УТВЕРЖДАЮ
Директор МБУДО
«Центр дополнительного
образования детей г. Медногорска»
_____ Старкова Н.П.
Приказ №64 от 01.12. 2019 года

ПОЛОЖЕНИЕ
об информационной безопасности в Муниципальном бюджетном учреждении дополнительного образования «Центр дополнительного образования детей г.Медногорска»

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы Муниципального бюджетного учреждения дополнительного образования «Центр дополнительного образования детей г.Медногорска» (далее по тексту – образовательного учреждения).

Рабочая станция - персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам Автоматизированной системы образовательного учреждения, приема передачи и обработки информации.

Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Системный администратор - должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса образовательного учреждения, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление

Пользователь – работник образовательного учреждения, использующий ресурсы информационной системы образовательного учреждения для выполнения должностных обязанностей.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе

(Адрес электронной почты, телефон и т.п.).

Пароль - секретная строка символов (букв, шифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

Изменение полномочий - процесс создания удаления, внесения изменений в учетные записи пользователей АС, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю АС.

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЕЯ

1.1. Настоящее Положение регламентирует порядок организации и правила обеспечения информационной безопасности в образовательном учреждении, распределение функций и ответственности за обеспечение информационной безопасности между структурными подразделениями и работниками образовательного учреждения, требования по информационной безопасности к информационным средствам, применяемым в образовательном учреждении.

1.2. Настоящее Положение является локальным нормативным актом. Требования настоящего Положения обязательны для всех структурных подразделений образовательного учреждения и распространяются на:

- автоматизированные системы образовательного учреждения;
- средства телекоммуникаций;
- помещения;
- работников образовательного учреждения.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Информационная безопасность является одним из составных элементов комплексной безопасности образовательного учреждения.

Под информационной безопасностью образовательного учреждения понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

2.2. Информационная безопасность - деятельность, направленная на обеспечение защищенного состояния объекта информации, в том числе объектов, автоматизированных и телекоммуникационных систем, противодействия техническим разведкам, включающая комплексные, криптографические, компьютерные, организационные, технические средства защиты.

2.3. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная защита - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2.4. Информационная безопасность включает:

- защиту интеллектуальной собственности образовательного учреждения;

- защиту компьютеров, локальных сетей и сети подключения к системе Интернета;

- организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся образовательного учреждения;

- учет всех носителей конфиденциальной информации.

2.5. Информационная безопасность образовательного учреждения 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).

2.6. К объектам информационной безопасности образовательного учреждения относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

- информацию, защита которой предусмотрена законодательными актами Российской Федерации, в т. ч. и персональные данные работников и обучающихся образовательного учреждения;

- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

2.7. Правовую основу настоящего Положения составляют:

- Конституция Российской Федерации;

- Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;

- Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;

- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;

- Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ;

- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология.

Практические правила управления информационной безопасностью», утвержденный приказом Ростехрегулирования от 29.12.2005 № 447-ст;

- другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации и Оренбургской области в части обеспечения информационной безопасности.

3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Главная цель обеспечения безопасности информации, циркулирующей в образовательном учреждении, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы образовательного учреждения.

3.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в образовательном учреждении;
- предотвращение нарушений прав личности обучающихся, работников образовательного учреждения на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

3.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам образовательного учреждения, нарушению нормального функционирования и развития образовательного учреждения;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- координация деятельности структурных подразделений образовательного учреждения по обеспечению защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз

информационной безопасности и ликвидации последствий ее нарушения;

- развитие и совершенствование защищенного юридически значимого электронного документооборота;

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

- создание механизмов управления системой информационной безопасности (СИБ).

4. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Система обеспечения информационной безопасности распространяются на:

- автоматизированные системы образовательного учреждения;
- средства телекоммуникаций;
- помещения;
- сотрудников образовательного учреждения.

4.2. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в образовательном учреждении осуществляются:

- защита персональных данных персонала и обучающихся;
- контроль за использованием электронных средств информационного обеспечения деятельности образовательного учреждения по прямому назначению;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности образовательного учреждения нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;
- внутрисетевой контроль за перемещением информации;
- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- проверка целесообразности использования персоналом и обучающимися образовательного учреждения интернет-ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;
- обучение персонала образовательного учреждения по вопросам обеспечения информационной безопасности;
- контроль за правильностью использования имеющихся в образовательном учреждении средств телефонной связи;
- защита персональных данных персонала и обучающихся;
- мероприятия по недопущению несанкционированного доступа к персональным данным персонала и обучающихся образовательного

учреждения при их обработке с использованием средств автоматизации или без использования таких средств;

- контроль за использованием электронных средств информационного обеспечения деятельности образовательного учреждения по прямому назначению;

- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности образовательного учреждения нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

- контроль за используемым программным обеспечением и проверка его подлинности;

- обучение персонала образовательного учреждения по вопросам обеспечения информационной безопасности в виде проведения занятий в целях формирования у них соответствующих знаний, умений и навыков, позволяющих соблюдать требования по обеспечению информационной безопасности образовательного учреждения;

- контроль за правильностью использования имеющихся в образовательном учреждении средств телефонной связи, выявление фактов нецелевого использования средств телефонной связи и принятие мер технического и организационного характера по их недопущению.

4.3. Общее руководство системой информационной безопасности образовательного учреждения осуществляет его директор.

5. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Организационное и техническое обеспечение рабочего процесса работников образовательного учреждения возлагается на педагогических работников.

5.2. С целью соблюдения принципа персональной ответственности за свои действия каждому работнику образовательного учреждения, допущенному к работе с конкретной подсистемой АС, должно быть сопоставлено персональное уникальное имя - учетная запись пользователя и пароль, под которым он будет регистрироваться, и работать в системе. Использование несколькими работниками при работе в АС одного и того же имени пользователя запрещено.

5.3. Проведение операций, указанных п. 4.2. работниками, не уполномоченными на проведение подобных действий, запрещено и идентифицируется как факт несанкционированного доступа.

5.4. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливается лаборантом по обслуживанию оргтехники при создании новой учетной записи. На нем же лежит ответственность за сохранность первичного пароля.

5.5. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью. Основной пароль - комбинация

символов (буквы, цифры, знаки препинания, специальные символы), известная только работнику образовательного учреждения, используемая для подтверждения подлинности владельца учетной записи.

Ответственность за сохранение в тайне основного пароля несет пользователь. Восстановление забытого основного пароля пользователя осуществляется лаборантом по обслуживанию оргтехники путем изменения (сброса) основного пароля пользователя на первичный пароль.

5.6. Для исполнения задач, связанных с производственной деятельностью работникам образовательного учреждения предоставляется доступ к ресурсам Интернет. Доступ к ресурсам Интернет в других целях запрещен.

5.7. К использованию в образовательном учреждении допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка средств антивирусного контроля на компьютерах (серверах ЛВС) образовательного учреждения осуществляется лаборантом по обслуживанию оргтехники. Установка и изменение настроек другими работниками образовательного учреждения запрещены.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

5.8. Антивирусная проверка должна проводиться:

- на компьютерах работников образовательного учреждения - не реже одного раза в неделю;

на серверах - не реже двух раз в неделю.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) лаборант по обслуживанию оргтехники должен провести внеочередной антивирусный контроль рабочей станции.

5.9. Правила работы работников и обучающихся образовательном учреждении в компьютерных сетях приведены в Приложении 1.

Приложение 1

Правила
работы работников и обучающихся в компьютерных сетях

1. Данные правила регулируют права и обязанности обучающихся образовательного учреждения, связанные с работой в компьютерной сети образовательного учреждения и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и работников образовательного учреждения.

Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности обучающихся.

2. Основными принципами политики образовательного учреждения для работы обучающихся в Сетях являются:

- равный доступ для всех обучающихся;
- использование Сетей обучающимися только для образовательных целей;
- защита обучающихся от вредной или незаконной информации, содержащей: порнография, пропаганда насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр и т.п.

3. Директор образовательного учреждения по безопасности образовательного процесса:

- организует и руководит всей деятельностью по реализации настоящих Правил;
- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;
- обеспечивать общую безопасность и эффективность работы в Сетях;
- предлагать и осуществлять меры по ограничению доступа обучающихся к вредным или незаконного содержания ресурсам в Сетях в соответствии с законодательством;
- периодически просматривать содержимое Сети образовательного учреждения с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;

5. Педагогические работники компьютеризированных кабинетов обязаны:

- разъяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;
- использовать возможности Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания;
- осуществлять непрерывный контроль работы обучающихся в Сетях в учебное время;

- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;

- немедленно сообщать директору образовательного учреждения о нарушении настоящих Правил или о создании незаконного контента в сети образовательного учреждения;

- не покидать учебный кабинет во время занятий и не допускать обучающихся во время перемены к работе в Сетях.

6. Педагогические работники несут ответственность за целостность оборудования образовательного учреждения, закрепленного за учебным кабинетом, в котором проводят занятия.

7. Права и обязанности обучающихся:

7.1. Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации образовательного учреждения;

-на получение доступа к сети Интернет (только под наблюдением преподавателя);

- на грамотное и ответственное обучение работе в Сетях;

- быть информированным о правилах работы в Сетях.

7.2. Обучающиеся обязаны соблюдать следующие правила:

- использовать Сети только для образовательных целей;

- не выходить на сайты, не включенные в перечень педагогическим работником для данного занятия;

- немедленно сообщить педагогическому работнику при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;

- не проводить любую деятельность, которая угрожает целостности компьютерной сети образовательного учреждения или атаки на другие системы;

- не использовать нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

8. Обучающиеся несут ответственность за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с Правилами внутреннего распорядка образовательного учреждения.

9. Педагогические работники и иные работники образовательного учреждения за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом Российской Федерации.

10. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб имуществу собственности образовательного учреждения, виновные несут ответственность в соответствии с законодательством Российской Федерации.

Приложение 2

Правила работы с ресурсами сети Интернет

1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Образовательное учреждение имеет право ограничивать доступ:

- к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению работниками образовательного учреждения трудовых обязанностей;
- к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством;
- к ресурсам, несущим вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

2. При работе с ресурсами сети Интернет недопустимо:

- разглашение коммерческой и служебной информации образовательного учреждения, ставшей известной работнику образовательного учреждения в связи с исполнением трудовых обязанностей либо иным путем;
- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

3. При работе с ресурсами Интернет запрещается:

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой компании.

4. Возможность получить доступ к ресурсам Интернета не является гарантией того, что запрошенный ресурс является разрешенным политикой образовательного учреждения.