



АДМИНИСТРАЦИЯ ГОРОДА ЛИПЕЦКА  
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ  
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ИНЖЕНЕРНО-ТЕХНОЛОГИЧЕСКАЯ ШКОЛА № 27

РАССМОТРЕНО  
на заседании  
педагогического  
совета, протокол от  
28.08.2020 № \_\_\_\_\_



## **ПОЛОЖЕНИЕ** **о защите персональных данных** **в информационной системе персональных данных** **«Барс. WEB-электронная школа»**

### **1. Общие положения**

1.1. Положение о защите персональных данных в информационной системе персональных данных «Барс. WEB-электронная школа» (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе «Барс. WEB-электронная школа» на протяжении всего цикла её эксплуатации в МАОУ инженерно-технологической школе №27 города Липецка.

Меры по обеспечению безопасности персональных данных, обрабатываемых в государственной информационной системе (далее – ГИС) «Барс. WEB-электронная школа», принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, обрабатываемых в ГИС.

Меры по обеспечению безопасности персональных данных, обрабатываемых в ГИС «Барс. WEB-электронная школа», реализуются в рамках системы защиты в соответствии с требованиями к защите информации, установленными нормативно-правовыми актами, приведенными в п. 2 настоящего Положения, и направлены на нейтрализацию актуальных угроз безопасности персональных данных, обрабатываемых в ГИС.



1.2. Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий защиты ПДн, обрабатываемых в ГИС «Барс. WEB-электронная школа».

## **2. Нормативные ссылки**

Положение разработано с учетом требований следующих нормативных правовых актов:

- Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной Обработке персональных данных»;
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющую государственную тайну, содержащейся в государственных информационных системах».

При разработке настоящего положения также был учтен утвержденный в МАОУ инженерно-технологической школе №27 города Липецка локальный правовой акт «Акт определения уровня защищенности персональных данных при их обработке в государственной информационной системе».

## **3. Описание ГИС «Барс. WEB-электронная школа»**

ГИС «Барс. WEB-электронная школа» располагается по адресу: 398008, г. Липецк, ул. Лутова, д. 15

Актом определения уровня защищенности персональных данных был установлен 3-й класс защищенности персональных данных при их обработке в ГИС «Барс. WEB-электронная школа».

## **4. Выбор мер по обеспечению безопасности персональных данных, обрабатываемых в ГИС «Барс. WEB-электронная школа».**

В соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющую государственную тайну, содержащейся в государственных информационных системах», базовый набор мер, необходимых для обеспечения 3-го класса



защищенности, включает в себя меры, приведенные в таблице 1 настоящего Положения.

Таблица 1.

Условное обозначение меры	Содержание мер защиты информации
<b>I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)</b>	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
<b>II. Управление доступом субъектов доступа к объектам доступа (УПД)</b>	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
<b>V. Регистрация событий безопасности (РСБ)</b>	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения



Условное обозначение меры	Содержание мер защиты информации
РСБ.7	Защита информации о событиях безопасности
	VI. Антивирусная защита (АВЗ)
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
	VIII. Контроль (анализ) защищенности информации (АНЗ)
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
	XII. Защита технических средств (ЗТС)
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Проведена адаптация базового набора мер с учетом структурно-функциональных характеристик ГИС «Барс. WEB-электронная школа», информационных технологий и особенностей функционирования информационной системы. Из базового набора мер исключены следующие меры, приведенные в таблице 2.

Таблица 2.

Условное обозначение меры	Содержание мер защиты информации	Причина исключения из базового набора мер
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В ИС нет внешних пользователей
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Удаленный доступ через внешние информационно-телекоммуникационные сети не осуществляется
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Технологии беспроводного доступа не используются
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Мобильные технические средства не используются



Для нейтрализации всех актуальных угроз безопасности ГИС проведено уточнение полученного набора мер путем его дополнения с учетом не выбранных ранее мер.

С целью снижения риска неработоспособности технических средств и программных средств обработки информации использованы меры ОДТ.3, ОДТ.4, ОДТ.5.

Более подробное описание выбранных мер по защите информации, обрабатываемой в ГИС, а также способ их реализации приведены в таблице 4.

Знаком «+» обозначены меры по обеспечению безопасности персональных данных, которые включены в базовый набор мер для 3-го класса защищенности.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», были добавлены при уточнении адаптированного базового набора мер.

Таблица 3.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		3	
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	СЗИ от НСД
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	СЗИ от НСД
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	Применение организационно-технических мер
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	СЗИ от НСД
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	СЗИ от НСД
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	СЗИ от НСД
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	СКЗИ



Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		3	
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	СЗИ от НСД
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	СЗИ от НСД
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	СЗИ от НСД
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).	+	СЗИ от НСД СКЗИ
<b>V. Регистрация событий безопасности (РСБ)</b>			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	СЗИ от НСД
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	СЗИ от НСД
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	СЗИ от НСД
РСБ. 7	Защита информации о событиях безопасности	+	СЗИ от НСД
<b>VI. Антивирусная защита (АВЗ)</b>			
АВЗ.1	Реализация антивирусной защиты	+	Антивирус
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	Антивирус
<b>VIII. Контроль (анализ) защищенности информации (АНЗ)</b>			
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	Применение организационных мер
<b>X. Обеспечение доступности персональных данных (ОДТ)</b>			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		Применение организационных мер
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных		Применение организационных мер



Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		3	
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала		Применение организационных мер
XII. Защита технических средств (ЗТС)			
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключая несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	Применение организационно-технических мер
ЗТС.4	Размещение устройств вывода (отображения) информации, исключая ее несанкционированный просмотр	+	Применение организационных мер
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	СКЗИ

## 5. Реализация мер по обеспечению безопасности персональных данных в информационной системе «Барс. WEB-электронная школа».

5.1. Для реализации технических мер по обеспечению безопасности персональных данных в ГИС «Барс. WEB-электронная школа» необходимо осуществить выбор, установку и настройку средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, в соответствии с установленным уровнем защищенности персональных данных и с учетом типа актуальных угроз.

5.2. Организационные меры по обеспечению безопасности персональных данных в ГИС «Барс. WEB-электронная школа» необходимо реализовать путем утверждения инструкций, регламентирующих функции, задачи и обязанности ответственных лиц и иных пользователей, инструкций, определяющих правила и процедуры управления системой защиты информации информационной системы,

выявления инцидентов безопасности обработки персональных данных, осуществления резервного копирования информации, содержащей персональные данные, а также определения правил разграничения доступа субъектов доступа к объектам доступа.

5.3. Для контроля за соблюдением мер по обеспечению безопасности персональных данных, обрабатываемых в ГИС «Барс. WEB-электронная школа», необходимо разработать документы, определяющие правила и процедуры проведения внутреннего контроля (анализа) защищенности персональных данных, в том числе контроля за обеспечением уровня защищенности персональных данных, содержащихся в ГИС.