МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ «РОВЕНЬКОВСКИЙ ТЕХНИКО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ»
(ГОУ СПО ЛНР «РТЭК»)

СОГЛАСОВАНО:
Председатель
ППО РТЭК ПРУП ЛНР
_____ О. А. Дудник
«10» октября 2023 года

УТВЕРЖДЕНО:
И.о. директора
ГОУ СПО ЛНР «РТЭК»
_____ А.С. Дудник
«10» октября 2023 год
Приказ от 10.10.2023 № 133-од

ПОЛОЖЕНИЕ
«ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ГОСУДАРСТВЕННОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
«РОВЕНЬКОВСКИЙ ТЕХНИКО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ».

г. Ровеньки 2023

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Положение об информационной безопасности (далее – Положение) в Государственном образовательном учреждении среднего профессионального образования Луганской Народной Республики «Ровеньковский технико-экономический колледж» (далее – Колледж) регламентирует вопросы информационной безопасности в Колледже.

1.2 Положение разработано в соответствии с:

– Конституцией Российской Федерации;

- главой 14 Трудового кодекса РФ;

– Федеральным законом от 29.12.2012 № 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»;

– постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– уставом Колледжа;

– другими федеральными законами, иными нормативными правовыми актами Российской Федерации, законами и иными нормативными правовыми актами Луганской Народной Республики, локальными нормативными актами Колледжа, содержащими нормы, регулирующие отношения в сфере образования, сфере защиты персональных данных, защиты информации.

1.3 Под информационной безопасностью (далее – ИБ) Колледжа понимается состояние защищённости информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности от случайного или преднамеренного вмешательства в нормальный процесс функционирования.

ИБ - деятельность, направленная на обеспечение защищенного состояния объекта информации, в том числе объектов автоматизированных и телекоммуникационных систем.

1.4 ИБ обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных, обучающихся. преподавателей, сотрудников Колледжа, с целью обеспечения доступности, целостности и конфиденциальности, связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

1.5 ИБ достигается защитой персональных данных, а также информации от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

1.6 ИБ в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим группам:

– персональные данные и сведения, которые имеют отношения к обучающимся, преподавательскому составу, персоналу Колледжа, оцифрованные архивные документы;

– обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения образовательного процесса;
– защищенная законом интеллектуальная собственность.

1.7 Обеспечение ИБ осуществляется по следующим направлениям:
– правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
– организационная защита – это регламентация деятельности образовательной организации 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.

1.8 Информационная безопасность включает:
- защиту интеллектуальной собственности Колледжа;
- защиту компьютеров, локальных сетей и сети подключения к системе Интернета;
- организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;
- учет всех носителей конфиденциальной информации.

2. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1 Основной целью, на достижение которой направлено настоящее Положение, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, её незаконного использования и нарушения работы информационной среды Колледжа.

2.2 Основными задачами обеспечения безопасности информации являются:

– соответствие положениям законодательных актов и нормативным требованиям по защите информации;

– своевременное выявление, оценка и прогнозирование источников угроз ИБ, причин и условий, способствующих нанесению ущерба интересам Колледжа, нарушению нормального функционирования и развития Колледжа;

– создание механизма оперативного реагирования на угрозы ИБ 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;

– развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз ИБ и ликвидации последствий ее нарушения;

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

– создание механизмов управления системой ИБ;

- координация деятельности преподавателей, сотрудников, структурных подразделений Колледжа по обеспечению защиты информации.

3. ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОЛЛЕДЖА

3.1 Информационные ресурсы, содержащие конфиденциальную информацию, персональные данные, представленные в виде документированных информационных массивов и баз данных.

3.2 Открытая (общедоступная) информация, необходимая для работы Колледжа, независимо от формы и вида ее представления.

3.3 Средства и системы информатизации, программные средства, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

3.4 Процессы обработки информации в информационных системах Колледжа, информационные технологии, регламенты и процедуры сбора, обработки, хранения, анализа и передачи информации.

3.5 Системы и средства защиты информации.

4. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОЛЛЕДЖА

4.1 Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты информации Колледжа в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, утвержденных органами государственной власти.

4.2 Системность.

Системный подход к построению системы защиты информации в Колледже предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения ИБ Колледжа.

4.3 Комплексность.

Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.4 Непрерывность защиты.

Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий).

4.5 Своевременность.

Предполагается упреждающий характер мер обеспечения ИБ, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем.

4.6 Персональная ответственность.

Предполагает возложение ответственности за обеспечение ИБ на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был чётко известен или сведен к минимуму.

4.7 Минимизация полномочий.

Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

4.8 Простота применения средств защиты.

Механизмы и методы системы защиты информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не требует от пользователя выполнения малопонятных ему операций.

4.9 Обоснованность и техническая реализуемость.

Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по ИБ.

4.10 Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы сотрудников. Также реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами Колледжа.

4.11 Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей.

Выявленные сотрудниками Колледжа недостатки системы защиты информации доводятся до сведения руководителя Колледжа.

5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1 Спецификой обеспечения ИБ в Колледже является состав характерных угроз. К ним относится не только возможность хищения или повреждения данных, но также деятельность преподавателей, сотрудников, студентов, которые могут сознательно или ненамеренно повредить оборудование или заразить систему вредоносными программами.

Существуют два вида угроз ИБ:

- Искусственные угрозы – это угрозы, вызванные деятельностью человека;
- Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

5.2 Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

– компьютерное и другое оборудование Колледжа, в отношении которого возможны воздействия вредоносного программного обеспечения, физические и другие воздействия;

– программное обеспечение, применяемое в образовательном процессе или для работы системы;

– данные, которые хранятся на жестких дисках или портативных носителях.

5.3 Основные источники угроз ИБ Колледжа:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем Колледжа (в том числе сотрудников, отвечающих за обслуживание и администрирование элементов информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам Колледжа пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование элементов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем Колледжа;
- удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;
- ошибки, допущенные при разработке элементов информационных систем Колледжа и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);
- технические сбои элементов информационных систем.

5.4 Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации достаточно эффективно и быстро устраняются подготовленным персоналом.

5.5 К более опасным относятся угрозы ИБ намеренного характера, результаты реализации которых, невозможно предвидеть. Намеренные угрозы могут исходить от обучающихся, работников Колледжа.

5.6 Существенную угрозу представляет хищение персональных данных, интеллектуальной собственности и нарушение авторских прав.

6. ПУТИ РЕАЛИЗАЦИИ НЕПРЕДНАМЕРЕННЫХ И ПРЕДНАМЕРЕННЫХ УГРОЗ ИБ КОЛЛЕДЖА

6.1 Сотрудники Колледжа, являющиеся авторизованными субъектами доступа информационных систем, а также сотрудники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз ИБ Колледжа (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Колледжа;
- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т.п.);
- игнорирование установленных правил при работе с информационными ресурсами;
- проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем и ИБ Колледжа;
- пересылка информации по ошибочному электронному адресу (устройства);
- ввод ошибочных данных;
- неосторожная порча носителей информации;
- неосторожное повреждение каналов связи;
- неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;
- заражение компьютеров *вирусами;*
- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);
- некомпетентное использование, настройка или неправомерное отключение средств защиты.

6.2 Пути реализации преднамеренных искусственных (субъективных) угроз ИБ - основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем Колледжа из строя, несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Колледжа;
- действия по дезорганизации функционирования информационных систем Колледжа, хищение электронных документов и носителей информации;
- несанкционированное копирование электронных документов и носителей информации;
- умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);
- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);
- несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;
- незаконное использование элементов информационных систем, нарушающее права третьих лиц.

7. ПРАВОВЫЕ НОРМЫ ОБЕСПЕЧЕНИЯ ИБ

7.1 Колледж имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников колледжа, требовать от своих работников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

7.2 Колледж обязан обеспечить сохранность конфиденциальной информации.

7.3 Администрация Колледжа:

– назначает ответственного за обеспечение ИБ;
– имеет право включать требования по обеспечению ИБ 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 колледжа со стороны государственных и судебных инстанций.

7.4 Порядок допуска работников колледжа к информации предусматривает:

– принятие работниками Колледжа обязательств о неразглашении доверенных им сведений конфиденциального характера;
– ознакомление сотрудников с нормами законодательства РФ и Колледжа об ИБ и ответственности за разглашение информации конфиденциального характера;
– инструктаж работников специалистом по ИБ;
– контроль сотрудников Колледжа лицом, ответственным за ИБ, при работе с информацией конфиденциального характера.

8. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИБ

В целях реализации стоящих перед системой обеспечения ИБ задач в Колледже устанавливаются:

– защита интеллектуальной собственности образовательной организации;
– защита компьютеров, локальных сетей и сети подключения к системе Интернет;

– организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Колледжа;

– учет всех носителей конфиденциальной информации;

– контроль над использованием электронных средств информационного обеспечения деятельности Колледжа по прямому назначению;

– противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности образовательной организации нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

– принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

– обучение работников Колледжа по вопросам обеспечения ИБ;

– контроль за правильностью использования имеющихся в колледже средств информационного обеспечения.

9. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ И РАБОТНИКОВ КОЛЛЕДЖА ПО ОБЕСПЕЧЕНИЮ ИБ

9.1 Директор Колледжа организует работу по построению системы обеспечения ИБ в образовательном учреждении, а именно:

- назначает ответственного за организацию ИБ из числа сотрудников Колледжа;
- утверждает круг лиц, имеющих доступ к защищаемой информации и порядок их работы;
- утверждает комплект документов, определяющих политику в отношении ИБ и защиты информации в Колледже, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ.

9.2 Ответственный за организацию ИБ:

- разрабатывает организационно-распорядительные документы по вопросам ИБ и защиты информации при её обработке с помощью информационной системы;
- контролирует исполнение приказов и распоряжений директора Колледжа по вопросам обеспечения и соблюдения ИБ;
- обеспечивает защиту информации в Колледже;
- проводит систематический контроль работы систем защиты информации, применяемых в информационной системе, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей информационной системы;
- участвует в работах по внесению изменений в аппаратно-программную конфигурацию информационной системы;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав информационной системы;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к информационной системе;
- требует устранения выявленных нарушений и недостатков, дает обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
-требует от работников представления письменных объяснений по фактам нарушения

режима конфиденциальности;
- в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает директору Колледжа.

9.3 Права, обязанности преподавателей, сотрудников Колледжа по обеспечению ИБ приведены в Инструкции по информационной безопасности для сотрудников Государственного образовательного учреждения среднего профессионального образования Луганской Народной Республики «Ровеньковский технико-экономический колледж» (ГОУ СПО ЛНР «РТЭК») - (Приложение № 1).

10. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИБ

10.1 Организованное подключение средства защиты, обеспечивающего контроль и фильтрацию сетевого трафика.

10.2 Принятие мер по разграничению доступа между сетями, взаимодействующими с сетью «Интернет» через самостоятельно организованное подключение, и имеющими несанкционированный доступ потенциальных нарушителей безопасности информации и вредоносного ПО, и иным сторонним ресурсам.

10.3 Соблюдение парольной политики, установленной для конкретного ресурса его создателем.

10.4 Использование актуальных версий средств защиты информации.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1 Настоящее Положение принимается на неопределенный срок.

11.2 Данное Положение вступает в силу со дня его утверждения директором Колледжа.

Приложение № 1

ИНСТРУКЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СОТРУДНИКОВ ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ «РОВЕНЬКОВСКИЙ ТЕХНИКО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ» (ГОУ СПО ЛНР «РТЭК»)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Инструкция определяет основные права, обязанности, ответственность, порядок действий преподавателей, сотрудников ГОУ СПО ЛНР «РТЭК», допущенных к обработке конфиденциальной информации, в том числе по средствам технических средств, при работе с ресурсами и сервисами сети Интернет.

1.2 Преподаватели, сотрудники при выполнении работ в пределах своих функциональных обязанностей обеспечивают безопасность конфиденциальной информации и несут персональную ответственность за соблюдение требований руководящих документов по защите информации, а именно:

- Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями);
- Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных (с изменениями);
- Федерального закона «О связи» от 07.07.2003 № 126-ФЗ (с изменениями);
- Федерального закона «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (с изменениями);
- постановления Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- других законодательных актов, руководящих и нормативно-методических документов Российской Федерации в области обеспечения информационной безопасности.

2. ОРГАНИЗАЦИЯ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В ГОУ СПО ЛНР «РТЭК»

2.1 Доступ к информационным ресурсам несовместимым с целями и задачами образования и воспитания студентов запрещен.

2.2 При использовании сети Интернет преподавателям, сотрудникам предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу, а также выполнению работ в пределах функциональных обязанностей преподавателей и сотрудников.

2.3 При использовании ресурсов сети Интернет обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

2.4 При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

2.5 Все компьютеры, подключаемые к сети Интернет, обязаны иметь установленное действующее и обновляющееся антивирусное программное обеспечение

2.6 К работе в сети Интернет допускаются лица, ознакомившиеся с настоящей инструкцией и обязавшиеся соблюдать правила работы. Доступ к ресурсам сети Интернет предоставляется преподавателям, сотрудникам ГОУ СПО ЛНР «РТЭК» исключительно для исполнения задач, связанных с образовательной и производственной деятельностью.

3. ПРАВА ПРЕПОДАВАТЕЛЕЙ, СОТРУДНИКОВ, ИМЕЮЩИХ ДОСТУП К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ И СЕТИ «ИНТЕРНЕТ»

3.1 Использовать ресурсы локальной сети и сети Интернет в целях образовательного процесса и выполнения работ в пределах функциональных обязанностей.

3.2 Бесплатно пользоваться доступом к глобальным Интернет-ресурсам.

3.3 Вносить предложения по совершенствованию мер информационной безопасности в ГОУ СПО ЛНР «РТЭК».

3.4 Обращаться к ответственному по информационной безопасности сотруднику для оказания необходимой технической и методологической помощи в своей работе.

3.5 Работать в сети Интернет в течение периода рабочего времени.

3.6 Сохранять полученную информацию на съемном диске (дискете, CD, флеш-накопителе).

4. ОБЯЗАННОСТИ ПРЕПОДАВАТЕЛЕЙ, СОТРУДНИКОВ, ИМЕЮЩИХ ДОСТУП К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ И СЕТИ «ИНТЕРНЕТ»

4.1 Знать требования руководящих документов по защите персональных данных, защите информации (пункт 1.2 настоящей Инструкции).

4.2 Строго соблюдать установленные правила обеспечения безопасности персональных данных, защиты информации при работе с программными и техническими средствами.

4.3 При наличии средства электронной подписи (далее – ключ ЭП) использовать для работы только рабочую копию своего ключевого носителя.

4.4 Сдавать свой ключ ЭП на временное хранение руководителю ГОУ СПО ЛНР «РТЭК» или ответственному за информационную безопасность сотруднику в период отсутствия на рабочем месте (например, на время отпуска или командировки).

4.5 Держать включённым антивирусное программное обеспечение на компьютере.

4.6 Ежедневно проверять состояние антивирусного программного обеспечения.

4.7 Быть крайне осторожным при работе с электронной почтой.

4.8 В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.

4.9 Хранить в тайне свой пароль (пароли).

5. ПРЕПОДАВАТЕЛЯМ, СОТРУДНИКАМ, ИМЕЮЩИМ ДОСТУП К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ И СЕТИ «ИНТЕРНЕТ», ЗАПРЕЩЕНО:

5.1 Посещать сайты, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушают законодательство Российской Федерации (пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности).

5.2 Загружать и распространять материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ.

5.3 Загружать и запускать файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

5.4 Распространять информацию, порочащую честь и достоинство граждан.

5.5 Осуществлять любые сделки через сеть Интернет.

5.6 Работать с объемными ресурсами (видео, аудио, чат, фото) без согласования с лицом, назначенным ответственным за организацию работы в сети Интернет.

5.7 Использовать чужие имена пользователей, чужие пароли и чужую электронную почту.

5.8 Электронная почта является собственностью ГОУ СПО ЛНР «РТЭК» и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено. Кроме этого категорически запрещено:

- открывать присоединенные к письмам, полученным от незнакомых лиц, файлы;
- использовать адрес почты ГОУ СПО ЛНР «РТЭК» для оформления подписок и массовых рассылок;
- публиковать свой адрес, либо адреса других сотрудников колледжа на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- осуществлять массовую рассылку почтовых сообщений рекламного характера;
- распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством, включая материалы, носящие 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. распространять информацию ограниченного доступа, представляющую коммерческую тайну;
- предоставлять кому бы то ни было пароль для доступа к почтовому адресу электронной почты ГОУ СПО ЛНР «РТЭК».

5.9 Использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

5.10 Устанавливать самостоятельно на персональный компьютер какие-либо аппаратные или программные средства.

5.11 Отключать средства антивирусной защиты информации.

5.12 Без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5.13 Осуществлять обработку конфиденциальной информации (персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц.

5.14 При наличии ключа ЭП оставлять ключевой носитель без личного присмотра; передавать свой ключ ЭП другим лицам (кроме как для хранения руководителю или ответственному за информационную безопасность); делать неучтенные копии ключа ЭП, вносить изменения в файлы, находящиеся на ключе ЭП и т.д.

5.15 Осуществлять обработку конфиденциальной информации (персональных данных) при подключенном ПК к сети Интернет.

5.16 Оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются.

5.17 Оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию.

5.18 Предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом.

6. ОТВЕТСТВЕННОСТЬ ПРЕПОДАВАТЕЛЕЙ, СОТРУДНИКОВ, ИМЕЮЩИХ ДОСТУП К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ И СЕТИ «ИНТЕРНЕТ»

6.1 Преподаватели, сотрудники ГОУ СПО ЛНР «РТЭК» несут ответственность согласно действующему законодательству за разглашение сведений, составляющих служебную, коммерческую тайну (в том числе персональные данные) и сведений ограниченного распространения, ставших им известными по роду работы.

Нарушения требований законодательства в сфере защиты информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в зависимости от ситуации и в соответствии с законодательством Российской Федерации.

6.2 Нарушения установленных правил и требований по обеспечению информационной безопасности также могут являться основанием для применения к преподавателям, сотрудникам мер наказания, предусмотренных трудовым законодательством.

6.3 За нанесение любого ущерба оборудованию (порча имущества, вывод оборудования из рабочего состояния) в результате нарушения установленных правил и требований по обеспечению информационной безопасности преподаватели, сотрудники ГОУ СПО ЛНР «РТЭК» несут материальную ответственность в соответствии с законодательством.

6.4 Также предусмотрена ответственность за разглашение пароля, выдаваемого для работы с информационными ресурсами, и за содержание передаваемой, принимаемой и печатаемой информации.

ВЕДОМОСТЬ ОЗНАКОМЛЕНИЯ
С ИНСТРУКЦИЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ДЛЯ СОТРУДНИКОВ ГОУ СПО ЛНР «РТЭК»

Ф.И.О.	Подпись	Дата ознакомления	№ п/п	Ф.И.О.	Подпись	Дата ознакомления
Аверков В. В.		10.10.23	36	Липко С. М.		28.11.2023
Амбицкая-Шеремет Н. Н.		28.XI.23	37	Литовченко Л. А.		28.11.23
Антонова И. Ю.		29.11.23	38	Лозыченко Е. Г.		10.10.2023
Баранова Л. Г.		10.10.23	39	Лукьянчикова Н. М.		29.11.2023
Безпальчая М. С.		10.10.23	40	Маловичко И. В.		10.10.23
Белокур А. Ш.		10.10.23	41	Мальцева О. Н.		10.10.23
Богатырёва Н. Б.		10.10.23	42	Медведева Р. С.		5.12.23
Бойко А. Н.		05.12.23	43	Митцель Н. П.		10.10.23
Бувака С. В.		10.10.23	44	Назаров С. А.		10.10.23
Василенко К. В.		8.12.23	45	Назарова А. Н.		10.10.23
Вовк Е. А.		10.10.23	46	Нелубкина З. Е.		8.12.23
Гайдаенко Е. С.		10.10.23	47	Нестеренко А. Н.		10.10.23
Галынкер Т. И.		10.11.23	48	Осадчая А. А.		08.12.23
Герасимова Н. В.		29.11.23	49	Охрименко Т. В.		10.10.23
Гришин В. А.		29.11.23	50	Пальчикова Н. А.		10.10.23
Дудник А. С.		10.10.23	51	Пичугина Л. Я.		10.10.23
Дудник О. А.		10.10.23	52	Погорелова Г. С.		10.10.23
Дьяченко В. А.		10.10.23	53	Прилуцкая Е. М.		10.10.23
Дьяченко И. А.		10.10.23	54	Руденко С. Г.		10.10.23
Дьячихин Д. А.		10.10.23	55	Рыбальченко А. В.		10.10.23
Евсеенко Е. В.		29.11.23	56	Свинарева Л. В.		10.10.23
Иблоцкая Л. М.	расчет	—	57	Сердюков Г. Ю.		10.10.23
Игорская Н. Я.		29.11.23	58	Склярова С. Н.		10.10.23
Иваниенко Н. А.		10.10.23	59	Старостенко А. Г.		10.10.23
Иващенко Ю. А.		28.10.23	60	Степанова Л. В.		10.10.23
Калашникова К. А.		10.1023	61	Стрельченко В. И.		10.10.23
Кашкарова Е. Н.		10.10.23	62	Терентьева Е. А.		29.11.2023
Колтунов С. Г.		10.10.23	63	Терзи В. В.		10.10.23
Кузнецова В. П.		12.12.23	64	Тихонова Е. И.		10.10.23
Курбатов В. Ю.		10.10.23	65	Фоменко И. В.		10.10.23
Куркина Т. Б.		10.10.23	66	Хорошаева Л. Г.		10.10.23
Луценко Л. И.		10.10.23	67	Шилина Е. А.		10.10.23
Ошнирук О. С.		10.10.23	68	Щербина А. П.		10.10.23
Назаренко Н. С.		5.12.23	69	Щетинин В. В.		10.10.23
Небединская В. В.		5.12.23	70	Юнусов А. М.		10.10.23

Прошито, пронумеровано и скреплено
печатью 15 (пятнадцать)
_____) лист(а/ов).

И. о. директора
ГОУ СПО ЛНР «РТЭК»
_____ С. Дудник
«10» октября 2023 г.