РАЗЪЯСНЕНИЯ

по выполнению требований законодательства Российской Федерации в сфере информационной безопасности при подключении к Федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» в части функциональности единого окна цифровой обратной связи

Принятые сокращения

ИБ – Информационная безопасность.

ИТ – Информационные технологии.

ИЭП – Инфраструктура электронного правительства.

МЭ – Межсетевой экран.

НСД – Несанкционированный доступ.

ОГВ – Орган государственной власти субъекта Российской Федерации.

ОМСУ – Орган местного самоуправления.

ОС – Операционная система.

ПДн – Персональные данные.

ПОС – функциональность единого окна цифровой обратной связи Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)».

САВЗ – Средство антивирусной защиты.

СЗИ – Средство защиты информации.

СКЗИ – Средство криптографической защиты информации.

СКУД – Система контроля и управления доступом.

СОВ – Система обнаружения вторжений.

ФГИС ЕПГУ – Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)».

ФОИВ – Федеральный орган исполнительной власти, либо государственные внебюджетные фонды, службы, агентства, иные органы и организации федерального уровня.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации.

ЦОД – Центр обработки данных.

Термины и определения

Рабочие места сотрудников органов и организаций – автоматизированные рабочие места, входящие в состав ИТ-инфраструктуры органов и организаций, с использованием которых сотрудники осуществляют доступ к web-интерфейсу ПОС для работы с обращениями заявителей.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Обращения – сообщения и обращения граждан и юридических лиц, направленные в органы и организации и их должностным лицам с использованием электронной формы ФГИС ЕПГУ и официальных сайтов таких органов и организаций, а также с помощью мобильного приложения ФГИС ЕПГУ.

Оператор ПДн – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Органы и организации – ФОИВ, ОГВ, ОМСУ, государственные и муниципальные учреждения, центры управления регионами, созданные и

осуществляющие свою деятельность в соответствии с постановлением Правительства Российской Федерации от 16 ноября 2020 года № 1844 «Об утверждении Правил предоставления субсидии из федерального бюджета автономной некоммерческой организации по развитию цифровых проектов в сфере общественных связей и коммуникаций «Диалог Регионы» на создание и обеспечение функционирования в субъектах Российской Федерации центров управления регионов и Правил создания и функционирования в субъектах Российской Федерации центров управления регионов», а также иные организации, осуществляющие публично значимые функции.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Аннотация

Настоящие разъяснения по выполнению требований законодательства Российской Федерации в сфере информационной безопасности при подключении к Федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» в части функциональности единого окна цифровой обратной связи (далее – рекомендации) разработаны с целью выработки единых подходов к выполнению органами и организациями требований законодательства Российской Федерации в сфере информационной безопасности при подключении к ПОС.

1 Общие сведения о ПОС

1.1 Назначение ПОС

ПОС предназначена для решения следующих задач:

- обеспечение возможности подачи обращений гражданами через единое окно подачи обращений – электронные формы, размещенные на официальных сайтах органов и организаций;
- регистрация и обработка поступивших обращений путем присвоения уникального идентификатора каждому обращению, структурирования и классификации обращений, маршрутизации обращений в органы и организации на основании классификации, подготовки ответов на обращения;
- информирование граждан о статусе рассмотрения обращений;
- получение гражданами ответов на обращения в электронной форме, возможности определения удовлетворенности ответом на обращение;
- сбор и анализ информации о работе с обращениями, в том числе:

- анализ деятельности органов и организаций в части соблюдения сроков рассмотрения обращений;

- анализ удовлетворенности граждан рассмотрением обращений;

- определение проблемных точек – вопросов, часто встречающихся в обращениях граждан;

- обеспечение возможности участия граждан в вопросах местного значения и распределения части бюджета путем голосования о выборе региональных и муниципальных проектов и иным вопросам;
- сбор мнения граждан путем проведения опросов;
- проведение социологических опросов мнения граждан по различным вопросам регионального и местного значения, национальным проектам;
- получение и отображение сводных комплексных данных на основе проведения анализа всей поступающей в ПОС информации об обращениях,

сообщениях, голосованиях и опросах;

- предоставление возможности анализа сообщений социальных медиа государственными органами исполнительной власти и ОМСУ.

ПОС включает следующие функциональные компоненты (подсистемы):

- компонент обработки обращений;
- компонент обработки сообщений в открытых источниках;
- компонент общественного голосования.
- компонент Госпаблики;
- мобильное приложение жителя;
- мобильное приложение исполнителя.

Каждая подсистема выполнена в виде определенного набора программных компонент и модулей, предоставляющих необходимый набор сервисов системы.

Создание и развитие ПОС осуществляется в соответствии с пунктом 3 перечня поручений Президента Российской Федерации от 1 марта 2020 года Пр-354, Постановления Правительства Российской Федерации «О проведении эксперимента по использованию федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» для направления гражданами и юридическими лицами в государственные органы, органы местного самоуправления, государственные и муниципальные учреждения, иные организации, осуществляющие публично значимые функции, и их должностным лицам сообщений и обращений, а также для направления такими органами и организациями ответов на указанные сообщения и обращения» от 10 ноября 2020 года № 1802. Функционально ПОС – подсистема ФГИС ЕПГУ, функционирующей в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 года № 210 и положениями постановления Правительства Российской Федерации от «Об инфраструктуре,

обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» 8 июня 2011 года № 451.

В соответствии с требованиями Постановления Правительства Российской Федерации «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» от 6 июля 2015 года № 676 при создании ПОС учитывались требования о защите информации, установленные федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России) в пределах их полномочий.

1.2 Сведения о реализованных мерах защиты информации, обрабатываемой в ПОС

ПОС входит в состав ФГИС ЕПГУ и функционирует на базе общей защищенной инфраструктуры ЦОД ИЭП.

ПОС (в составе ФГИС ЕПГУ) классифицирована как государственная информационная система первого класса защищённости, в которой предусмотрена обработка ПДн, в том числе, специальных категорий и должен быть обеспечен второй уровень защищенности ПДн.

В соответствии с документом «Инфраструктура электронного правительства. Государственная информационная система «Единый портал государственных услуг (функций). Единое окно цифровой обратной связи». Модель угроз и нарушителя безопасности информации» от 31 марта 2021 года, рабочие места сотрудников органов и организаций, с которых осуществляется доступ к web-интерфейсу ПОС, являются внешними пользователями системы и не входят в состав ФГИС ЕПГУ.

Обеспечение безопасности защищаемой информации (в том числе ПДн)

при её обработке в ПОС реализовано комплексом организационных и технических мероприятий, определенных в соответствии с требованиями Постановления Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 года № 1119, Приказа ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 года № 21 и Приказа ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года № 17, и направленных на нейтрализацию актуальных угроз безопасности информации, определенных в модели угроз и нарушителя безопасности информации ФГИС ЕПГУ.

2 Порядок обеспечения соответствия обработки обращений заявителей требованиям Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ.

При работе с обращениями заявителей органы и организации осуществляют обработку ПДн, которые содержатся в обращениях и прилагаемых к обращениям документах, и в соответствии с положениями Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ являются операторами ПДн.

В соответствии частью 1 статьи 18.1 Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ органы и организации должны принимать следующие меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» от 27 июля 2006 года № 152-ФЗ:

- назначить ответственного за организацию обработки ПДн;
- издать документ, определяющий политику органа (организации) в

отношении обработки ПДн[1], локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику органа (организации) в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

– обеспечить применение правовых, организационных и технических мер по обеспечению безопасности ПДн при их обработке на рабочих местах сотрудников в соответствии с пунктом 3 настоящего документа;

– обеспечить осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн положениям Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике органа (организации) в отношении обработки ПДн, локальным актам органа (организации);

– провести оценку вреда, который может быть причинен субъектам ПДн (заявителям) в случае нарушения требований Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ, соотношения указанного вреда и принимаемых органом (организацией) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ;

– ознакомить работников, непосредственно осуществляющих обработку обращений заявителей, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн,

[1] Например, в соответствии с Рекомендациями по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом «О персональных данных» от 27 июля 2006 года № 152-ФЗ, опубликованными на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

документами, определяющими политику органа (организации) в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

3 Порядок обеспечения соответствия рабочих мест сотрудников органов и организаций установленным нормативными правовыми актами Российской Федерации требованиям по обеспечению ИБ

В соответствии с назначением ПОС (п. 1.1 настоящих рекомендаций), при работе с функциональностью единого окна цифровой обратной связи на рабочих местах сотрудников органов и организаций осуществляется обработка обращений заявителей, которые могут содержать ПДн, в том числе в составе приложенных к обращению документов.

При обработке ПДн, содержащихся в обращениях заявителей, в соответствии с частью 1 статьи 19 Федерального закона «О персональных данных» от 27 июля 2006 года № 152 - ФЗ органы и организации обязаны принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн, обрабатываемых на рабочих местах сотрудников, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

При определении требований к техническим и организационным мерам защиты ПДн, обрабатываемых на рабочих местах сотрудников, органы и организации обязаны:

– определить необходимый уровень защищённости ПДн, обрабатываемых на рабочих местах сотрудников, в соответствии с положениями Постановления Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 года № 1119, включая определение категории ПДн, которые могут содержаться в обращениях заявителей, с учётом области деятельности и полномочий органа или организации (специальные, биометрические, общедоступные или иные категории ПДн);

– разработать модель угроз и нарушителя безопасности информации, обрабатываемой на рабочих местах сотрудников, с целью

определения актуальных угроз безопасности информации.[2]

На основании установленного уровня защищенности ПДн, а также перечня актуальных угроз безопасности информации, органы и организации в соответствии с требованиями Постановления Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 года № 1119 обязаны реализовать организационные и технические мероприятия по защите ПДн, которые должны включать:

– организацию режима обеспечения безопасности помещений, в которых размещены рабочие места сотрудников, на которых осуществляется обработка обращений заявителей, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей ПДн, содержащихся в обращениях заявителей (в случае, если бизнес-процесс предусматривает выгрузку, обработку или хранение обращений и приложенных к обращениям документов в органе и организации на локальных носителях);

– утверждение документа, определяющего перечень лиц, доступ которых к ПДн, содержащимся в обращениях заявителей, необходим для выполнения ими служебных (трудовых) обязанностей;

– использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения ИБ[3], в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн при их обработке на рабочих местах сотрудников органов и организаций;

[2] В соответствии с Методическим документом «Методика оценки угроз безопасности информации», утверждённом ФСТЭК России 5 февраля 2021 г.

[3] В соответствии с п.12 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённых Приказом ФСТЭК России от 18 февраля 2013 г. №21

– назначение должностного лица, ответственного за обеспечение безопасности ПДн при их обработке на рабочих местах сотрудников (в случае, когда органом или организацией определена необходимость обеспечения третьего уровня защищенности ПДн, обрабатываемых на рабочих местах сотрудников, и выше);

– организацию доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) органа или организации, или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей (в случае, когда органом или организацией определена необходимость обеспечения второго уровня защищенности ПДн, обрабатываемых на рабочих местах сотрудников, и выше);

– автоматическую регистрацию в электронном журнале безопасности изменения полномочий сотрудника органа или организации по доступу к ПДн, содержащимся в обращениях заявителей (в случае, когда органом или организацией определена необходимость обеспечения первого уровня защищенности ПДн, обрабатываемых на рабочих местах сотрудников);

– создание структурного подразделения, ответственного за обеспечение безопасности ПДн при их обработке на рабочих местах сотрудников либо возложение на одно из структурных подразделений органа или организации функций по обеспечению такой безопасности (в случае, когда органом или организацией определена необходимость обеспечения первого уровня защищенности ПДн, обрабатываемых на рабочих местах сотрудников).

В зависимости от установленного органом или организацией уровня защищённости ПДн, обрабатываемых на рабочих местах сотрудников, технические меры защиты в соответствии с требованиями Приказа ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от

18 февраля 2013 года № 21 должны обеспечивать:

– идентификацию и аутентификацию субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защиту машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн;

– регистрацию событий безопасности;

– антивирусную защиту;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности ПДн;

– обеспечение целостности ПДн;

– обеспечение доступности ПДн;

– защиту среды виртуализации;

– защиту технических средств;

– защиту ПДн при их передаче.

В соответствии с пунктом 10 статьи 2 Приказа ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 года № 21 при невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности ПДн.

При этом, к компенсирующим мерам защиты информации можно отнести:

– замену части средств защиты информации мерами физической

защиты:

- ограничение физического доступа в помещения и к рабочим местам сотрудников органов и организации, на которых осуществляется обработка ПДн;
- опечатывание/опломбирование системных блоков;
- опечатывание/опломбирование портов для подключения съемных устройств;
- использование имеющейся СКУД и системы видеонаблюдения;

– замену части средств защиты информации организационными мерами:

- ограничение, контроль и учёт использования съемных носителей информации и мобильных устройств;
- запрет на использование пользователями административных учётных записей;
- утверждение перечней разрешенного и запрещенного программного обеспечения;
- ограничение использования сети интернет путем определения перечня разрешенных для посещения сайтов;
- утверждение перечня пользователей, которым разрешен доступ к ПДн;

– использование встроенных механизмов защиты ОС:

- идентификация/аутентификация пользователей;
- разграничение доступа;
- ограничение программной среды;
- межсетевое экранирование;
- журналирование;
- шифрование дисков;
- отключение возможности загрузки с внешних носителей.

Также в соответствии со статьей 19 Федерального закона «О

персональных данных» от 27 июля 2016 года № 152 - ФЗ органы и организации должны проводить оценку эффективности принимаемых мер по обеспечению безопасности ПДн. В соответствии с информационным сообщением ФСТЭК России от 15 июля 2013 года № 240/22/2637 решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, должно приниматься органами и организациями самостоятельно.

4 Порядок организации защищенного взаимодействия рабочих мест сотрудников органов и организаций с ПОС

В рамках взаимодействия рабочих мест сотрудников органов и организаций с ПОС для защиты ПДн от несанкционированного доступа при их передаче по каналам связи, не защищённым организационно-техническими средствами, должны применяться СКЗИ, сертифицированные по требованиям ФСБ России.

Для нейтрализации угроз безопасности ПДн, содержащихся в обращениях заявителей, при их передаче по информационно-телекоммуникационным сетям общего пользования в рамках взаимодействия рабочих мест сотрудников органов и организаций с ПОС должны выполняться следующие требования:

– взаимодействие межу рабочими местами сотрудников органов и организаций и ПОС должно осуществляться посредством использования протокола TLS 1.2 с односторонней аутентификацией;

– на рабочих местах сотрудников органов и организаций должны применяться СКЗИ класса КС1, которые поддерживают следующие отечественные алгоритмы при осуществлении криптографических операций в рамках реализации взаимодействия – ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.

– на рабочих местах сотрудников органов и организаций должна обеспечиваться возможность установки и проверки доверенных сертификатов.