

Утверждаю
Директор колледжа транспорта
Нугымаров А.С.
« 2025 г.



ПОЛОЖЕНИЕ **об информационной безопасности** **КГКП «Колледж транспорта» управления образования области Абай.**

Термины и определения

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы колледжа.

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

Специалист по программному обеспечению - должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса колледжа, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление

Пользователь - сотрудник колледжа, использующий ресурсы информационной системы колледжа для выполнения должностных обязанностей.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.)

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

Изменение полномочий - процесс создания, удаления, внесения изменений в учетные записи пользователей АС, создание, удаление, изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление, изменение групп безопасности и групп почтовой рассылки,

а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю АС.

1. Назначение и область применения

1.1. Положение об информационной безопасности КГКП «Колледж транспорта» управления образования ВКО акимата (далее - Положение, колледж)

регламентирует порядок организации и правила обеспечения информационной безопасности в колледже, распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и 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.

Положение утверждается приказом директора колледжа в установленном порядке.

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, противодействия техническим разведкам, включающая комплексные, криптографические, компьютерные, организационные, технические средства защиты.

2.3. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2.4. Информационная безопасность включает:

- защиту интеллектуальной собственности 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.

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, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РК, 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:

1. Конституция Республики Казахстан; (с изменениями и дополнениями по состоянию на 10.03.2017 г.)
2. Закон «О национальной безопасности Республики Казахстан»; (с изменениями и дополнениями по состоянию на 11.07.2017г.)
3. Закон Республики Казахстан «О связи» от 5 июля 2004 года № 567-П; (с изменениями и дополнениями по состоянию на 09.01.2018г.)
4. Закон Республики Казахстан «О доступе к информации»; (с изменениями и дополнениям и по состоянию на 28.12.2016г.)
5. Закон Республики Казахстан «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017г.)
6. Другие законодательные акты, руководящие и нормативно-методические документы Республики Казахстан 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 Республики Казахстан 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;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- координация деятельности структурных подразделений колледжа по обеспечению защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- развитие и совершенствование защищенного юридически значимого электронного документооборота.
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности
- создание механизмов управления системой информационной безопасности (СИБ).

4. Организация системы обеспечения-информационной безопасности

4.1 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;
- внутрисетевой контроль за перемещением информации;
- принятие мер к воспрепятствованию доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- проверка целесообразности использования персоналом и обучающимися колледжа интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;
- защита персональных данных персонала и обучающихся - мероприятия по недопущению несанкционированного доступа к персональным данным персонала и обучающихся колледжа при их обработке с использованием средств автоматизации или без использования таких средств;

- контроль за использованием электронных средств информационного обеспечения деятельности колледжа по прямому назначению - плановые и внеплановые проверки в структурных подразделениях колледжа.
- принятие мер к воспреещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими, доведение этих сведений до администрации и персонала колледжа и принятие мер к воспреещению доступа к этим материалам (мерами технического противодействия - в отношении материалов, находящихся в сети Интернет;
- проверка целесообразности использования персоналом и обучающимися колледжа интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;
- установление и доведение в форме инструкций до персонала и обучающихся колледжа общедоступных требований об ограничениях при использовании- ресурса, предоставляемого им администрацией колледжа, постоянный контроль за выполнением указанных ограничений, разработка, внедрение, и применение технических (программных) средств противодействия возникающим нарушениям, либо злоупотреблениям;
- обучение персонала колледжа по вопросам обеспечения информационной безопасности - проведение занятий с персоналом в целях формирования у них соответствующих знаний, умений и навыков, позволяющих соблюдать требования по обеспечению информационной безопасности колледжа.

4.2 Общее руководство системой информационной безопасности колледжа осуществляет заместитель директора по учебной работе. Руководители структурных подразделений колледжа обязаны участвовать в ее поддержании в надлежащем состоянии, дальнейшем развитии и совершенствовании по своим направлениям деятельности.

5 Требования к паролям

5.1 При выборе пароля необходимо руководствоваться следующими правилами:

- длина пароля должна составлять не менее 8 символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр;
- запрещается использовать в качестве пароля название учетной записи или имя пользователя, а также легко угадываемые сочетания символов.

5.2 Пользователь несет персональную ответственность за сохранение в тайне пароля. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.3 Пользователь обязан не реже одного раза в три месяца производить смену пароля, соблюдая требования настоящего Положения.

5.4 В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом специалисту по ПО и изменить пароль.

5.5 Восстановление забытого пароля пользователя осуществляется специалистом по ПО путем изменения (сброса) пароля пользователя на основании письменной заявки пользователя.

5.6 Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

5.7 Для предотвращения угадывания паролей специалист по ПО обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

6. Доступ к ресурсам Интернет

6.1 Для исполнения задач, связанных с производственной деятельностью сотрудникам колледжа, предоставляется доступ к ресурсам Интернет. Доступ к ресурсам Интернет в других целях запрещен.

6.2 Требуемый уровень доступа предоставляется сотруднику колледжа на основании заявки «на изменение списков доступа» зам. директора по УР.

6.3 Специалист по ПО обязан предоставлять руководителю колледжа лимит использования Интернет на предстоящий месяц.

6.4 Специалист по ПО обязан не реже одного раза в месяц представлять отчет об использовании Интернет ресурсов сотрудниками колледжа зам. директору по УР.

6.5 Доступ к ресурсам Интернет может быть заблокирован специалистом по ПО без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

6.6 Сотрудникам колледжа может быть предоставлен дополнительный объем трафика Интернет согласно заявлению, на имя руководителя колледжа.

Правила работы с ресурсами Интернет приведены в приложении 1.

7. Электронная почта

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

7.2 Доступ к электронной почте предоставляется сотруднику колледжа на основании заявки «на изменение списков доступа» зам. директора по УР.

7.3 Электронная почта является собственностью колледжа и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

7.4 Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию руководства.

7.5 В случае обнаружения значительных отклонений в параметрах работы средств обеспечения работы электронной почты, специалист по ПО обязан немедленно сообщить об этом зам. директора по УР для принятия решений.

7.6 Доступ к электронной почте может быть заблокирован специалистом по ПО без предварительного уведомления при возникновении нештатных ситуаций, либо в иных случаях, предусмотренных организационными документами.

Правила работы с электронной почтой приведены в приложении 3.

8. Антивирусная защита

8.1 К использованию в колледже допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

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

8.3 Настройка параметров средств антивирусного контроля осуществляется специалистом по ПО в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками запрещено.

8.4 Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов РС.

8.5 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 (магнитных дисках, CD-ROM и т.п.).

8.6 Антивирусная проверка должна проводиться:

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

8.7 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 подразделения совместно со специалистом по ПО должен провести внеочередной антивирусный контроль своего ПК.

9. Хранение данных

9.1 Служебная информация сотрудников колледжа должна храниться в специально отведенных папках на серверах ЛВС колледжа. Хранение служебной информации на компьютерах сотрудников запрещено.

9.2 Ответственность:

9.2.1 Ответственность за обеспечение целостности данных, хранимых на серверах колледжа в соответствии с требованиями настоящего положения возлагается на специалиста по ПО.

9.2.2 Ответственность за обеспечение целостности данных, хранимых на локальных компьютерах сотрудников колледжа в соответствии с требованиями настоящего Положения возлагается на самих сотрудников.

10. Установка и обслуживание оборудования

10.1 Установка и обслуживание оборудования возможна только специалистом по ПО. Установка и обслуживание оборудования другими сотрудниками запрещена.

10.2 Для определения несанкционированной замены оборудования вся техника колледжа должна быть опечатана в местах возможного вскрытия.

10.3 Ответственность за сбои в работе оборудования лежит на специалисте по ПО.

11. Установка и обслуживание программ

11.1 Установка программ возможна только специалистом по ПО. Установка программ другими сотрудниками запрещена.

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: 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.

Полномочия преподавателей и сотрудников.

Специалист по ПО:

- организует и руководит всей деятельностью по реализации настоящих Правил;
- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями колледжа;
- организует и руководит всей деятельностью по реализации настоящих Правил;
- создает возможности для обогащения и расширения образовательного процесса через Сети;
- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;
- проверяет в учебной части соответствие календарно-тематическому плану заявки преподавателей на открытие доступа в сеть Интернет для групп обучающихся. Открывает доступ для данной группы на время проведения занятия, по списку необходимых для занятия сайтов;
- обеспечивает контроль за соблюдением правил работы, обучающихся в сетях;
- предоставляет технические возможности в области мониторинга трафика, передаваемого через Сеть колледжа;
- организует в начале каждого учебного года ознакомление обучающихся с правилами безопасной работы в Сети. Информирует обучающихся, что трафик контролируется;
- организует поддержку и обновление сайта. Размещает на сайте только материалы, утвержденные директором;

- незамедлительно сообщает директору о выявлении нарушений и принимает меры по устранению нарушений;

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;
- своевременно подавать заявки на предоставление доступа для группы обучающихся в пределах учебных занятий, предусмотренных календарно-тематическими планами, а также для открытия доступа вне учебных планов с указанием перечня необходимых ресурсов с обоснованием;
- 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 специалисту по ПО 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.

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);
- 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;
- немедленно сообщить преподавателю при обнаружении материалов, 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.

Ответственность

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 РК.

ПРАВИЛА работы с ресурсами сети Интернет

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Специалист по ПО колледжа имеет 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 Казахстанским 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 политикой колледжа.
- Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой колледжа.
- Вся информация о ресурсах, посещаемых сотрудниками колледжа, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также администрации колледжа для детального изучения.

ПРАВИЛА работы с электронной почтой

Электронная почта является собственностью колледжа и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с электронной почтой сотрудникам колледжа запрещается:

- использовать адрес почты для оформления подписок и массовых рассылок;
- публиковать свой адрес, либо адреса других сотрудников колледжа на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
- осуществлять массовую рассылку почтовых сообщений рекламного характера;
- рассылка через электронную почту материалов, содержащие 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 ссылки на вышеуказанную информацию;
- 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 сторон;
- распространять информацию содержание и направленность которой запрещены международным и Казахстанским 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 своему почтовому адресу.