государственное бюджетное
профессиональное образовательное учреждение
«Кунгурский колледж агротехнологий и управления»

СОГЛАСОВАНО:	УТВЕРЖДЕНО:
Протокол педагогического совета	Приказ директора ГБПОУ «ККАТУ»
№ 1 от 28 августа 2023 г.	№ 100-о от 27 сентября 2023 г.

ПОЛОЖЕНИЕ
об информационной безопасности в ГБПОУ «Кунгурский колледж агротехнологий и управления»

Кунгур, 2023

Термины и определения

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей в виду высоких требований по обеспечению надёжности, степени готовности и мер безопасности информационной системы колледжа.

Рабочая станция - персональный компьютер, предназначенный для доступа пользователей к ресурсам автоматизированной системы колледжа, приёма передачи и обработки информации.

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

Учётная запись- информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учётная запись может содержать дополнительную информацию. 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 ГБПОУ «Кунгурский колледж агротехнологий и управления» (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.

1.3. 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.

Информационная безопасность включает:

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

2.4. 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, в соответствии с перечнем сведений конфиденциального характера;
- 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 ;

- ГОСТ Р ИСО/МЭК 27001—2021 (ISO/IEC 27001-1:2013) «Информационная технология. Методы и средства обеспечения безопасности»
- 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;
- 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. 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 нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;
- внутрисетевой контроль за перемещением информации;
- принятие мер к воспрещению 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;
- обучение персонала колледжа по вопросам обеспечения информационной безопасности;
- контроль за правильностью использования имеющихся в колледже средств телефонной связи;
- 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.
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности колледжа нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами - контроль за используемым программным обеспечением и проверка его подлинности.
- 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.
- контроль за правильностью использования имеющихся в колледже средств телефонной связи - выявление фактов нецелевого использования средств телефонной связи и принятие мер технического и организационного характера по их недопущению.

4.3. Общее руководство системой информационной безопасности колледжа осуществляет заместитель директора.

5. Порядок обеспечения информационной безопасности

5.1. Организационное и техническое обеспечение рабочего процесса сотрудников возлагается на сотрудников отдела по безопасности.

5.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику учреждения, допущенному к работе с конкретной подсистемой АС, должно быть сопоставлено персональное уникальное имя - учетная запись пользователя и пароль, под которым он будет регистрироваться, и работать в системе. Использование несколькими сотрудниками при работе в АС одного и того же имени пользователя запрещено.

5.3. Проведение операций, указанных п. 4.2. сотрудниками, не уполномоченными на проведение подобных действий, запрещено и идентифицируется как факт несанкционированного доступа.

5.4. Правила работы сотрудников колледжа и обучающихся в компьютерных сетях приведены в Приложении 1.

6. Учетные записи

6.1. Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования сотрудниками отдела по безопасности при настройке системы и не предназначены для повседневной работы.

6.2. Создание и использование локальных учетных записей на рабочих станциях, подключенных к ВС колледжа запрещено.

6.3. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях в составе ВС колледжа при первоначальном конфигурировании операционной системы.

7. Требования к паролям

7.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

7.2. Установку первичного пароля производит системный администратор при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

7.3. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

7.4. При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

7.5. Первичный пароль также используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

7.6. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику колледжа, используемая для подтверждения подлинности владельца учетной записи.

7.7. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

7.8. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам отдела по безопасности, записывать его, а также пересылать открытым текстом в электронных сообщениях.

7.9. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в отдел по безопасности и изменить основной пароль.

7.10. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль.

11. Доступ к ресурсам Интернет

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

11.2. Доступ к ресурсам Интернет может быть блокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

11.3. Правила работы с ресурсами Интернет приведены в приложении2.

12. Антивирусная защита

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

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

12.3. Настройка параметров средств антивирусного контроля осуществляется сотрудниками отдела по безопасности в соответствии с руководствами по применению конкретных антивирусных средств. Изменение
настроек другими сотрудниками запрещено.

12.4. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по телекоммуникационным каналам.

12.5 Антивирусная проверка должна проводиться :
- на компьютерах сотрудников – не реже одного раза в неделю;
-на серверах - не реже двух раз в неделю.

13. Установка и обслуживание оборудования, программ

13.1. Установка и обслуживание программ возможна только инженером программистом.

13.2. Установка программ студентами и сотрудниками запрещена.