МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

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

Москва 2024

Принятые сокращения

АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПДн	Персональные данные
ПОС	Платформа обратной связи
СКЗИ	Средство криптографической защиты информации
ФГИС ЕПГУ	Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭЦП	Электронно цифровая подпись

Термины и определения

Автоматизированные рабочие места органов и организаций – автоматизированные рабочие места (далее – АРМ), входящие в состав ИТ-инфраструктуры органов и организаций, с использованием которых осуществляется доступ к Web-интерфейсу платформы обратной связи (далее – ПОС) для работы с обращениями граждан и юридических лиц.

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

Обращения – обращения граждан и юридических лиц, направленные в органы и организации и их должностным лицам с использованием электронной формы федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (далее – ФГИС ЕПГУ) и официальных сайтов таких органов и организаций, а также с помощью мобильного приложения «Госуслуги Решаем вместе».

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

Органы и организации – государственные органы, органы местного самоуправления, государственные и муниципальные учреждения, иные организации, осуществляющие публично значимые функции.

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

Платформа обратной связи – федеральная государственная

информационная система «Единый портал государственных и муниципальных услуг (функций)» в части функциональности единого окна цифровой обратной связи, классифицированная как государственная информационная система первого класса защищённости (К1), в которой предусмотрена обработка ПДн, в том числе, специальных категорий и для которой должен быть обеспечен второй уровень защищенности (УЗ 2) ПДн.

Аннотация

Настоящие методические рекомендации по выполнению требований законодательства Российской Федерации (далее – РФ) в сфере информационной безопасности (далее – ИБ) при подключении АРМ органов и организаций, с которых осуществляется доступ к Web-интерфейсу ФГИС ЕПГУ в части функциональности ПОС, разработаны с целью выработки единых подходов к выполнению требований законодательства РФ в сфере ИБ при подключении к ПОС.

1 Общие сведения о платформе обратной связи

ПОС входит в состав ФГИС ЕПГУ и функционирует на базе общей защищенной инфраструктуры программно-аппаратного комплекса инфраструктуры электронного правительства.

ПОС (в составе ФГИС ЕПГУ) классифицирована как государственная информационная система **первого класса защищённости (К1)**, в которой предусмотрена обработка ПДн, в том числе, специальных категорий и должен быть обеспечен **второй уровень защищенности (УЗ 2)** ПДн.

АРМ органов и организаций, с которых осуществляется доступ к Web-интерфейсу ПОС, являются внешними пользователями системы и не входят в состав ФГИС ЕПГУ.

В связи с этим в органах и организациях необходимо выполнить следующие мероприятия по защите информации на АРМ, осуществляющих подключение к ПОС[1].

[1] Данные рекомендации предназначены только для служебных АРМ органов и организаций (как автономных, так и входящих в доменную структуру организации), при подключении к ПОС

2 Порядок обеспечения соответствия автоматизированных рабочих мест органов и организаций, с которых осуществляется доступ к Web-интерфейсу платформы обратной связи, установленным нормативными правовыми актами Российской Федерации требованиям по обеспечению информационной безопасности

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

В соответствии с требованиями Постановления Правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании акта классификации «Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)». Единое окно цифровой обратной связи», которой присвоен 2-й уровень защищенности ПДн (УЗ 2), органы и организации обязаны реализовать организационные мероприятия по защите ПДн, которые должны включать:

– организацию режима обеспечения безопасности помещений, в которых размещены АРМ органов и организаций, на которых осуществляется обработка обращений граждан и юридических лиц, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей ПДн, содержащихся в обращениях граждан и юридических лиц (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 граждан и юридических лиц, необходим для

выполнения ими служебных (трудовых) обязанностей;

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения ИБ[2], в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн при их обработке на АРМ органов и организаций;

– назначение должностного лица, ответственного за обеспечение безопасности ПДн при их обработке на АРМ органов и организаций.

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

3 Требования к автоматизированным рабочим местам органов и организаций, с которых осуществляется доступ к Web-интерфейсу платформы обратной связи, для обеспечения их соответствия техническим требованиям по обеспечению информационной безопасности, а также обеспечения возможности подписывать ответы на обращения с использованием электронно цифровой подписи

3.1 Требования к автоматизированным рабочим местам органов и организаций на базе операционной системы Альт Линукс СП 8

На АРМ органов и организаций, осуществляющих подключение к ПОС, необходимо выполнить следующие технические мероприятия по защите информации:

– установленная на АРМ органов и организаций операционная система (далее – ОС) Альт 8 Линукс СП («Альт 8 СП» Рабочая станция) должна иметь все последние обновления, предоставляемые производителем (ссылка на сайт производителя https://www.basealt.ru/altsp);

– установить и настроить программно-аппаратный комплекс (далее – ПАК) обеспечивающий доверенную загрузку ОС («Соболь» версии 4, либо «Аккорд-АМДЗ», или аналог. Ссылки на сайты производителей: https://www.securitycode.ru/products/pak_sobol/?tab=support; https://www.okbsapr.ru/products/accord/accord-amdz/?ysclid=ll23u7qc2d382502525);

– установить и настроить средство антивирусной защиты (Kaspersky Endpoint Security для Linux либо Dr.Web Desktop Security Suite / Dr.Web Security Space (для Linux). Ссылки на сайты производителей: https://support.kaspersky.ru/kes-for-linux/11.3.0; https://products.drweb.ru/linux/);

– установить и настроить средство контроля (анализа) защищенности информации («Red Check» или аналог). Ссылки на сайт производителя: https://docs.redcheck.ru/home/ru-ru/;

– установить средство криптографической защиты (далее – СКЗИ) «КриптоПро CSP» версии 5.0 (ссылка на сайт производителя: https://cryptopro.ru/products/csp);

– установить плагин «КриптоПро ЭЦП Browser plug-in» версии 2.0, для выбранного браузера (ссылка на сайт производителя: https://www.cryptopro.ru/products/cades/plugin?ysclid=ll237o9456334846617)

(необходимо только для сотрудников с ролью «Руководитель» в ПОС, которым необходимо будет осуществлять подписание ответов на обращения граждан с помощью электронно цифровой подписи (далее – ЭЦП)).

Все используемые ОС и средства защиты информации должны иметь действующие сертификаты соответствия федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) и/или федеральной службы безопасности Российской Федерации (далее – ФСБ России). Ответственность за контроль за сроками действия сертификатов соответствия средств защиты информации возлагается на органы и организации.

3.2 Требования к автоматизированным рабочим местам органов и организаций на базе операционной системы Astra Linux Special Edition

На АРМ органов и организаций, осуществляющих подключение к ПОС, необходимо выполнить следующие технические мероприятия по защите информации:

– установленная на АРМ органов и организаций операционная система Astra Linux Special Edition должна иметь все последние обновления, предоставляемые производителем (ссылка на сайт производителя https://wiki.astralinux.ru/pages/viewpage.action?pageId=3276859);

– установить и настроить ПАК, обеспечивающий доверенную загрузку ОС («Соболь» версии 4, либо «Аккорд-АМДЗ», или аналог. Ссылки на сайты производителей: https://www.securitycode.ru/products/pak_sobol/?tab=support; https://www.okbsapr.ru/products/accord/accord-amdz/?ysclid=ll23u7qc2d382502525);

– установить и настроить средство антивирусной защиты (Kaspersky Endpoint Security для Linux либо Dr.Web Desktop Security Suite / Dr.Web Security Space (для Linux). Ссылки на сайты производителей: https://support.kaspersky.ru/kes-for-linux/11.3.0; https://products.drweb.ru/linux/);

– установить и настроить СКЗИ «КриптоПро CSP» версии 5.0 (ссылка на сайт производителя: https://cryptopro.ru/products/csp);

– установить и настроить средство контроля (анализа) защищенности информации (Сканер-ВС «Инспектор» версия 3.0 или аналог). Ссылка на сайт производителя: https://npo-echelon.ru/production/65/11246);

– установить плагин «КриптоПро ЭЦП Browser plug-in» версии 2.0, для

выбранного браузера (ссылка на сайт производителя: https://www.cryptopro.ru/products/cades/plugin?ysclid=ll237o9456334846617) (необходимо только для сотрудников с ролью «Руководитель» в ПОС, которым необходимо будет осуществлять подписание ответов на обращения граждан с помощью ЭЦП).

Все используемые ОС и средства защиты информации должны иметь действующие сертификаты соответствия ФСТЭК России и/или ФСБ России. Ответственность за контроль за сроками действия сертификатов соответствия средств защиты информации возлагается на органы и организации.

3.3 Требования к автоматизированным рабочим местам органов и организаций на базе операционной системы Windows (версии 7 и 10)

На АРМ органов и организаций, осуществляющих подключение к ПОС, необходимо выполнить следующие технические мероприятия по защите информации:

– установленная на АРМ органов и организаций операционная система Windows должна иметь все последние обновления, предоставляемые производителем;

– установить и настроить ПАК, обеспечивающий доверенную загрузку ОС («Соболь» версии 4, либо «Аккорд-АМДЗ» или аналог. Ссылки на сайты производителей: https://www.securitycode.ru/products/pak_sobol/?tab=support; https://www.okbsapr.ru/products/accord/accord-amdz/?ysclid=ll23u7qc2d382502525);

– установить и настроить средство антивирусной защиты (Kaspersky Endpoint Security 11 для Windows либо Dr.Web Desktop Security Suite (для Windows). Ссылки на сайт производителя: https://support.kaspersky.ru/kes11?ysclid=ll23sba35p646132827; https://company.drweb.ru/licenses_and_certificates/fstek/);

– установить и настроить средство защиты от несанкционированного доступа («Secret Net Studio», либо «Dallas Lock 8.0», или аналог). Ссылки на сайты производителей: https://www.securitycode.ru/products/secret-net-studio/?tab=support https://dallaslock.ru/products/szi-dallas-lock-8-0/szi-ot-nsd-dallas-lock-8-0-k/);

– установить СКЗИ «КриптоПро CSP» версии 5.0 (ссылка на сайт производителя: https://cryptopro.ru/products/csp);

– установить и настроить средство контроля (анализа) защищенности информации («Red Check», либо «Сетевой сканер безопасности XSpider 7.8.25», или аналог). Ссылки на сайты производителей: https://docs.redcheck.ru/home/ru-ru/ https://www.ptsecurity.com/ru-ru/products/xspider/#resources);

– установить плагин «КриптоПро ЭЦП Browser plug-in» версии 2.0, для выбранного браузера (ссылка на сайт производителя: https://www.cryptopro.ru/products/cades/plugin?ysclid=ll237o9456334846617) (необходимо только для сотрудников с ролью «Руководитель» в ПОС, которым необходимо будет осуществлять подписание ответов на обращения граждан с помощью ЭЦП).

Все используемые средства защиты информации должны иметь действующие сертификаты соответствия ФСТЭК России и/или ФСБ России. Ответственность за контроль за сроками действия сертификатов соответствия средств защиты информации возлагается на органы и организации.

4 Дополнительные требования к автоматизированным рабочим местам органов и организаций в платформе обратной связи для обеспечения защищенного взаимодействия автоматизированных рабочих мест органов и организаций с платформой обратной связи

При условии выполнения требований из п.3 к АРМ дополнительно для обеспечения защищенного взаимодействия АРМ органов и организаций с ПОС необходимо использовать браузеры, поддерживающие протоколы TLS по ГОСТу (Яндекс или Chromium-Gost);

– Браузер Яндекс доступен для скачивания по ссылке: https://browser.yandex.ru/.

– Браузер Chromium-Gost доступен для скачивания по ссылке: https://github.com/deemru/chromium-gost/releases/latest.

5 Требование к должностному лицу, ответственному за безопасность ПДн

Должностное лицо, ответственное за обеспечение безопасности ПДн при их обработке на АРМ органов и организаций, в своей работе должно руководствоваться требованиями, указанными в документах на средства защиты информации (Руководство администратора безопасности, Формуляр на изделие).