Государственное бюджетное учреждение дополнительного профессионального образования
«Челябинский институт развития образования»

ГБУ ДПО ЧИРО

Требования информационной безопасности при организации обработки заявлений граждан в процессе предоставления массовых социально значимых услуг в инфраструктуре ФГИС «Единая система предоставления государственных и муниципальных услуг (сервисов)» (ПГС)

Начальник отдела обеспечения информационной безопасности

Забиров Наркис Исрафилович

Подключение к ПГС через защищенную сеть №3660

Платформа государственных сервисов (далее – ПГС) функционирует в закрытой сети №604.

Работа на данном ресурсе возможна через защищенную сеть Министерства образования и науки Челябинской области (далее – защищенная сеть №3660) при соблюдении некоторых условий.

Для работы в ПГС через защищенную сеть необходимо:

I. Выполнить обязанности, предусмотренные пунктом 4.2.3 регламента функционирования защищенной сети №3660 (далее – Регламент). (https://www.chiro74.ru/files/documents/регламент_функционирования_защищенной_сети.pdf)
II. Провести проверку корректности функционирования защищенной сети.
III. Выполнить настройку рабочего места в зависимости от используемой операционной системы (далее – ОС).

I. Выполнение требований Регламента

Для выполнения этого требования необходимо в АИС МУЗС проверить наличие загруженного Заключения по результатам оценки соответствия…, Аттестата соответствия… или иного документа, подтверждающего выполнение пункта 4.2.3 Регламента.

Если такой документ не был ранее загружен, загрузите его в соответствии с Инструкцией по работе с системой. Данную инструкцию можно найти в разделе Справка в личном кабинете АИС МУЗС или на главной странице АИС МУЗС.

Ссылка на страницу АИС МУЗС: http://192.168.74.9/ (данный ресурс откроется только с рабочего места, подключенного к защищенной сети №3660).

II. Проверка корректности функционирования защищенной сети № 3660.

Для рабочих мест с ОС Windows:

1. Открыть ViPNet Client. Открыть вкладку «Защищенная сеть».

2. Найти сетевой узел «Челябинск РЦОКИО Координатор HW2000» и «Челябинск РЦОКИО Координатор.

3. Кликнуть правой кнопкой мыши по данным сетевым узлам. Выбрать «Проверить соединение». Статус должен быть «Доступен».

4. Если статус «Недоступен» или отсутствует сетевой узел «Челябинск РЦОКИО Координатор HW2000», то необходимо обращаться в ООИБ ГБУ ДПО «ЧИРО» по адресу электронной почты: support@chiro74.ru с указанием в теме письма «ООИБ Проблема с защищенной сетью». К письму необходимо приложить скриншот проблемы.

II. Проверка корректности функционирования защищенной сети № 3660.

Для рабочих мест с ОС Linux:

1. Открыть ViPNet Client for Linux.

2. Открыть вкладку «Главная».

3. Если будет указано «VPN-соединение работает», то это значит, что вы подключены к защищенной сети и VPN-соединение работает корректно.

В случае, если будет указано «VPN-соединение не работает» или долгое время будет указан статус «Проверка соединения», значит защищенная сеть функционирует некорректно. В таком случае, необходимо обращаться в ООИБ ГБУ ДПО «ЧИРО» по адресу электронной почты: support@chiro74.ru с указанием в теме письма «ООИБ Проблема с защищенной сетью». К письму необходимо приложить скриншот проблемы.

III. Настройка рабочего места с ОС Windows

Для того, чтобы работать в ПГС необходимо провести настройку рабочего места, подключенного к защищенной сети №3660.

Актуальная информация по настройке доступа в ПГС представлена в письме ГБУ ДПО «ЧИРО» №2916 от 26.12.2023г.

По вопросам подключения к ПГС через защищенную сеть №3660 необходимо обращаться в отдел обеспечения информационной безопасности ГБУ ДПО «ЧИРО» по телефону: 8 (351) 217-30-94 или по адресу электронной почты: support@chiro74.ru, с указанием в теме письма «ООИБ ПГС».

Федеральные законы

Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Статья 16. Защита информации:

Обладатель информации, оператор информационной системы, в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
2. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
3. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
4. постоянный контроль за обеспечением уровня защищенности информации;

Федеральные законы

4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. постоянный контроль за обеспечением уровня защищенности информации;
7. нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Федеральные законы

Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК), в пределах их полномочий.

Федеральные законы

Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке.

Обеспечение безопасности персональных данных достигается, в частности:

1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
2. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

Федеральные законы

3.1) применением для уничтожения персональных данных прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

Федеральные законы

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

Постановления Правительства

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

Для обеспечения **4-го уровня защищенности** персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

Постановления Правительства

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения **3-го уровня защищенности** персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Постановления Правительства

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

ФСТЭК России

Приказ ФСТЭК от 18 февраля 2013г. №21 «От утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Данный документ устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

В методическом документе ФСТЭК России от 11 февраля 2014г. «Меры защиты информации в государственных информационных системах» можно посмотреть требования к реализации каждой меры.

Дополнительные требования при использовании СКЗИ

Приказ ФАПСИ от 13 июня 2001г. № 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 10 июля 2014 г. N 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"

Памятка для работников

- Используйте надёжные пароли
- Своевременно обновляйте программное обеспечение, используемое в вашей информационной системе
- Регулярно создавайте резервные копии данных
- Проверяйте ссылки на ресурсе в интернете, особенно, если доступ осуществляется по протоколу http
- Рабочую почту используйте только для рабочих целей
- При получении письма, файлов по электронной почте обращайте внимание на отправителя
- Проверяйте тип файлов перед открытием. Некоторые исполняемые файлы могут попытаться замаскировать под легитимный документ
- Перед запуском исполняемых файлов, подключением внешних носителей проверяйте их антивирусом

Памятка для работников

- Персональные данные передавайте только посредством защищенных каналов связи или перед передачей шифруйте их
- Периодически проводите обучение и инструктажи работников
- Для работы используйте учётные записи с минимально необходимыми привилегиями. Не стоит использовать учётную запись с правами Администратора для повседневной работы.

СПАСИБО ЗА ВНИМАНИЕ!

Государственное бюджетное учреждение дополнительного профессионального образования
«Челябинский институт развития образования»

ГБУ ДПО ЧИРО

454111, г. Челябинск, ул. Комсомольская, д. 20А
454090, г. Челябинск, ул. Красноармейская, д. 88
454087, г. Челябинск, ул. Знаменская, д. 22
454087, г. Челябинск, ул. Блюхера, д. 91

info@chiro74.ru

8 (351) 217 30 89

МЫ В СОЦИАЛЬНЫХ СЕТЯХ

сайт ГБУ ДПО ЧИРО

Телеграм-канал

Сообщество в ВКонтакте

Сообщество в Одноклассниках