УТВЕРЖДАЮ
Директор
В.С.Зайцев
«30» 12 2020 г.
приказ №265-осн

ПОЛОЖЕНИЕ
об информационной безопасности
ГПОУ ТО «Узловский машиностроительный колледж»

1. Общие положения

1.1.Настоящее Положение об информационной безопасности ГПОУ ТО «Узловский машиностроительный колледж» разработано в соответствии с положениями:

- Конституции Российской Федерации;
- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федерального закона от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";
- Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
- Национального стандарта РФ ГОСТ Р ИСО/МЭК 27033-1-2011 "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. N 683-ст);
- общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности.

1.2. Положение об информационной безопасности определяет порядок доступа к информационным ресурсам государственного профессионального образовательного учреждения Тульской области «Узловский машиностроительный Колледж» (далее по тексту – Колледж), основные направления и способы защиты информации в Колледже.

1.3. Основные понятия, используемые в настоящем Положении:

информация - сведения (сообщения, данные) независимо от формы их представления;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.4. Основными целями информационной безопасности в Колледже являются:

- обеспечение управления и поддержки информационной безопасности в соответствии с требованиями Колледжа, соответствующими законами и нормами;
- защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;
- обеспечение целостности и конфиденциальности информации;
- обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности.

1.5. Основными задачами информационной безопасности Колледжа являются:

- доступность обрабатываемой информации;
- защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;
- контроль целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи Колледжа;
- обеспечения конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи Колледжа;
- защита детей от информации, причиняющей вред их здоровью и развитию в Колледже, а также от информации доступ к которой обучающимся запрещен;
- оценка рисков информационной безопасности.

1.6. Защите подлежит вся принимаемая, передаваемая, обрабатываемая и

хранимая информация, содержащая:

- сведения, составляющие служебную и коммерческую тайну, доступ к которым ограничен Колледжем, как собственником информации, в соответствии с положениями, предоставленными Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";
- персональные данные, доступ к которым ограничен в соответствии с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- открытые сведения в части обеспечения доступности и целостности информации.

1.7. Основными способами защиты информационных ресурсов Колледжа являются:

- оценка рисков сетевой безопасности;
- мониторинг информационной безопасности;
- системный аудит;
- антивирусный контроль;
- анализ инцидентов.

1.8. Основными средствами защиты информационных ресурсов Колледжа являются:

- криптографические средства: КриптоПро CSP; ViPNet CSP;
- средства обеспечения и контроля целостности программных и информационных ресурсов: Kaspersky Endpoint Security;
- средства идентификации и аутентификации пользователей: DALLAS LOCK 8.0;
- технические средства защиты: Kaspersky Endpoint Security.

1.9. Основные положения и требования настоящего положения распространяются на все структурные подразделения Колледжа.

2. Субъекты правоотношений, связанные с использованием информации и обеспечением ее безопасности

2.1. К субъектам правоотношений, связанных с использованием информационных ресурсов Колледжа и обеспечением их безопасности (далее - субъекты правоотношений), относятся:

- Колледж как собственник информационных ресурсов;
- работники Колледжа как пользователи информацией в соответствии с возложенными на них трудовыми обязанностями;
- внутренние структурные подразделения Колледжа, обеспечивающие эксплуатацию информационных ресурсов;
- иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в Колледже (далее - пользователи).

2.2. Информационные ресурсы Колледжа это электронные документы и (или) информация на машиночитаемых носителях, обычные документы, коллекции документов, документы и массивы документов в информационных системах

(библиотеках, архивах, фондах, банках данных, других информационных системах).

2.3. В целях организации процесса использования информационных ресурсов Колледж обязан обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

В целях организации процесса использования информационных ресурсов Колледж как обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

2.4. Доступ к информационным ресурсам Колледжа имеют работники Колледжа, наделенные полномочиями в соответствии с должностными инструкциями, локальными актами Колледжа, лица, определённые приказом директора Колледжа.

2.5. Уровень доступа к информационным ресурсам Колледжа определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;
- конфиденциальная и открытая информация Колледжа размещается на разных источниках хранения информации;
- непосредственный руководитель работника имеет право на просмотр информации, используемой работником.

В процессе использования информационных ресурсов Колледжа работники Колледжа обязаны:

- не разглашать конфиденциальную информацию, ставшую известной работнику в связи с выполнением его трудовых обязанностей, в течение действия

трудового договора и одного года со дня прекращения действия трудового договора;

- не разглашать ставшие ему известными, в связи с выполнением его трудовых обязанностей, сведения, относящиеся к персональным данным, в соответствии с действующей Политикой Колледжа в области обработки персональных данных, Положения об обработке и защите персональных данных в Колледже.

Все работники Колледжа должны быть ознакомлены персонально под роспись с организационно-распорядительными документами по информационной безопасности, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению защиты информации.

Работники Колледжа, наделенные правом доступа к конфиденциальной информации и (или) персональным данным, при приеме на работу подписывают обязательство о соблюдении требований по сохранению конфиденциальной информации и ответственности за их нарушение, а также о выполнении правил работы с информацией.

Все работники, допущенные к работе с информацией Колледжа, несут персональную ответственность за нарушение правил ее использования, передачи, хранения, а также требований по сохранению конфиденциальной информации и (или) персональных данных.

2.6. Пользователи (физические и юридические лица) имеют право доступа к информационным ресурсам Колледжа в части информации, которая обрабатывается, накапливается и хранится в Колледже в отношении них.

В процессе использования информационных ресурсов Колледжа пользователи обязаны соблюдать:

- требования локальных нормативных актов Колледжа, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- требования о неразглашении конфиденциальной информации и (или) персональных данных ставших известными им по любым причинам, в том числе независящим обстоятельствам;
- запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Для пользователей разрабатываются инструкции о порядке использования информационных ресурсов Колледжа, включающие требования по обеспечению безопасности информации.

До предоставления доступа к информационным ресурсам Колледжа пользователи должны быть ознакомлены с перечнем конфиденциальной информации, персональных данных и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

Пользователи, допущенные к работе с информационными ресурсами

Колледжа, несут ответственность за нарушение правил ее использования, передачи, хранения, а также требований по сохранению конфиденциальной информации.

3. Угрозы безопасности информации и их источники

3.1. Угрозы безопасности информации, с которыми сталкивается Колледж, могут быть связаны с проблемами:

- несанкционированного доступа к информации;
- несанкционированной передачи информации;
- внесения вредоносной программы, отказа от факта приема или источника информации;
- отказа в обслуживании и недоступности информации или услуг.

3.2. Указанные угрозы могут быть связаны с утратой:

- конфиденциальности информации и программы (в сетях и системах, соединенных с сетями);
- целостности информации и программы (в сетях и системах, соединенных с сетями);
- доступности информации и программ (и систем, соединенных с сетями);
- подотчетности сетевых транзакций;
- подлинности информации (а также аутентичности сетевых пользователей и администраторов);
- достоверности информации и программы (в сетях и системах, соединенных с сетями);
- способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов, включая осуществление контроля в контексте настоящего положения, выполнение обязательств в отношении законодательства и предписаний надзорных и контрольных органов;
- способности контролировать злоупотребление санкционированным доступом.

4. Оценка рисков сетевой безопасности

4.1. Для идентификации и подтверждения технических мер и средств контроля и управления безопасностью информации в Колледже проводится оценка риска сетевой безопасности.

Для этого выполняются следующие действия:

- определение степени значимости информации, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность Колледжа в случае возникновения нежелательных инцидентов;
- идентификация и оценка вероятности или уровней угроз, направленных против информации;
- идентификация и оценка степени серьезности или уровня уязвимостей (слабых мест), которые могли бы быть использованы идентифицированными угрозами;
- оценка величины рисков, основывающихся на определенных последствиях потенциального неблагоприятного воздействия на операции деятельности Колледжа и уровнях угроз и уязвимостей;

- идентификация аспектов специализированной архитектуры/проекта безопасности и оправданных потенциальных областей действия мер и средств контроля и управления безопасностью, необходимых для обеспечения того, чтобы оцененные риски оставались в допустимых пределах.

5. Мониторинг информационной безопасности

5.1. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих информацию, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

5.2. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей;
- периодическую, не реже шести месяцев, проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

5.3. Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий.

5.4. Мониторинг попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

5.5. Мониторинг производительности автоматизированных систем, обрабатывающих информацию, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

6. Системный аудит

6.1. Системный аудит производится ежеквартально и в особых ситуациях.

6.2. Системный аудит включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

6.3. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности.

6.4. Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

6.5. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

6.6. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.

Информация об известных уязвимостях извлекается из документации и внешних источников, затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

6.7. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале, уведомлением каждого сотрудника, которого касается изменение, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

7. Антивирусный контроль

7.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные

действия программ;

- утилиты для обнаружения и анализа новых вирусов.

7.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

7.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

7.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

7.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

7.6. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

7.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

7.8. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флеш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

7.9. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

7.10. На серверах систем, обрабатывающих персональные данные,

необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

7.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

7.12. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

7.13. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

7.14. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

8. Анализ инцидентов

8.1. Если администратор системы, обрабатывающей информацию, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (далее -НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точку входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

8.2. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях;
- выявить подозрительную активность пользователей;
- проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго;

- проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

8.3. При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

8.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

8.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

8.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

9. Организация контентной фильтрации для защиты обучающихся от нежелательной информации

9.1. Информация запрещенная к появлению на экранах компьютерных устройств субъектов образовательного процесса в Колледже указана в перечне видов информации, запрещенной к распространению посредством информационно-телекоммуникационной сети Интернет, причиняющей вред здоровью

и (или) развитию детей, а также не соответствующей задачам образования (приложение к настоящему положению).

9.2. Для организации защиты детей от вышеизложенной нежелательной информации в Колледже используются следующие мероприятия:

- использование системы контентной фильтрации (далее СКФ), которая устанавливается на компьютеры и мобильные устройства обучающихся;
- заключение с провайдером договора о фильтрации данных, поступающих через браузер на компьютеры Колледжа.

9.3. Средствами контент-фильтрации доступа в Интернет являются аппаратно-программные или программные комплексы, обеспечивающие ограничение доступа к интернет - ресурсам, не совместимым с задачами образования и воспитания обучающихся.

Наиболее применимы в Колледже три алгоритма фильтрации:

- фильтрация по ключевым словам - конкретные слова и словосочетания используются для включения блокировки веб-сайта;
- динамическая фильтрация - содержимое запрашиваемого веб-ресурса анализируется в момент обращения. Загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное;
- URL фильтрация - запрашиваемая страница или целый домен (например, dosug.nu) могут быть определены или категорированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется.

9.4. Средствами контент-фильтрации, используемые в Колледже, должны отвечать следующим требованиям:

- установка СКФ должна производиться на все компьютерное оборудование Колледжа участвующее в образовательном процессе обучающихся и имеющих доступ к Интернету;
- обеспечивать беспрепятственный доступ к информации, распространение к которой в Российской Федерации в соответствии с законодательством Российской Федерации не ограничивается или не запрещается;
- обеспечить мониторинг использования интернет ресурсов в образовательном процессе в целях обучения и воспитания обучающихся;
- обеспечить возможность адаптации к изменяющимся угрозам, условиями эксплуатации, требованиям законодательства Российской Федерации предписаниям надзорных органов;
- реализовывать единую политику для всех образовательных организаций по исключению доступа к интернет - ресурсам, несовместимым с задачами образования и воспитания обучающихся.

10. Особенности обеспечения безопасности конфиденциальной информации и защиты персональных данных

10.1. Обеспечение безопасности сведений содержащих конфиденциальную информацию и персональных данных в Колледже, представляет собой комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений содержащих конфиденциальную информацию, сведений относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

10.2. В комплекс мероприятий по защите конфиденциальной информации и персональных данных в Колледже входят:

- разработка необходимых документов в интересах Колледжа по обеспечению защиты конфиденциальной информации и персональных данных;
- обоснование требований по защите конфиденциальной информации и персональных данных в информационных ресурсах Колледжа;
- применение методики оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- определение состава и структуры программно-аппаратных средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
- иные мероприятия.

10.3. Обработка и защита конфиденциальной информации и персональных данных в Колледже осуществляется в соответствии с требованиями Законодательства Российской Федерации, иных правовых актах действующих на территории Российской федерации, Политике Колледжа в области обработки персональных данных, Положения об обработке и защите персональных данных в Колледже, Положения о конфиденциальной информации в Колледже и иных локальных нормативных актах Колледжа по вопросам обработки, защиты конфиденциальной информации и персональных данных.

10.4. Отнесение сведений к конфиденциальной информации и персональным данным осуществляется в соответствии с Гражданским кодексом Российской Федерации, федеральными законами Российской Федерации, определяются локальными нормативными актами Колледжа.

10.5. Персональные данные субъекта персональных данных являются конфиденциальной информацией и не могут быть использованы Колледжем или любым иным лицом в личных целях.

10.6. Колледж сообщает субъекту персональных данных о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

10.7. Персональные данные хранятся в информационных ресурсах Колледжа, в соответствии с локальными нормативными актами Колледжа.

10.8. Право доступа к персональным данным имеют:

- работники Колледжа, наделенные полномочиями в соответствии с должностными инструкциями, локальными актами Колледжа, лица, определённые приказом директора Колледжа;
- субъект персональных данных на доступ к своим персональным данным.

10.9. Колледж принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите конфиденциальной информации и персональных данных, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

Колледж самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по защите конфиденциальной информации и персональных данных, предусмотренных

Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

К таким мерам могут, в частности, относиться:

- назначение ответственного за организацию обработки персональных данных;
- издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;
- иные меры.

10.10. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

10.11. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

10.12. Лица, виновные в разглашении конфиденциальной информации, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

Моральный вред, причиненный владельцу конфиденциальной информации вследствие нарушения его прав, подлежит возмещению в соответствии с

законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных владельцем конфиденциальной информации убытков.

Положение об информационной безопасности ГПОУ ТО «Узловский машиностроительный колледж» принято на конференции работников и обучающихся «14» декабря 2020г., протокол № 3.

Приложение к Положению
об информационной безопасности
государственного профессионального
образовательного учреждения Тульской
области «Узловский
машиностроительный Колледж»
от 30. 12. 2020 г.

Перечень видов информации, запрещенной к распространению посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

№ п\п	Виды информации	Описание видов информации
Информация, запрещенная для распространения среди детей, согласно части 2 статьи 5 Федерального закона N 436-ФЗ*		
1.	Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая описания и\или изображения способов причинения вреда своему здоровью, самоубийства; обсуждения таких способов и их последствий, мотивирующих на совершение таких действий
2.	Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая рекламу, объявления, предложения и другую информацию, направленную на продажу детям наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий, алкогольную и спиртосодержащую продукции, а также вовлечение детей в азартные игры и использование или вовлечение в проституцию, бродяжничество или попрошайничество
3.	Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая акты насилия или жестокости, жертв насилия и жестокости, участников

		актов насилия и жестокости, обосновывающая, оправдывающая и вовлекающая детей в акты насилия и жестокости, а также формирующая культуру насилия и жесткости у несовершеннолетних
4.	Отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), рекламирующая, изображающая нетрадиционные сексуальные отношения, отказ от родителей (законных представителей), семьи и детей и влияющая на ухудшение и разрыв отношений детей с родителями и (или) другим членам семьи
5.	Оправдывающая противоправное поведение	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая призывы и вовлечение детей в противоправное поведение и одобряющая его
6.	Содержащая нецензурную брань	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая нецензурную брань
7.	Содержащая информацию порнографического характера	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, аудио и видеоматериалы по данной теме
8.	О несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учёбы или работы, иную информацию, позволяющую прямо	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, аудио и видеоматериалы по данной теме

или косвенно установить личность такого несовершеннолетнего	
9. Представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, видеоматериалы по данной теме
10. Вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, видеоматериалы по данной теме
11. Представляемая в виде изображения или описания половых отношений между мужчиной и женщиной	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, видеоматериалы по данной теме
12. Содержащая бранные слова и выражения, относящиеся к нецензурной брани	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, видеоматериалы по данной теме
Информация, не соответствующая задачам образования [1,2,3] (не имеет нормативного закрепления и используется для целей настоящих Методических рекомендаций)	
13. Компьютерные и сетевые игры, за исключением соответствующих задачам образования	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация) по тематике компьютерных игр, не соответствующим задачам образования, в

	том числе порталы браузерных игр, массовые многопользовательские игры и другие игры, игровой процесс которых осуществляется через сеть "Интернет"
14. Ресурсы, базирующиеся либо ориентированные на обеспечении анонимности распространителей и потребителей информации	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), обеспечивающие анонимизацию сетевого трафика в сети "Интернет", такие как анонимные форумы, чаты, доски объявлений и гостевые книги, анонимайзеры и другие программы и сервисы
15. Банки рефератов, эссе, дипломных работ, готовых домашних заданий и других информационных ресурсов, предоставляющих обучающимся готовые решения в форме материала, ответов и другой информации для осуществления ими учебной деятельности	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация) такие как сайты готовых рефератов, эссе, курсовых и дипломных работ, готовых домашних заданий, решебников, ответов на контрольные и самостоятельные работы и другие информационные ресурсы, направленные на предоставление обучающимся готовых решений в форме материала, ответов и другой информации, позволяющая им не осуществлять учебную деятельность самостоятельно
16. Онлайн-казино и тотализаторы	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая информацию об электронных казино, тотализаторах и других видах игр на денежные средства или их аналоги, а также способах и методах получения к ним доступа в сети "Интернет"
17. Мошеннические сайты	Сайты, навязывающие услуги на базе СМС-платежей, сайты, обманным путем собирающие личную информацию (фишинг)
18. Магия, колдовство, чарoдейство, ясновидящие, приворот по фото, теургия, волшебство, некромантия и секты	Информационная продукция, оказывающая психологическое воздействие на детей, при которой человек обращается к тайным силам с целью влияния на события, а также реального или кажущегося воздействия на состояние
19. Ресурсы, содержащие рекламу и направленные на продажу товаров и/или	Информационная продукция (в том числе сайты, сетевые средства массовой

услуг детям	информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), направленная на побуждение и создание заинтересованности у несовершеннолетних к убеждению родителей или других лиц либо самостоятельно приобрести товары и/или услуги
20. Службы знакомств, социальные сети, мессенджеры и сайты и сервисы для организации сетевого общения	Информационная продукция (в том числе сайты, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов), направленная на организацию общения между пользователями с помощью сети "Интернет", такая как служба знакомств, социальные сети, мессенджеры и другие сайты, сервисы и программы, направленные и предоставляющие необходимый функционал и возможности, за исключением электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность
21. Интернет-ресурсы, нарушающие исключительные права обладания (авторские права)	Информационная продукция (в том числе сайты, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов), направленная на предоставление пользователям сети "Интернет" информационного контента и программного обеспечения при нарушении авторского права, в форме торрентов, пиринговых сетей и других сайтов, сервисов и программ, предоставляющих необходимый функционал и возможности
22. Пропаганда национализма, фашизма и межнациональной розни	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, видеоматериалы по данной теме
23. Ресурсы, ориентированные на предоставление неправдивой информации об истории России и формирование неуважительного отношения к ней	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), содержащая текстовые описания, фотографии, рисунки, видеоматериалы по данной теме

24. Ресурсы, ориентированные на продажу документов об образовании и (или) обучении, без прохождения итоговой аттестации в организациях, осуществляющих образовательную деятельность	Информационная продукция (в том числе сайты, сетевые средства массовой информации, социальные сети, интерактивные и мобильные приложениях и другие виды информационных ресурсов, а также размещаемая на них информация), предлагающие приобрести за плату документ об образовании и (или) обучении без прохождения обучения и итоговой аттестации в организациях, осуществляющих образовательную деятельность