	12.2021	Минкомсвязь России, Минпромторг России	Фонд развития промышленности, АНО "Центр компетенций по импортозамещению в сфере ИКТ", АНО "Цифровая экономика", Фонд "Сколково", ООО "ВЭБ Инновации", Заинтересованные институты развития	Утвержден ежегодный отчет, включающий следующую информацию: - описание утвержденных мер по льготному кредитованию разработчиков программного обеспечения, - описание утвержденных мер по поддержке инновационных отечественных разработок программного обеспечения, - отчет о результатах мониторинга по реализации утвержденных мер поддержки отечественных разработчиков.
05.03.001.011.004		Разработка Концепции, определяющей приоритетные направления разработки отечественного общесистемного и прикладного программного обеспечения, включая вопросы совместимости	10.2018	03.2019	Минкомсвязь России	АНО "Центр компетенций по импортозамещению в сфере ИКТ"	Концепция согласована и утверждена.

05.03.001.011.005		Обеспечение структурных подразделений центрального аппарата Росгвардии, территориальных органов Росгвардии, органов управления (объединений, соединений, воинских частей, организаций и подразделений) войск национальной гвардии отечественным офисным программным обеспечением и программным обеспечением в сфере информационной безопасности и оказание технической поддержки в рамках применения поставленных программных продуктов	02.2019	12.2021	Минкомсвязь России, Росгвардия	Организация отобранная по конкурсу	Утверждён ежегодный отчёт, включающий следующую информацию: - утверждённый перечень программных продуктов. - заключённые договора на поставку программного обеспечения. - подписанные акты оказания типовых цифровых услуг по сервисной модели
05.03.001.011		Созданы механизмы стимулирования разработки отечественного программного обеспечения и увеличения его доли в условиях цифровой экономики с помощью акселерации перспективных бизнес идей, венчурного финансирования, льготного кредитования, премирования за найденные уязвимости		12.2021			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Определены приоритетные направления и объемы поддержки разработки отечественного программного обеспечения и увеличения его доли в условиях цифровой экономики институтами развития. 2. Запущены и реализуются инвестиционные программы в целях поддержки разработчиков отечественного программного обеспечения для нужд цифровой экономики на поздних стадиях развития. 3. Осуществляется стимулирование разработки отечественного программного обеспечения и увеличения его доли в условиях цифровой экономики. 4. Обеспечены координация и мониторинг выделения инвестиций по приоритетным направлениям разработки программного обеспечения. 5. Победители получают денежные призы (гранты) за найденные уязвимости. Разработчики их исправляют. Программное и программно-аппаратное обеспечение становится надежнее. 6. Создан механизм коммерциализации продуктов, созданных на основе новых отечественных ИТ. 7. Структурные подразделения центрального аппарата Росгвардии, территориальных органов Росгвардии, органов управления (объединений, соединений, воинских частей, организаций и подразделений) войск национальной гвардии обеспечены отечественным офисным программным обеспечением и программным обеспечением в сфере информационной безопасности. Оказывается техническая поддержка. 					
05.03.001.012.001		Исследование по формированию базовых требований к антивирусным программам, допускаемым к установке на персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации	02.2019	08.2019	Минкомсвязь России, ФСБ России, ФСТЭК России, ФАС России, МЧС России		Утверждена Методика проведения выбора антивирусных программ, допускаемых к установке на персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации.
05.03.001.012.002		Разработка проекта нормативного правового акта, регулирующего вопрос предустановки отечественных антивирусных программ на все пользовательские устройства, ввозимые и создаваемые на территории Российской Федерации	02.2019	08.2020	Минкомсвязь России, ФАС России, Минэкономразвития России, ФСТЭК России, МЧС России	АНО "Центр компетенций по импортозамещению в сфере ИКТ", Фонд "Сколково"	Подготовленный Проект нормативного правового акта направлен в ЦК "Нормативное регулирование".
05.03.001.012		В целях обеспечения национальной безопасности законодательно обеспечена предустановка отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации		08.2020			
		<p>Ожидаемые результаты:</p> <ol style="list-style-type: none"> 1. Методика проведения выбора антивирусным программ, допускаемым к установке на персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации. 2. Утверждена концепция проектов нормативных правовых актов, регулирующих вопросы предустановки отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации. 3. Утвержден нормативный правовой акт, регулирующий вопрос предустановки отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации. 					

**МЕТОДИКИ РАСЧЕТА ПОКАЗАТЕЛЕЙ И ИНДИКАТОРОВ
федерального проекта "Информационная безопасность"**

№ п/п	Наименование показателя и индикатора, единица измерения	Методика расчета	Источник
1.	Объем затрат на продукты и услуги в области информационной безопасности (млрд руб.)*	Разрабатывается в рамках мероприятия 05.01.001.005.001	
2.	Средний срок простоя государственных информационных систем в результате компьютерных атак, часов	Разрабатывается в рамках мероприятия 05.01.001.005.001	
3.	Доля населения, использовавшего отечественные средства защиты информации по субъектам Российской Федерации (в процентах от общей численности населения, использовавшего сеть "Интернет" в течение последних 12 месяцев, соответствующего субъекта)	Разрабатывается в рамках мероприятия 05.01.001.005.001	
4.	Количество подготовленных специалистов по образовательным программам в области информационной безопасности, с использованием в образовательном процессе отечественных высокотехнологичных комплексов и средств защиты информации, тыс. чел.	Разрабатывается в рамках мероприятия 05.01.001.005.001	
5.	Стоимостная доля закупаемого и (или) арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов и иными органами государственной власти отечественного программного обеспечения, проценты	Разрабатывается в рамках мероприятия 05.01.001.005.001	
6.	Стоимостная доля закупаемого и (или) арендуемого государственнымными корпорациями, компаниями с государственным участием отечественного программного обеспечения, проценты**	Разрабатывается в рамках мероприятия 05.01.001.005.001	

Ключевые проекты и инициативы с максимальными эффектами для бизнеса и граждан на 2018-2021 гг.
федерального проекта "Информационная безопасность"

№ п/п	Наименование проекта или инициативы	Срок реализации	Ожидаемые эффекты от реализации для граждан, бизнеса, государства	Ответственный исполнитель
1.	Создан специализированный ресурс, предназначенный для взаимодействия с уполномоченными органами в части оперативной передачи данных о признаках противоправных действий в области информационных технологий (компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем) в целях противодействия компьютерной преступности, в том числе в финансовой сфере, а также иных случаев криминального и противоправного использования информационных технологий	01.02.2019-01.06.2020	Граждане имеют возможность подать обращение о правонарушении в цифровой среде непосредственно во время и по "месту" его обнаружения; МВД России имеет инструмент для автоматизированной обработки обращений и выделения информации, необходимой для оперативного пресечения и последующего предотвращения правонарушений в цифровой среде; уполномоченные государственные органы получают оперативно-значимую и достоверную статистическую информацию о правонарушениях в цифровой среде; операторы связи, банки, платежные операторы, интернет-компании получают информацию, которую могут использоваться для повышения защищенности своей инфраструктуры и сервисов, предотвращения их противоправного использования	МВД России, Минкомсвязь России, ФСБ России, Роскомнадзор, Банк России, Генеральная прокуратура
2.	Обеспечена целостность, устойчивость и безопасность функционирования российского сегмента сети "Интернет"	01.01.2019-31.12.2021	В общественных интересах обеспечена устойчивость функционирования национального сегмента сети Интернет, в т.ч. за счет "резервирования" на территории России критических информационных ресурсов, пассивного мониторинга маршрутов пропуска трафика, информирования и предоставления возможности координации действий интернет-провайдеров, в т.ч. в условиях масштабных сбоев, атак и DDoS-атак. В общественных интересах обеспечены целостность и устойчивость функционирования сети связи общего пользования, мониторинг ресурсов сетей связи, управление оказанием услуг связи и пропуска трафика, координация и оперативное взаимодействие уполномоченных государственных органов, операторов связи, в т.ч. в условиях чрезвычайных ситуаций и иных предусмотренных законом случаях	Минкомсвязь России, Роскомнадзор, ПАО "Ростелеком", заинтересованные операторы связи
3.	Развитие подходов повышения грамотности и практико-ориентированной подготовки в области кибербезопасности для представителей бизнеса и государства на базе опыта ведущих компаний цифровой экономики	01.02.2019-31.12.2021	Повышение киберкультуры бизнеса и граждан в условиях цифровой экономики. В интересах бизнеса и государства обеспечена возможность получения практико-ориентированного обучения в области кибербезопасности и противодействия киберпреступности на базе опыта ведущих компаний цифровой экономики	Минкомсвязь России, ФСБ России, ФСТЭК России, МВД России, Банк России, ПАО Сбербанк, АО "Лаборатория Касперского" (научно-образовательные центры), РТУ МИРЭА, ЦК "Кадры цифровой экономики"
4.	Создание корпоративных центров ГосСОПКА, обеспечивающих оказание услуг в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты для физических лиц, индивидуальных предпринимателей и малого бизнеса, в том числе не относящимся к субъектам КИИ.	01.11.2018-31.12.2020	Присоединившиеся к системе компании и госорганы, в т.ч. не имеющие ресурсов и компетенция для создания собственных служб обнаружения и реагирования на киберугрозы, имеют возможность оперативно в автоматизированном режиме обмениваться и получать от ведущих компаний в области ИБ информацию об актуальных киберугрозах, средствах и методах их предотвращения и устранения их последствий, а также пользоваться сопутствующими услугами и сервисами	ФСБ России, Банк России, ООО "БИЗОН", ПАО Сбербанк

5.	Законодательное закрепление норм, обеспечивающих преференции для компьютерного, серверного и телекоммуникационного оборудования и ПО отечественного производства при осуществлении закупок для государственных и муниципальных нужд, а также при предоставлении различных форм государственной поддержки	01.11.2018-30.06.2019	Обеспечена поддержка и защита разработчиков и производителей отечественного ПО и оборудования ИКТ за счет установления запретов и ограничений для ПО и оборудования ИКТ иностранного происхождения при госзакупках, закупках компаниями с государственным участием, а также при предоставлении различных форм господдержки. Созданы условия для достижения технологической независимости в области базовых информационных технологий, преимущественного использования отечественного ПО и оборудования ИКТ в условиях цифровой экономики	Минкомсвязь России, Минпромторг России, Минфин России, Минэкономразвития России, Казначейство России, ФАС России, АНО "Центр компетенций по импортозамещению в сфере ИКТ", Фонд "Сколково"
6.	Разработка и реализация государственными институтами развития скоординированного комплекса мер поддержки разработчиков, производителей и заказчиков отечественного ПО и оборудования, на различных стадиях жизненного цикла разработки, производства и внедрения решений	01.02.2019-31.12.2021	Обеспечена поддержка и защита разработчиков и производителей отечественного ПО и оборудования ИКТ за счет реализации мер стимулирования и поддержки, в т.ч. в отношении заказчиков и пользователей отечественного ПО и оборудования ИКТ. Созданы условия для достижения технологической независимости в области базовых информационных технологий, преимущественного использования отечественного ПО и оборудования ИКТ в условиях цифровой экономики	Минкомсвязь России, Минпромторг России, Минэкономразвития России, государственные институты развития
7.	Введена в эксплуатацию система фильтрации интернет-трафика при использовании информационных ресурсов детьми	15.03.2019-31.12.2021	Граждане получают инструмент, который позволяет автоматически отображать содержимое, предназначенное для детей, на компьютере, портативном устройстве	Роскомнадзор, Минкомсвязь России, МВД России, ФСБ России
8.	Обеспечение перехода на отечественное офисное ПО в государственных и муниципальных унитарных предприятиях; федеральных, региональных и муниципальных органах власти; государственных и муниципальных учреждениях (в т.ч. казенных учреждениях, бюджетных учреждениях, автономных учреждениях); публично-правовых компаниях; государственных внебюджетных фондах; Банке России; организациях с государственным/муниципальным участием; государственных корпорациях	01.11.2018-31.12.2020	Сформирован устойчивый спрос государственных заказчиков и компаний на отечественное офисное ПО, в том числе за счет реализации механизма централизованных закупок и формирования сквозной системы планирования перехода на отечественное офисное ПО на среднесрочную перспективу. Оказана государственная финансовая поддержка разработчиков отечественного офисного ПО для обеспечения ускоренного развития российских офисных программных продуктов и обеспечения интеграции с используемыми в настоящее время в государственном секторе информационными системами. Преодолена критическая зависимость государственных и муниципальных органов, государственных внебюджетных фондов, государственных компаний и Банка России от поставок импортного офисного ПО. Созданы условия для достижения технологической независимости в области применения офисного программного обеспечения и технологий обработки данных и электронных документов в системе государственной власти и в государственном секторе экономики в условиях цифровой экономики	Минкомсвязь России, ключевые отраслевые федеральные министерства, государственные внебюджетные фонды, государственные институты развития, Банк России
9.	Создание киберполигона, реализованного в том числе с использованием облачных технологий, для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ, современным практикам обеспечения безопасности	01.02.2019-31.12.2019	Введен в эксплуатацию киберполигон для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ современным практикам обеспечения безопасности	Минкомсвязь России, МВД России, ФСТЭК России, ФСБ России, Банк России, Минобрнауки России, Фонд "Сколково", ПАО Сбербанк, ООО "Бизон", ООО "АльтЭль"
10.	Оказание мер финансовой поддержки органам государственной власти субъектов Российской Федерации по реализации требований №187-ФЗ «О безопасности критической информационной инфраструктуры»	01.11.2019-31.12.2021	С помощью мер по разработке типовых решений КИИ и оказания финансовой поддержки органов государственной власти субъектов Российской Федерации ускорена реализация требований №187-ФЗ "О безопасности критической информационной инфраструктуры". Повышена безопасность объектов КИИ в субъектах Российской Федерации.	Минкомсвязь России

11.	Создание защищенной цифровой среды взаимодействия двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 для нужд МВД России, МЧС России, Росгвардии	01.02.2019-31.12.2021	<p>Разработана концепция защищенной цифровой среды взаимодействия двойного назначения на базе отечественных технологий для нужд МВД России, МЧС России, Росгвардии. Концепция определяет защищенные способы обеспечения связи территорий Российской Федерации, в которых в настоящее время связь отсутствует.</p> <p>Утверждены номенклатура и требования к оборудованию двойного назначения на базе отечественных технологий для работы в стандарте LTE-450</p> <p>Приняты и реализуются меры поддержки потребителей пользовательского оборудования двойного назначения на базе отечественных технологий для работы в стандарте LTE-450</p>	Минкомсвязь России, Минпромторг России, МВД России, МЧС России, ФСБ России, Росгвардия
-----	---	-----------------------	--	--

12.	<i>Разработка специализированного ресурса, обеспечивающего гражданам России доступ к информации о случаях использования их персональных данных, а также возможность отказа от такого использования</i>	01.02.2020-31.12.2021	<i>Создан единый специализированный ресурс и сервисы (для использования в рамках портала Госуслуг), которые позволяют гражданам в виде "одного окна" получить доступ к информации о случаях использования их персональных данных всеми операторами персональных данных (более 10 000 операторов), комплексного и выборочного отказа от такого использования</i>	<i>Роскомнадзор, Минкомсвязь России, МВД России, ФСБ России, ФСТЭК России</i>
13.	<i>Разработка технологических решений и проведение пилотных проектов по реализации федеральных и региональных государственных информационных систем с использованием технологий распределённых реестров, методов и технологий искусственного интеллекта, анализа данных</i>	01.02.2019-31.12.2021	<i>Проведено не менее 10 пилотных проектов по реализации федеральных и региональных государственных информационных систем с использованием технологий распределённых реестров в различных регионах.</i>	<i>Минкомсвязь России, ФСБ России, Роскомнадзор, Банк России</i>

003	Разработка программно-аппаратных средств, обеспечивающих мониторинг маршрутов трафика в сети Интернет	бюджетные средства, млн руб.				169,00								169,00
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 003													169,00
004	Разработка программно-аппаратных средств, обеспечивающих устойчивое и безопасное функционирование системы доменных имен	бюджетные средства, млн руб.												-
		внебюджетные средства, млн руб.				111,09		43,52			43,98			198,59
	Итого по мероприятию 004													198,59
005	Приобретение программно-аппаратных средств обеспечивающих безопасность российского сегмента сети Интернет	бюджетные средства, млн руб.				4121,00				4541,35			12181,24	20 843,59
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 005													20 843,59
006	Разработка программно-аппаратных средств, обеспечивающих мониторинг и управление сетями связи общего пользования	бюджетные средства, млн руб.				245,00				100,00			100,00	145,00
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 006													145,00
007	Обеспечение сбора информации об адресах, номерах автономных систем и связей между ними, маршрутов трафика в сети Интернет, а также управления программно-техническими средствами, обеспечивающими безопасность российского сегмента сети Интернет	бюджетные средства, млн руб.				688,42				1387,12			2548,84	4 524,38
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 007													4 524,38
008	Создание национального удостоверяющего центра, для обеспечения устойчивости взаимодействия устройств в российском сегменте сети "Интернет"	бюджетные средства, млн руб.												-
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 008													-
009	Создание распределенной системы управления и мониторинга информационной безопасности в рамках развития российского государственного сегмента сети "Интернет" (RSNet)	бюджетные средства, млн руб.				206,10				142,30			131,30	479,70
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 009													479,70
010	Разработка целевых значений информационной безопасности функционирования российского сегмента сети "Интернет" с учетом ранее полученных результатов анализа элементов действующей инфраструктуры российского сегмента сети "Интернет" на территории России, включая существующую схему маршрутизации интернет-трафика, проходящего через сети связи иностранных государств/сети иностранных операторов связи, а также определенных на основе анализа подходов по замыканию сетевого трафика на	бюджетные средства, млн руб.												-
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 010													-
011	Проведение ежегодных учений направленных на обеспечение целостности, устойчивости и безопасности функционирования российского сегмента сети Интернет	бюджетные средства, млн руб.												-
		внебюджетные средства, млн руб.												-
	Итого по мероприятию 011													-
	Итого по веке	бюджетные средства, млн руб.				5 429,52				6 170,77			14 961,38	30 831,05

