

Муниципальное бюджетное учреждение дополнительного образования
Лесновский Дом детского творчества муниципального образования-
Шиловский муниципальный район Рязанской области

УТВЕРЖДЕНО
приказом от 25.12.2018 № 85
Директор МБУ ДО Лесновский ДДТ

И.И. Пушкина

И.И. Пушкина



ПОЛОЖЕНИЕ

об информационной безопасности

р.п. Лесной
2018

1. Общие положения

- 1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в Муниципальном бюджетном учреждении дополнительного образования Лесновский Дом детского творчества (МБУДО Лесновский ДДТ, далее - Учреждение), порядок организации работ по её созданию и функционированию.
- 1.2. Данное положение разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации», 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» и имеет статус локального нормативного акта Учреждения. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.
- 1.3. Под информационной безопасностью Учреждения следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.
- 1.4. Использование сети Интернет в образовательной организации подчинено следующим принципам:
 - соответствие образовательным целям;
 - способствование гармоничному формированию и развитию личности;
 - уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;
 - приобретение новых навыков и знаний;
 - расширение применяемого спектра учебных и наглядных пособий;
 - социализация личности, введение в информационное общество.
- 1.5. К объектам информационной безопасности в Учреждении относятся:
 - информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
 - информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. Персональные данные;
 - средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.
- 1.6. Система информационной безопасности (далее - СИБ) должна обеспечивать:
 - конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
 - целостность (точность и полноту информации и компьютерных программ);
 - доступность (возможность получения пользователями информации в пределах их компетенции).
- 1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:
 - правовая защита – специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная защита – регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита – использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности

- 2.1. Учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Учреждения, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.
- 2.2. Учреждение обязано обеспечить сохранность конфиденциальной информации.
- 2.3. Администрация Учреждения:
 - назначает ответственного за обеспечение информационной безопасности;
 - издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
 - имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
 - имеет право включать требования по защите информации в договоры по всем видам деятельности;
 - разрабатывает перечень сведений конфиденциального характера;
 - имеет право требовать защиты интересов Учреждения со стороны государственных и судебных инстанций.
- 2.4. Организационные и функциональные документы по обеспечению информационной безопасности:
 - приказ директора Учреждения о назначении ответственного за обеспечение информационной безопасности;
 - должностные обязанности ответственного за обеспечение информационной безопасности;
 - перечень защищаемых информационных ресурсов и баз данных;
 - инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Учреждения и др.
- 2.5. Порядок допуска сотрудников Учреждения к информации предусматривает:
 - принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
 - ознакомление работника с нормами законодательства РФ и Учреждения об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
 - инструктаж работника специалистом по информационной безопасности;
 - контроль работника ответственного за информационную безопасность при работе с информацией конфиденциального характера.

3. Использование сети Интернет

- 3.1. Использование сети Интернет в Учреждении осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.
- 3.2. Работники Учреждения вправе:

- размещать информацию в сети Интернет на интернет-ресурсах Учреждения;
 - иметь учетную запись электронной почты на интернет-ресурсах Учреждения.
- 3.3. Работникам Учреждения запрещено размещать в сети Интернет и на образовательных ресурсах информацию:
- противоречащую требованиям законодательства РФ и локальным нормативным актам Учреждения, не относящуюся к образовательному процессу и не связанную с деятельностью Учреждения;
 - нарушающую нравственные и этические нормы, требования профессиональной этики.
- 3.4. Обучающиеся Учреждения вправе:
- использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Учреждения, в порядке и на условиях, которые предусмотрены настоящим Положением;
 - размещать информацию и сведения на интернет-ресурсах Учреждения.
- 3.5. Обучающимся запрещено:
- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство РФ;
 - осуществлять любые сделки через Интернет;
 - загружать файлы на компьютер Учреждения без разрешения уполномоченного лица;
 - распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.
- 3.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Учреждения.
- 3.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.
- 3.8. Уполномоченное лицо обязано:
- принять сообщение пользователя;
 - принять меры по отключению выхода на данный ресурс с интернет-ресурсов Учреждения;
 - если обнаруженный ресурс явно нарушает законодательство РФ - сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством РФ (в течение суток).
- 3.9. Передаваемая информация должна содержать:
- интернет-адрес (URL) ресурса;
 - тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;
 - дату и время обнаружения;
 - информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

4. Мероприятия по обеспечению информационной безопасности

- 4.1. Для обеспечения информационной безопасности в Учреждении требуется проведение следующих первоочередных мероприятий:
- защита интеллектуальной собственности Учреждения;
 - защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Учреждения;
- учет всех носителей конфиденциальной информации.

5. Организация работы с информационными ресурсами и технологиями

5.1. Система организации делопроизводства:

- учет всей документации Учреждения, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов Учреждения в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

5.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

- 5.2.1 Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
- 5.2.2 Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.
- 5.2.3 Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в учебную часть в тот же день.
- 5.2.4 Передача документов исполнителю производится только через ответственного за организацию делопроизводства.
- 5.2.5 Запрещается выносить документы с грифом «Для служебного пользования» за пределы Учреждения.
- 5.2.6 При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.
- 5.2.7 Для организации делопроизводства приказом директора Учреждения назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Учреждения. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

6. Обеспечение безопасности на портале Учреждения

6.1. Сайт Учреждения относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

Сайт Учреждения обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой на сайте Учреждения.

- 6.2. Регламент общих ограничений для участников образовательного процесса при работе с порталом Учреждения, обеспечивающей предоставление Услуги.
- 6.2.1 Участники образовательного процесса, имеющие доступ к сайту Учреждения, не имеют права передавать персональные логины и пароли для входа на сайт Учреждения другим лицам. Передача персонального логина и пароля для входа на портал Учреждения другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.
- 6.2.2 Участники образовательного процесса, имеющие доступ к сайту Учреждения, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).
- 6.2.3 Участники образовательного процесса, имеющие доступ к сайту Учреждения, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя Учреждения, ответственного за ведение сайта.
- 6.2.4 Все операции, произведенные участниками образовательного процесса, имеющими доступ к сайту Учреждения, с момента получения информации руководителем Учреждения о нарушении, указанном в предыдущем абзаце, признаются недействительными.
- 6.2.5 При проведении работ по обеспечению безопасности информации на сайте Учреждения участники образовательного процесса, имеющие доступ к сайту Учреждения, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

7. О системном администрировании и обязанностях ответственного за информационную безопасность

- 7.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора в Учреждении.
- 7.2. Для решения задач информационной безопасности системный администратор обязан:
- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);
 - обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
 - обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
 - обеспечивать нормальное функционирование системы резервного копирования.

8. Антивирусная защита

- 8.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения.
- 8.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.
- 8.3. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.