КОМИТЕТ ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ЛЕНИНГРАДСКОЙ ОБЛАСТИ
Государственное автономное нетиповое профессиональное образовательное учреждение Ленинградской области
«МУЛЬТИЦЕНТР СОЦИАЛЬНОЙ И ТРУДОВОЙ ИНТЕГРАЦИИ»
(ГАНПОУ ЛО «МЦ СиТИ»)

ПРИКАЗ

14.07.2022 № 01.1-06/56-п

г. Всеволожск

О мерах повышения защищенности информационной безопасности и утверждения Порядка действий работников ГАНПОУ ЛО «МЦ СиТИ» в условиях повышения защищенности информационной безопасности

В целях предупреждения утечки персональной информации, организации обеспечения информационной безопасности в Государственном автономном нетиповом профессиональном образовательном учреждении Ленинградской области «Мультицентр социальной и трудовой интеграции» (далее – Учреждение), распределения функций и ответственности за обеспечение информационной безопасности между подразделениями и работниками Учреждения, а также на основании письма №22-04-18-2029/2022 от 13.07.2022 Комитета цифрового развития Ленинградской области

ПРИКАЗЫВАЮ:

1. Утвердить Порядок действий работников ГАНПОУ ЛО «МЦ СиТИ» в условиях повышения защищенности информационной безопасности (Приложение №1).
2. Работникам Учреждения при получении электронного письма, содержащего вредоносное вложение незамедлительно обратиться к сетевому администратору, с целью предотвращения реализации угроз безопасности информации и действовать в строгом соответствии с Порядком действий работников ГАНПОУ ЛО «МЦ СиТИ» в условиях повышения защищенности информационной безопасности.
3. Руководителям структурных подразделений ознакомить с настоящим приказом работников соответствующих структурных подразделений.
4. Настоящий приказ вступает в силу с момента подписания.
5. Документоведу первой категории ознакомить ответственных лиц согласно листу ознакомления
6. Контроль за исполнением приказа возложить на заместителя директора по инженерно-технической работе.

Директор И.Г. Дрозденко

Приложение №1
к приказу №01.1-06/56к от «14» 04 2022 г.

УТВЕРЖДЕНО
приказом директора
ГАНПОУ ЛО «МЦ СиТИ»
№ 01.1-06/56к от 14.04. 2022 г.

Порядок
действий работников Государственного автономного нетипового профессионального образовательного учреждения Ленинградской области «Мультицентр социальной и трудовой интеграции» в условиях защищенности повышения информационной безопасности

г. Всеволожск
2022

1. Общие положения

1.1. Настоящий Порядок устанавливает порядок организации и правила обеспечения информационной безопасности в Государственном автономном нетиповом профессиональном образовательном учреждении Ленинградской области «Мультицентр социальной и трудовой интеграции» (далее - Порядок), распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками, требования по информационной безопасности к используемым средствам информатизации осуществляемых в Государственном автономном нетиповом профессиональном образовательном учреждении Ленинградской области «Мультицентр социальной и трудовой интеграции» (далее – ГАНПОУ ЛО «МЦ СиТИ», Учреждение).

Действие Порядка распространяются на все структурные подразделения Учреждения, в которых для работы с информацией применяются различного рода технические средства.

1.2. В Порядке используются следующие основные термины и определения:

сетевой администратор - сотрудник Учреждения, отвечающий за поддержание работоспособности локальной вычислительной сети и разграничение доступа к информационным ресурсам этой сети;

безопасность информации – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.;

доступ к информации – комплекс организационно-технических мероприятий, позволяющих сотруднику получить возможность ознакомления с информацией, в том числе с помощью технических средств, в соответствии с предоставленными ему для этого правами;

защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и(или) правил на изменение информации, приводящего к её искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

защита информации от несанкционированного доступа – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами и собственником (Учреждение) прав или правил доступа к защищаемой информации;

информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), используемые в целях принятия решений;

информация Учреждения – информация, принадлежащая Учреждению, то есть:

– созданная Учреждением (его сотрудниками) в процессе его деятельности;

– приобретенная Учреждением на законных основаниях;

– переданная Учреждением его партнерами (клиентами) при установлении сотрудничества на правах совместного владения;

– полученная в результате целенаправленного сбора информации подразделениями Учреждения;

информационная безопасность – состояние защищённости информационной среды, обеспечивающее минимизацию ущерба, вызванного возможной утечкой защищаемой информации, а также несанкционированных и непреднамеренных воздействий;

нарушение информационной безопасности – факт несанкционированного или непреднамеренного действия (операции) над информационной сферой, приводящий к нежелательным для предприятия последствиям;

обработка информации – совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией;

система защиты информации – совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации;

средства связи – технические средства, используемые для формирования, обработки, передачи или приёма сообщений электросвязи либо почтовых отправлений;

техническая защита информации – защита (не криптографическими методами) информации, содержащей сведения, составляющие государственную или коммерческую тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях её уничтожения, искажения и блокирования, и противодействие техническим средствам разведки;

угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированным и/или непреднамеренным воздействиям на неё;

шифрование – способ защиты информации, заключающийся в криптографическом преобразовании информации по специальному алгоритму для получения шифротекста и позволяющий предотвратить ее несанкционированное использование;

цифровая подпись – дополнительные данные или криптографическое преобразование какого-либо блока данных, позволяющие получателю блока данных убедиться в подлинности отправителя и целостности блока данных и защитить его от искажения с помощью, например, средств получателя.

Формы нарушения информационной безопасности:

а) пассивные

- получение информации нарушителем для использования в своих целях;
- анализ характеристик информации без доступа к самой информации;

б) активные

- изменение информации;
- внесение ложной информации
- нарушение (разрушение) информации;
- нарушение работоспособности системы обработки информации.

Принципы информационной безопасности:

- системный подход, предусматривающий комплексное решение проблемы информационной безопасности;
- ответственность всех сотрудников;
- непрерывность мер информационной безопасности;
- документальность любого действия в информационной системе для установления в
- последующем причины, авторства и самого факта совершения действия;
- компетентность в осуществлении мер информационной безопасности.

2. Меры, методы и средства обеспечения информационной безопасности.

2.1. Меры обеспечения информационной безопасности.

2.1.1. Законодательные (правовые) меры обеспечения информационной безопасности к правовым мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем Учреждения.

2.1.2. Технологические меры обеспечения информационной безопасности к данному виду мер обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

2.1.3. Организационные (административные) меры обеспечения информационной безопасности.

Организационные (административные) меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются:

– регламентация доступа в здание Учреждения;

– регламентация допуска работников к использованию информационных ресурсов;

– анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;

– обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники;

– обучение пользователей; деятельность по обеспечению информационной безопасности;

– условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами Учреждения.

2.1.4. Физические меры обеспечения информационной безопасности.

Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

2.1.5. Технические меры обеспечения информационной безопасности.

Технические (аппаратно-программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации)

3. Порядок действий сотрудников Учреждения в условиях повышения информационной безопасности

3.1. С целью предотвращения реализации угроз безопасности информации Учреждения, сотрудники Учреждения, работающие с информацией должны принять следующие меры защиты информации:

3.1.1. Проверить адрес отправителя на предмет соответствия официальному адресу отправителя.

3.1.2. Осуществлять проверку вложений, содержащихся в электронных письмах, средствами антивирусной защиты до их вскрытия.

3.1.3. Активировать (при возможности) механизмы проверки электронной почты, проверки подлинности домена отправителя (например, использовать технологии SPF, DKIM, DMARC), а также настроить проверку входящих писем с использованием этих технологий.

3.2. В случае получения подозрительного письма сотрудник Учреждения, должен обратиться к сетевому администратору Учреждения для его проверки.

4. Заключительные положения.

4.1. Настоящий Порядок вступает в силу с момента его принятия и действует до официальной отмены или принятия Порядка в новой редакции.

КОМИТЕТ ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ЛЕНИНГРАДСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ НЕТИПОВОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЛЕНИНГРАДСКОЙ ОБЛАСТИ «МУЛЬТИЦЕНТР СОЦИАЛЬНОЙ И ТРУДОВОЙ ИНТЕГРАЦИИ»

ЛИСТ СОГЛАСОВАНИЯ ПРОЕКТА ПРИКАЗА

О мерах повышения защищенности информационной безопасности и утверждения Порядка действий работников ГАНПОУ ЛО «МЦ СиТИ» в условиях повышения защищенности информационной безопасности

ФИО и должность лица, осуществляющего согласование	**Отметка о согласовании (согласовано /не согласовано) Краткое изложение причин отказа в согласовании**	**Дата согласования**	**Подпись**
Зам. директора по инженерно-технической работе **К.Б. Полнов**	Согласовано		
Начальник правового отдела **А.А. Багдасарян**	ГАНПОУ ЛО «МЦ СиТИ» ПРАВОВОЙ ОТДЕЛ СОГЛАСОВАНО «__» _____ 20___ г.		

Инициатор проекта:
Юрисконсульт правового отдела И.С. Малинина