«УТВЕРЖДАЮ»
И.о. директора МУДО «Ветлужский центр
дополнительного образования»
_____ Е.С.Веселова
Приказ № 177 от 29 декабря 2025 г.

Положение об информационной безопасности МУДО «Ветлужский центр дополнительного образования»

1. Общие положения

1.1. Настоящее Положение определяет порядок обеспечения информационной безопасности в Муниципальном учреждении дополнительного образования «Ветлужский центр дополнительного образования» (далее — Центр) и устанавливает требования к защите информации, в том числе персональных данных, при осуществлении образовательной и иной деятельности Центра.

1.2. Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- иными нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности и обработки персональных данных.

1.3. Под информационной безопасностью в рамках настоящего Положения понимается состояние защищённости информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности от внутренних и внешних угроз.

1.4. Цель Положения — обеспечить защиту информации в Центре, включая персональные данные обучающихся, работников, родителей (законных представителей), а также иные сведения, защита которых предусмотрена законодательством.

1.5. Положение распространяется на всех работников Центра, обучающихся, их родителей (законных представителей), а также иных лиц, получающих доступ к информационным ресурсам Центра.

2. Объекты информационной безопасности

К объектам защиты относятся:

- информационные ресурсы (базы данных, электронные журналы, методические материалы, документы в электронном виде);
- средства и системы информатизации (компьютеры, серверы, локальная сеть, офисное программное обеспечение, системы записи в кружки и иные автоматизированные системы);

- информация, обрабатываемая при осуществлении образовательной деятельности (включая персональные данные, служебную информацию, результаты мониторинга и отчётности);
- официальный сайт Центра и иные информационные ресурсы, доступные пользователям;
- носители информации (жёсткие диски, флеш-накопители, карты памяти и т. п.).

3. Основные задачи и принципы обеспечения информационной безопасности

3.1. Задачи обеспечения информационной безопасности:

- защита от несанкционированного доступа к информационным ресурсам и носителям информации;
- обеспечение конфиденциальности, целостности и доступности информации в соответствии с её категорией и назначением;
- разграничение прав доступа пользователей в соответствии с их должностными обязанностями и функциональными задачами;
- организация антивирусной защиты, контроля уязвимостей и регулярного резервного копирования данных;
- контроль за использованием сети Интернет, в том числе ограничение доступа обучающихся к информации, причиняющей вред их здоровью и развитию;
- своевременное выявление, регистрация и реагирование на инциденты информационной безопасности;
- повышение уровня информационной грамотности участников образовательного процесса.

3.2. Принципы обеспечения информационной безопасности:

- законность — соблюдение требований действующего законодательства РФ;
- системность — учёт всех возможных угроз и реализация комплекса взаимосвязанных мер защиты;
- непрерывность защиты — поддержание мер безопасности на всех этапах жизненного цикла информации;
- достаточность мер защиты — соразмерность применяемых мер уровню актуальных угроз и имеющимся ресурсам Центра;
- персональная ответственность — закрепление обязанностей по обеспечению информационной безопасности за конкретными должностными лицами.

4. Организационные меры

4.1. Директор Центра издаёт приказ о назначении ответственного за обеспечение информационной безопасности (далее — ответственный).

4.2. В обязанности ответственного за информационную безопасность входит:

- разработка, актуализация и контроль исполнения локальных нормативных актов и инструкций по информационной безопасности;
- контроль соблюдения правил работы с информацией, в том числе при использовании информационных систем и носителей информации;
- проведение инструктажей и обучения работников по вопросам информационной безопасности;
- мониторинг состояния средств защиты информации и выявление уязвимостей;

- расследование инцидентов информационной безопасности, подготовка предложений по устранению причин и условий, способствовавших их возникновению;
- взаимодействие с внешними организациями (в том числе надзорными органами) по вопросам информационной безопасности.

4.3. Для каждого сотрудника, работающего с информационными ресурсами, приказом директора устанавливается перечень прав доступа, минимально необходимый для выполнения трудовых функций (принцип минимальных привилегий).

4.4. В Центре ведётся журнал учёта средств защиты информации, эксплуатационной документации, а также журнал регистрации инцидентов информационной безопасности.

4.5. Доступ к критически важным информационным ресурсам предоставляется только после прохождения работником инструктажа по информационной безопасности и ознакомления с настоящим Положением под подпись.

5. Технические меры защиты информации

5.1. На рабочих станциях, серверах и иных вычислительных устройствах Центра установлены и регулярно обновляются средства антивирусной защиты.

5.2. Реализовано разграничение доступа к информационным ресурсам в соответствии с ролями пользователей (администраторы, педагоги, технические специалисты, обучающиеся и др.).

5.3. Организовано регулярное резервное копирование важных данных (не реже одного раза в неделю), хранение резервных копий осуществляется на отдельном защищённом носителе или в выделенном хранилище.

5.4. При использовании сети Интернет применяются средства контентной фильтрации для ограничения доступа к запрещённым и вредоносным ресурсам, в том числе к информации, запрещённой для распространения среди детей.

5.5. Соблюдаются правила работы с паролями:

- пароль должен соответствовать требованиям сложности (длина не менее 8 символов, наличие букв разного регистра, цифр и специальных символов — при технической возможности);
- периодическая смена паролей — не реже одного раза в 90 дней;
- запрет на передачу паролей третьим лицам, запись паролей в открытом виде, использование одинаковых паролей для разных систем.

5.6. Доступ к информационным системам осуществляется с использованием уникальных учётных записей для каждого пользователя.

6. Работа с персональными данными

6.1. Обработка персональных данных осуществляется только при наличии письменного согласия субъекта персональных данных или его законного представителя, за исключением случаев, предусмотренных законодательством РФ.

6.2. Установлен порядок сбора, хранения, использования и уничтожения персональных данных, включающий:

- определение перечня обрабатываемых персональных данных;
- назначение ответственных лиц за обработку персональных данных;
- регламентацию сроков хранения и порядка уничтожения данных;
- фиксацию фактов доступа к персональным данным (при наличии технической возможности).

6.3. Обеспечена защита персональных данных при их передаче третьим лицам: передача осуществляется только по защищённым каналам связи либо на материальных носителях с соблюдением требований к конфиденциальности.

6.4. Доступ к персональным данным предоставляется только уполномоченным работникам в объёме, необходимом для выполнения должностных обязанностей.

7. Действия при инцидентах информационной безопасности

7.1. При выявлении признаков инцидента (попытка несанкционированного доступа, утечка информации, сбой в работе информационных систем, обнаружение вредоносного ПО и т. д.) работник обязан незамедлительно сообщить об этом ответственному за информационную безопасность.

7.2. Ответственный проводит оценку ситуации, принимает меры по локализации и устранению последствий инцидента, фиксирует факт инцидента в журнале регистрации инцидентов.

7.3. По результатам расследования инцидента готовится отчёт с указанием причин, последствий и мер по предотвращению аналогичных ситуаций в будущем.

7.4. При необходимости осуществляется уведомление уполномоченных органов в порядке, установленном законодательством РФ.

8. Обучение и информирование участников образовательного процесса

8.1. Работники Центра проходят инструктаж по информационной безопасности не реже одного раза в год, а также при приёме на работу и при изменении требований к информационной безопасности. Факт прохождения инструктажа фиксируется в журнале под подпись работника.

8.2. Для обучающихся проводятся мероприятия (беседы, квесты, уроки цифровой грамотности), направленные на формирование навыков безопасного поведения в цифровой среде.

8.3. Родителям (законным представителям) предоставляются рекомендации по защите детей в интернете, в том числе памятки и информационные материалы.

9. Ответственность за нарушение требований Положения

9.1. Нарушение требований настоящего Положения влечёт дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

9.2. Персональная ответственность за обеспечение информационной безопасности возлагается на директора Центра, ответственного за информационную безопасность, а также на работников в пределах их должностных обязанностей.

10. Заключительные положения

10.1. Все изменения и дополнения к настоящему Положению утверждаются приказом директора Центра.

10.2. Настоящее Положение вступает в силу с момента его утверждения директором Центра.

10.3. Копия Положения размещается на официальном сайте Центра в разделе «Документы».