Государственное бюджетное профессиональное образовательное учреждение Самарской области
«Сызранский колледж искусств и культуры им. О.Н. Носцовой»

РАССМОТРЕНО
на заседании комиссии по обработке и защите персональных данных
Протокол от 03.02.2020 № 1

УТВЕРЖДАЮ:
Директор ГБПОУ СКИК
_____ Т.В. Алмаева
03.02.2020г.

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБПОУ СКИК

г. Сызрань,2020г.

1. Общие положения

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБПОУ СКИК (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 26 июля 2007 года № 152-ФЗ «О персональных данных», постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, приказом Федеральной службы по техническому и экспортному 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».
1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) государственного бюджетного профессиионального образовательного учреждения Самарской области «Сызранский колледж искусств и культуры им. О.Н. Носцовой» (далее – Учреждение, Оператор) на протяжении всего жизненного цикла ИСПДн.

2. Термины и Сокращения

2.1. В настоящем Положении используются следующие термины и определения:

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

- **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.
- **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
- **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
- **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- **Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Порядок организации и проведения работ по обеспечению безопасности персональных данных

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПДн).

3.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает Оператор или лицо, осуществляющее обработку ПДн по поручению Оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между Оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечит безопасность ПДн при их обработке в информационной системе.
3.4. Выбор средств защиты информации для СЗПДн осуществляется оператором в соответствии с нормативно-правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнении Федерального закона «О персональных данных».
3.5. Структура, состав и основные функции СЗПДн определяются исхордя из уровня защищенности ПДн при их обработке в ИСПДн.
3.6. СЗПДн создается в три этапа:
Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на СЗПДн.
Этап 2. Проектирование СЗПДн, закупка, установка, настройка необходимых средств защиты информации.
Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.
3.7. Этап 1. Проведение предпроектного обследования и разработка технического задания на СЗПДн.
3.7.1. Назначение ответственного за организацию обработки ПДн Учреждением.
3.7.2. Определение целей обработки ПДн Учреждением.
3.7.3. Определение перечня ИСПДн Учреждения и состава ПДн, обрабатываемых в ИСПДн.
3.7.4. Определение перечня обрабатываемых Учреждением ИСПДн.
3.7.5. Определение сроков обработки и хранения ИСПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.
3.7.6. Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.
3.7.7. Определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах.
3.7.8. Назначение ответственного за обеспечение безопасности ПДн в ИСПДн (далее – ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн. Для каждой ИСПДн может быть назначен отдельный ответственный.
3.7.9. Назначение ответственного пользователя криптосредств, обеспечивающего функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждение перечня

лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей криптосредств).
3.7.10 Определение перечня помещений, в которых размещены ИСПДн и материальные носители ПДн.
3.7.11. Определение конфигурации и топологии ИСПДн в целом и их отдельных компонентов, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.
3.7.12. Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.
3.7.13. Формирование технических паспортов ИСПДн.
3.7.14. Разработка организационно-распорядительных документов (далее – ОРД), регламентирующих процесс обработки и защиты ПДн:
- Политика в отношении обработки персональных данных
- Инструкции (ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИСПДн, пользователя ИСПДн, ответственного пользователя криптосредств);
- Раздел должностных инструкций сотрудников Учреждения в части обеспечения безопасности ПДн при их обработке, включая включая установление персональной ответственности за нарушение правил обработки ПДн.
3.7.15. Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательств о соблюдении конфиденциальности ПДн с сотрудником Учреждения.
3.7.16. Утверждение форм уведомлений субъектов ПДн и форм журналов, необходимых в целях обеспечения безопасности ПДн.
3.7.17. Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с «Требованиями к защите ПДН при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 (подготовка и утверждение акта определение уровня защищенности ПДн при их обработке в ИСПДн).
3.7.18. Определение типа угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными и правовыми актами, принятыми во исполнение Федерального закона «О персональных данных». Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).
3.7.19. Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;

- исходные данные создаваемой (модернизируемой ИСПДн) в техническом, программном, информационном и организационном аспектах;

- уровень защищенности ПДН при их обработке в ИСПДн;

- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн.

- конкретизацию мероприятий и требований к СЗПДн;

- состав и содержание работ по этапам разработки и внедрения СЗПДн

- перечень предполагаемых к использованию сертифицированных средств защиты информации.

3.8. Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

3.8.1. Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствую требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и/или не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

3.8.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Учреждения. Применение технических мер должно быть регламентировано нормативным актом Учреждения.

3.8.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.8.4. На стадии проектирования и создания СЗПДн для ИСПДн Учреждения проводятся следующие мероприятия:

- разработка технического проекта СЗПДн;

- приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки , передачи и хранения информации;

- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

- приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации в том числе (при необходимости) средств криптографической защиты информации;

- реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;

- подготовка эксплуатационной документации на используемые средства защиты информации;

- корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

3.9. Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.9.1. На стадии ввода в ИСПДн (СЗПДн) осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);

- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);

-контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

3.9.2. 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 три года в сроки, определяемые оператором (уполномоченным лицом).

4. Проведение работ по обеспечению безопасности персональных данных

4.1. Работы по обеспечению безопасности персональных данных проводятся в соответствии с Планом мероприятий по защите персональных данных (Приложение 1). Внутренние проверки режима защиты ПДн Учреждением проводятся в соответствии Планом внутренних проверок режима защиты персональных данных (Приложение 2).

4.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участие в разработке требований по защите ПДн, организацией работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн Учреждения требованиям безопасности ПДн.

4.3. При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

4.4. В соответствии с п.5.2 Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144, при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн Учреждению необходимо привлекать специализированные организации. имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты

информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащей сведений, составляющих государственную тайну.

5. Решение вопросов обеспечения безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты

5.1. Модернизация СЗПДн для функционирующих ИСПДн Учреждения должна осуществляться в случае:
- изменения состава или структуры ИСПДн или технических особенностей ее построения (изменение состава или структуры программного обеспечения, технических средств обработки ПДн, топологии СИПДн);
- изменение состава угроз безопасности ПДН в ИСПДн;
- изменение уровня защищенности ПДн при их обработке в ИСПДн;
- прочих случаях, по решению оператора.

5.2. В целях определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год ответственным за организацию обработки ПДн должна проводится проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем Учреждения.

5.3. Анализ инцидентов безопасности ПДн и составление заключения в обязательном порядке должно проводится в случае выявления следующих фактов:
- несоблюдение условий хранения носителей ПДн;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- нарушение заданного уровня безопасности ПДн (конфиденциальность/целостность/доступность).

ПРИЛОЖЕНИЕ 1 к
Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБПОУ СКИК

План мероприятий по защите персональных данных в ГБПОУ СКИК

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
1	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн, в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом, «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначно содержащему собственноручную подпись субъекта ПДн в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников оператора к ПДн
5	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение

			журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
6	Ведение журналов учета	постоянно	
7	Повышение квалификации сотрудников в области защиты ПДн	постоянно	
8	Инвентаризация информационных ресурсов	Раз в полгода	
9	Установка сроков обработки ПДн и процедуры их уничтожения	При необходимости	Для ПДн оператором устанавливаются сроки обработки ПДн
10	Уничтожение электронных (бумажных) носителей	При необходимости	
11	Определение уровня защищенности ПДн при их обработке в информационных системах ПДн	При необходимости	
12	Выявление угроз безопасности и разработка моделей угроз	При необходимости	Разрабатывается при создании системы защиты ИСПДн
13	Аттестация (сертификация) СЗПДН или декларирование соответствия требованиям безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
14	Эксплуатация ИСПДн контроль безопасности ПДН		
15	Понижение требований по защите ПДн	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн

ПРИЛОЖЕНИЕ 2 к
Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБПОУ СКИК

План внутренних проверок режима обработки и защиты персональных данных в ГБПОУ СКИК

№ п/п	Мероприятия	Периодичность	Дата, подпись исполнителя
1	Контроль соблюдения правил обработки ПДн	ежемесячно	
2	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	ежегодно	
3	Контроль соблюдения парольной защиты	ежемесячно	
4	Контроль выполнения антивирусной защиты	еженедельно	
5	Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	еженедельно	
6	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	еженедельно	
7	Контроль за обеспечение резервного копирования	ежемесячно	
8	Организация анализха и пересмотра имеющихся угроз безопасности ПДн	ежегодно	
9	Поддержание в актуальном состоянии нормативно-организационных документов	ежеквартально	

Алмаева Татьяна Васильевна

Подписано цифровой подписью: Алмаева Татьяна Васильевна
Дата: 2020.11.30 10:30:52 +04'00'