ПРИЛОЖЕНИЕ № 3
к протоколу президиума Правительственной
комиссии по цифровому развитию, использованию
информационных технологий для улучшения качества жизни
и условий ведения предпринимательской деятельности
от 25 июня 2021 г. № 19

УТВЕРЖДЕНЫ
протоколом президиума Правительственной
комиссии по цифровому развитию, использованию
информационных технологий для улучшения качества жизни
и условий ведения предпринимательской деятельности
от 25 июня 2021 г. № 19

Е Д И Н Ы Е Т Р Е Б О В А Н И Я
по переводу массовых социально значимых государственных и муниципальных услуг в электронный формат

1. Общие положения

1.1. Единые требования по переводу массовых социально значимых услуг в электронный формат (далее соответственно – услуги, Единые требования) разработаны для федеральных органов исполнительной власти (далее – ФОИВ), органов исполнительной власти субъектов Российской Федерации (далее – РОИВ) и органов местного самоуправления (ОМСУ) в целях исполнения Указа Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» в части увеличения доли массовых социально значимых услуг, доступных в электронном виде, до 95 процентов, а также поручения Президента Российской Федерации от 10 октября 2020 г. № Пр-1648 об обеспечении к 1 января 2023 г. перевода в электронный формат массовых социально значимых государственных и муниципальных услуг.

1.2. Во исполнение подпункта «в» пункта 1 перечня поручений Президента Российской Федерации от 10 октября 2020 г. № Пр-1648 в результате перевода массовых социально значимых государственных и муниципальных услуг в электронный формат ФОИВ и РОИВ к 1 января 2023 г. должно быть обеспечено целевое состояние предоставления массовых социально значимых государственных и муниципальных услуг, соответствующее концепции цифровой трансформации «0-0-0» (нулевой вход – нулевое ожидание – ноль бумажных документов).

2. Критерии перевода государственных и муниципальных услуг в электронный формат

2.1. Критериями перевода услуг в электронный формат считаются:

– отсутствие в интерактивной форме услуги запроса документов и сведений, которые могут быть получены посредством межведомственного взаимодействия, в том числе с использованием единой системы межведомственного электронного взаимодействия (далее – СМЭВ);

– ручное заполнение сведений в интерактивной форме услуги допускается только в случае невозможности получения указанных сведений из цифрового профиля посредством СМЭВ или витрин данных;

– обеспечение автозаполнения форм из профиля гражданина ЕСИА, цифрового профиля;

– наличие в интерактивной форме услуги опросной системы для определения индивидуального набора документов и сведений, обязательных для предоставления в определенной жизненной ситуации заявителя;

– онлайн-оплата государственной пошлины и иных платежей (при наличии);

– подача и рассмотрение заявления без личного посещения органа власти или многофункционального центра предоставления государственных или муниципальных услуг;

– автоматическое формирование межведомственных запросов;

– онлайн-информирование в Едином личном кабинете ЕПГУ заявителя о ходе рассмотрения заявления вне зависимости от канала подачи заявления (автоматические статусы);

– автоматизация процедур принятия решения в соответствии с критериями принятия решения;

– автоматическое формирование результата предоставления услуги в электронном виде, подписанного усиленной квалифицированной электронной подписью уполномоченного должностного лица;

– ведение электронного реестра решений;

– передача оценок качества оказания услуги в автоматизированную информационную систему «Информационно-аналитическая система мониторинга качества государственных услуг»;

– средняя оценка качества оказания услуги не ниже, чем в показателе федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации», утвержденной протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

2.2. Целевое состояние оказания услуги, предоставляемой ФОИВ, – в один клик, электронный результат день в день (так называемая концепция 0-0-0: нулевой вход – нулевое ожидание – ноль бумажных документов).

2.3. При переводе услуг, предоставляемых ФОИВ, в электронный формат должны быть концептуально пересмотрены сроки предоставления услуг в части их существенного сокращения с учетом следующего подхода:

– сведения из витрин данных поступают в режиме, близком к реальному времени;

– сведения, получаемые через СМЭВ, – срок продлевается до 5 дней;

– в случае необходимости обоснованной выездной проверки или обоснованного выпуска бумажного документа устанавливается срок меньше текущего значения в административном регламенте.

3. Дополнительные требования к переводу государственных услуг субъектов Российской Федерации и муниципальных услуг в электронный формат

3.1. Субъект Российской Федерации при предоставлении государственных и муниципальных услуг, включенных в перечень массовых социально значимых государственных услуг субъектов Российской Федерации и муниципальных услуг, подлежащих переводу в электронный формат (далее – Перечень МСЗУ РОИВ и ОМСУ), самостоятельно принимает решение о способе приема и обработки заявлений:

– посредством федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (далее – ЕПГУ) с использованием модуля выполнения участниками информационного взаимодействия административных процедур (действий) при предоставлении государственных, муниципальных и иных услуг, исполнении государственных, муниципальных и иных функций, содержащихся в разделах федерального реестра (далее – ПГС) или ведомственной информационной системы (далее – ВИС);

– посредством региональных порталов государственных и муниципальных услуг (далее – РПГУ) с использованием ВИС.

3.2. В случае принятия субъектом Российской Федерации решения о предоставлении государственных и муниципальных услуг, включенных в перечень МСЗУ РОИВ и ОМСУ посредством ЕПГУ с использованием ПГС высший орган исполнительной власти субъекта Российской Федерации заключает с Минцифры России соглашение об организации информационного и технологического взаимодействия при использовании ПГС.

Форма указанного соглашения разработана Минцифры России.

3.3. В случае принятия субъектом Российской Федерации решения о предоставлении государственных и муниципальных услуг, включенных в Перечень МСЗУ РОИВ и ОМСУ, посредством ЕПГУ с использованием ВИС высший орган исполнительной власти субъекта Российской Федерации обеспечивает интеграцию ВИС с ЕПГУ в соответствии с разрабатываемыми Минцифры России Едиными функциональными техническими требованиями по каждой из услуг из Перечня МСЗУ РОИВ и ОМСУ.

3.4. В случае принятия субъектом Российской Федерации решения о предоставлении государственных и муниципальных услуг, включенных в Перечень МСЗУ РОИВ и ОМСУ, посредством РПГУ с использованием ВИС, помимо критериев, предусмотренных пунктом 2.1 настоящих Единых требований,

субъектом Российской Федерации должно быть обеспечено выполнение следующих дополнительных критериев:

– авторизация на РПГУ с использованием федеральной государственной системы «Единая система идентификации и аутентификации»;

– доля активных пользователей РПГУ в субъекте Российской Федерации не менее 50% от числа жителей субъекта Российской Федерации в возрасте от 14 лет;

– доля государственных и муниципальных массовых социально значимых услуг, предоставляемых в электронном виде с использованием РПГУ, не менее 50%;

– доля электронных заявлений, подаваемых через РПГУ по государственным и муниципальным массовым социально значимым услугам, не менее 40% от общего количества подаваемых заявлений.

4. Требования к обеспечению информационной безопасности при переводе государственных услуг органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления в электронный формат

4.1 Общие требования обеспечению информационной безопасности

Требования по обеспечению безопасности информации на объектах инфраструктуры, используемых при оказании государственных и муниципальных услуг, определяются в соответствии с нормами законодательства Российской Федерации в области обеспечения информационной безопасности (далее – ИБ) и должны учитывать требования, установленные нормативными документами в области защиты информации Федеральной службы безопасности (ФСБ России) и Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

Требования по обеспечению ИБ должны быть применены в отношении следующих элементов объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг:

– информационно-телекоммуникационную инфраструктуру, в которой размещаются информационные системы (далее – ИС) ФОИВ, РОИВ, ОМСУ;

– ИС ФОИВ, РОИВ, ОМСУ, создаваемых в целях оказании государственных и муниципальных услуг;

– программное обеспечение, разработанное с целью реализации функций по предоставлению региональных и муниципальных услуг;

– средства криптографической защиты информации, применяемые в ИС региональных и муниципальных органов власти.

Порядок создания и модернизации объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг должен соответствовать положениям, установленным Постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных

информационных систем, и дальнейшего хранения содержащейся в их базах данных информации».

При реализации мер защиты информации на объектах инфраструктуры, используемых при оказании государственных и муниципальных услуг, необходимо руководствоваться, в том числе, следующими нормативными документами в области защиты информации Российской Федерации:

– Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Федеральный закон Российской Федерации от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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

– Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 21 декабря 2017 года №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

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

– Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 05 февраля 2021 года;

– Приказ ФАПСИ от 13 июня 2001 года № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– Приказ ФСБ России от 9 февраля 2005 года № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

– Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

4.2 Классификация объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг

Объекты инфраструктуры, используемые при оказании государственных и муниципальных услуг, должны быть классифицированы в соответствии со следующими нормативными документами:

– в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» должен быть определен необходимый уровень защищённости персональных данных (далее – ПДн).

– в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» должен быть определен класс защищенности объекта инфраструктуры, используемого при оказании государственных и муниципальных услуг;

– в соответствии с приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» и приказом Минкомсвязи России от 25 августа 2009 г. № 104 «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования» должен быть определен класс информационной системы общего пользования.

4.3 Требования к разработке модели угроз и модели нарушителя информационной безопасности

Перечень актуальных угроз безопасности информации (далее – УБИ) должен определяться в рамках разработки Модели угроз и нарушителя безопасности информации (далее – Модель угроз) в соответствии методическим документом «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 05 февраля 2021 года и с данными банка данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/threat).

Модель угроз должна быть направлена на согласование (согласована) в ФСБ России и ФСТЭК России.

4.4 Требования к мерам защиты информации на объектах инфраструктуры, используемых при оказании государственных и муниципальных услуг

Для защиты информации в на объектах инфраструктуры, используемых при оказании государственных и муниципальных услуг необходимо обеспечить реализацию мер защиты информации в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России от 11 февраля 2013 года № 17, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных Приказом ФСТЭК России от 18 февраля 2013 года № 21, и Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 года №239.

Обоснование выбора и уточнение мер защиты информации должно проводиться на основании согласованной с ФСТЭК России и ФСБ России Модели угроз информационной безопасности, с учетом требований, определенных в методическом документе «Меры защиты информации в государственной информационной системе», утвержденном ФСТЭК России 11 февраля 2014 г, на этапе технического проектирования системы защиты информации.

С учётом классификации объектов информатизации, установленных актуальных угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик объектов информатизации должны быть реализованы следующие меры защиты информации:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;
- ограничения программной среды;
- защиты машинных носителей информации;
- регистрации событий безопасности;
- антивирусной защиты;
- обнаружения (предотвращения) вторжений;
- контроля (анализа) защищенности информации;
- обеспечения целостности информационной системы и информации;
- обеспечения доступности информации;
- защиты среды виртуализации
- защиты технических средств;
- защиты информационной системы, ее средств, систем связи передачи данных.
- реагирования на компьютерные инциденты;

– управления конфигурацией.

Определение мер по обеспечению безопасности информации, подлежащих реализации в рамках системы защиты информации объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг, осуществляется в следующем порядке:

– определение базового набора мер по обеспечению безопасности информации для установленного класса защищенности информационной системы и его адаптация с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы;

– уточнение адаптированного базового набора мер по обеспечению безопасности информации, в результате которого определяются меры по обеспечению безопасности информации, направленные на нейтрализацию всех актуальных угроз безопасности;

– дополнение уточненного адаптированного базового набора мер по обеспечению безопасности информации мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации с использованием средств криптографической защиты информации (далее – СКЗИ).

4.5 Средства защиты информации

В составе системы защиты информации должны использоваться сертифицированные по требованиям ФСТЭК России средства защиты информации. Используемые средства криптографической защиты информации должны выбираться исходя из модели угроз безопасности информации и модели нарушителя и быть сертифицированы ФСБ России.

В отношении разрабатываемых компонентов объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг, реализующих функции защиты информации, должна быть проведена оценка соответствия требованиям безопасности информации в соответствии Положением о системе сертификации средств защиты информации, утвержденном приказом ФСТЭК России от 03.04.2018г. №55, по требованиям ФСТЭК России, с привлечением специализированной лаборатории, обладающей лицензией ФСТЭК России.

В отношении СКЗИ, встраиваемого в программное обеспечение ИС, реализующих функции оказания государственных и муниципальных услуг, должны быть проведены тематические исследования на корректность встраивания СКЗИ и оценке невлияния среды функционирования на СКЗИ, по требованиям ФСБ России, с привлечением специализированной лаборатории, обладающей лицензией ФСБ России.

4.6 Дополнительные требования к обеспечению информационной безопасности

Объекты инфраструктуры, используемые при оказании государственных и муниципальных услуг, должны быть сертифицированы на соответствие требованиям, предъявляемым к уровню предоставления услуг центрами обработки данных, требованиям к инфраструктуре центров обработки данных, а также должны отвечать следующим ключевым требованиям:

– обеспечение уровня резервирования и надежности, требуемого в каждом конкретном случае национальным стандартом (после введения в действие стандарта) классификации центров обработки данных;

– обеспечение резервирования инфраструктуры, используемой при оказании государственных и муниципальных услуг, в том числе каналов связи, используемых при оказании государственных и муниципальных услуг.

4.7 Оценка соответствия объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг, требованиям безопасности информации

Оценка соответствия объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг, требованиям безопасности информации должна быть проведена в форме Аттестации.

Аттестация объектов информатизации по требованиям безопасности информации должна быть проведена по классу не ниже чем класс защиты размещаемых государственных информационных систем, систем обработки персональных данных, а также исходя из критериев значимости объектов информационной инфраструктуры.

Аттестация объектов инфраструктуры, используемых при оказании государственных и муниципальных услуг должна включать в себя проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие объектов информатизации требованиям нормативных правовых актов Российской Федерации, руководящих документов ФСТЭК России, ФСБ России, регламентирующих вопросы защиты информации.

В качестве исходных данных, необходимых для аттестации объектов информатизации, должна использоваться согласованная с ФСБ России и ФСТЭК России модель угроз и нарушителя безопасности информации, частное техническое задание на создание системы защиты информации, проектная и эксплуатационная документация на систему защиты информации, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС, материалы предварительных и приемочных испытаний системы защиты информации.