

Государственное профессиональное
образовательное учреждение
Тульской области
«Тульский колледж
профессиональных технологий и
сервиса» (ГПОУ ТО «ТКПТС»)



УТВЕРЖДАЮ
Директор
С.С. Курдюмов
2017 г.

ПОЛОЖЕНИЕ

31. 01. 2017 г. № 202

Об информационной безопасности

1. Назначение и область применения

1.1. Положение об информационной безопасности Государственного профессионального образовательного учреждения Тульской области «Тульский колледж профессиональных технологий и сервиса» (далее – Положение, колледж) регламентирует порядок организации и правила обеспечения информационной безопасности в колледже, распределение функций и ответственности за обеспечение информационной безопасности между сотрудниками колледжа, требования по информационной безопасности к информационным средствам, применяемым в колледже.

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

- автоматизированные системы колледжа;
- средства телекоммуникаций;
- помещения;
- сотрудников колледжа.

2. Общие положения

2.1. Информационная безопасность является одним из составных

элементов комплексной безопасности колледжа. Под информационной безопасностью колледжа понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

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

2.3. Информационная безопасность включает:

- защиту интеллектуальной собственности колледжа;
- защиту компьютеров и локальных сетей;
- организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;
- учет всех носителей конфиденциальной информации.

2.4. Информационная безопасность колледжа должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

2.5. К объектам информационной безопасности колледжа относятся:

- информационные ресурсы, содержащие документированную информацию;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

2.6. Правовую основу Положения составляют:

- Конституция Российской Федерации;
- Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;
- Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;
- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;
- Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ
- Другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

3. Цели и задачи обеспечения безопасности информации

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

3.2. Основными целями обеспечения безопасности информации являются:

- Предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в колледже;
- предотвращение нарушений прав личности обучающихся, работников колледжа на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации;

3.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным

- требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам колледжа, нарушению нормального функционирования и развития колледжа;
 - эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
 - координация деятельности структурных подразделений колледжа по обеспечению защиты информации;
 - развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
 - развитие и совершенствование защищенного электронного документооборота.

4. Организация системы обеспечения информационной безопасности

4.1. Система обеспечения информационной безопасности распространяются на:

- автоматизированные системы колледжа;
- средства телекоммуникаций;
- помещения;
- сотрудников колледжа.

4.2. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в колледже устанавливаются:

- защита персональных данных персонала и обучающихся;
- контроль за использованием электронных средств информационного обеспечения деятельности колледжа по прямому назначению;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности колледжа

электронных носителей информации способных произвести заражение программного обеспечения вирусами;

- внутрисетевой контроль за перемещением информации;
- принятие мер к воспрепятствованию доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- обучение персонала колледжа по вопросам обеспечения информационной безопасности - проведение бесед с персоналом в целях формирования у них соответствующих знаний, умений и навыков позволяющих соблюдать требования по обеспечению информационной безопасности колледжа.

5. Доступ к ресурсам сети Интернет

5.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам колледжа предоставляется доступ к ресурсам Интернет.

5.2. Доступ к ресурсам Интернет может быть заблокирован инженером-электроником без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

Правила работы с ресурсами Интернет приведены в приложении 1.

6. Электронная почта

6.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам колледжа может быть предоставлен доступ к электронной почте колледжа. Использование электронной почты колледжа в других целях запрещено.

6.2. Электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

7. Антивирусная защита

7.1. К использованию в колледже допускаются только лицензионные антивирусные средства.

7.2. Установка средств антивирусного контроля на компьютерах (серверах ЛВС) колледжа осуществляется уполномоченными сотрудниками.

Настройка параметров средств антивирусного контроля осуществляется инженером-электроником в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками запрещено.

Ежедневно в начале работы при загрузке в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютера.

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

7.3. Антивирусная проверка должна проводиться:

- на компьютерах сотрудников - не реже одного раза в неделю;
- на серверах ЛВС - не реже двух раз в неделю.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник самостоятельно или вместе с инженером-электроником должен провести внеочередной антивирусный контроль своей рабочей станции.

8. Хранение данных

8.1. Для обеспечения целостности данных необходимо проводить резервное копирование не реже одного раза в неделю. Резервное копирование личной информации не предусмотрено.

9. Установка и обслуживание оборудования

9.1. Установка и обслуживание оборудования возможна только сотрудниками отдела информационно-программного обеспечения. Установка и обслуживание оборудования другими сотрудниками запрещена.

9.2. Ответственность за устранение сбоев в работе оборудования лежит на сотрудниках отдела информационно-программного обеспечения.

Правила работы персонала и обучающихся колледжа в компьютерных сетях

Данные правила регулируют права и обязанности обучающихся, связанные с работой в компьютерной сети колледжа и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и сотрудников колледжа. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности студентов.

Основными принципами политики колледжа для работы в Сетях являются:

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

Правила работы в Сетях должны быть расположены в каждом компьютерном классе.

Преподаватели компьютерных классов обязаны:

- объяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;
- использовать возможности Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания и приводить перечень соответствующих интернет-адресов;
- осуществлять непрерывный контроль работы обучающихся в Сетях в

учебное время;

- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;
- немедленно сообщать сотрудникам отдела информационно-программного обеспечения о нарушении правил или о создании незаконного контента в сети колледжа;
- не покидать учебный кабинет во время пары, и не допускать обучающихся во время перемены к работе в Сетях;

Преподаватели несут ответственность за целостность оборудования колледжа, закрепленного за учебным кабинетом, в котором проводят занятия.

Сотрудники отдела информационно-программного обеспечения обязаны:

- обеспечивать общую безопасность и эффективность работы в Сетях;
- осуществлять меры по ограничению доступа обучающихся к вредным ресурсам в Сетях в соответствии с законодательством;
- просматривать содержимое компьютеров колледжа с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;

Права и обязанности обучающихся

Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации колледжа;
- на получение доступа к сети Интернет (только под наблюдением преподавателя);
- на грамотное и ответственное обучение работе в Сетях;
- быть информированным о правилах работы в Сетях.

Обучающиеся обязаны соблюдать следующие правила:

- использовать Сети только для образовательных целей;
- запрещается выход на сайты, не включенные в перечень преподавателем для данного занятия;

1. The first part of the document discusses the importance of maintaining accurate records of all transactions. It emphasizes that proper record-keeping is essential for the integrity of the financial system and for ensuring that all parties involved are held accountable for their actions.

2. The second part of the document outlines the specific procedures that must be followed when recording transactions. This includes the requirement that all entries be made in a clear, legible, and consistent manner, and that all supporting documentation be properly filed and retained for a minimum of five years.

3. The third part of the document addresses the issue of audits and the role of external auditors. It states that all entities subject to the provisions of this document must undergo a regular audit by a qualified external auditor to ensure compliance with the applicable laws and regulations.

4. The fourth part of the document discusses the consequences of non-compliance with the provisions of this document. It states that any entity found to be in violation of these provisions may be subject to civil penalties, fines, and in severe cases, criminal prosecution.

5. The fifth part of the document provides a summary of the key provisions of this document and offers guidance on how to ensure compliance. It encourages all entities to take the necessary steps to ensure that they are fully compliant with the applicable laws and regulations.

- немедленно сообщить преподавателю при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;
- не должны отправлять или отвечать на сообщения, оскорбительные, угрожающие или непристойные;
- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети колледжа или атаки на другие системы;
- запрещается использование чужих имен пользователя, пароля и электронной почты;
- запрещено использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка колледжа.

Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ.

ПРАВИЛА

работы с ресурсами сети Интернет

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Сотрудники отдела информационно-программного обеспечения имеют право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых 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.

При работе с ресурсами сети Интернет недопустимо:

- разглашение коммерческой и служебной информации колледжа, ставшей известной сотруднику колледжа по служебной необходимости либо иным путем;
- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для

получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

При работе с ресурсами Интернет запрещается:

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