ГБПОУ РМ «Ковылкинский аграрно-строительный колледж»

УТВЕРЖДАЮ
Директор ГБПОУ РМ «Ковылкинский аграрно-строительный колледж»
_____ Г.Н. Киржаева
«26» марта 20 18 г.

ЛОКАЛЬНЫЙ НОРМАТИВНЫЙ АКТ

Правила информационной безопасности

Рассмотрено
на заседании педагогического совета
Протокол №6 от 22.03.18

Ковылкино, 2018

Содержание документа

Перечень сокращений и обозначений

ИБ - информационная безопасность

ГБПОУ РМ КАСК - Государственное бюджетное профессиональное образовательное учреждение Республики Мордовия «Ковылкинский аграрно-строительный колледж»

НСД - несанкционированный доступ ЛВС - локальная вычислительная сеть

1. Назначение и область применения

1.1. Настоящие Правила являются локальным нормативным актом и определяют политику ГБПОУ РМ КАСК (далее - колледж) в сфере информационной безопасности (далее - ИБ). Устанавливают совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются сотрудники и обучающиеся колледжа при осуществлении своей деятельности.

1.2. Целью настоящих правил является защита информации колледжа при осуществлении уставной деятельности от случайного или преднамеренного изменения, раскрытия или уничтожения информации; соблюдение конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.

1.3. Выполнение требований настоящих правил является обязательным для всех руководителей структурных подразделений колледжа.

1.4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник колледжа. На лиц, работающих по договорам гражданско-правового характера, условия настоящего положения распространяются в случае, если это обусловлено в таком договоре.

2. Термины и определения

2.1. Информационная безопасность - состояние сохранности информационных ресурсов колледжа и защищённости в информационной сфере.

2.2. Компьютерное оборудование - (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (факс-модемы, сетевые адаптеры и концентраторы)

2.3. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации

физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы; другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

2.4. Внешних носителей информации - диски, дискеты, флэш-карты и т.п.

3. Требования

3.1. Общие положения

3.1.1. Политика ИБ колледжа направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников; уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников колледжа, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации; защиту несовершеннолетних обучающихся от информации, причиняющей вред их здоровью и развитию и обеспечение эффективного и бесперебойного процесса деятельности.

3.1.2. Объектами защиты с точки зрения ИБ являются информационный процесс профессиональной деятельности и информационные активы колледжа.

3.1.3. К защищаемой информации относится информация по финансово-экономической деятельности колледжа, персональные данные.

3.1.4. Основными мерами обеспечения ИБ являются:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов колледжа;

- своевременное обнаружение проблем, потенциально способных

повлиять на ИБ колледжа, корректировка моделей угроз и нарушителя;

- разработка и внедрение защитных мер;
- блокирование недопустимого контента интернет-траффика;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками колледжа за обеспечение ИБ колледжа исходит из принципа персональной и единоличной ответственности за совершаемые операции.

3.1.5 Управление ИБ колледжа включает в себя:

-разработку и поддержание в актуальном состоянии Политики информационной безопасности;

-разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;

-обеспечение бесперебойного функционирования комплекса средств ИБ;

осуществление контроля (мониторинга) функционирования системы ИБ;

-оценку рисков, связанных с нарушениями ИБ.

3.1.6. В отношении всех собственных информационных активов колледжа, активов, находящихся под контролем колледжа, а также активов, используемых для получения доступа к инфраструктуре колледжа, устанавливается ответственность соответствующего сотрудника колледжа.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами колледжа должна доводиться до сведения директора колледжа.

3.1.7. Все сотрудники и обучающиеся колледжа при работе в сети интернет должны руководствоваться локально-нормативным актом.[1]

3.1.8. Все работы в пределах колледжа должны выполняться в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в колледже.

3.1.9. Внос в здание и помещения колледжа личных портативных компьютеров и внешних носителей информации, а также вынос их за

[1] ЛНА Правила информационной безопасности

пределы колледжа производится только при согласовании с заведующим сектором по информационно-техническому обеспечению.

3.1.10. Все данные, составляющие тайну колледжа и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

3.1.11. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

3.1.12. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети колледжа, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

3.1.13. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

3.1.14. Компьютерное оборудование, предоставленное колледжем, предназначено для использования исключительно в производственных целях.

3.1.15. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования.

3.1.16. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

3.1.17. Все программное обеспечение, установленное на предоставленном управлением компьютерном оборудовании, является собственностью колледжа и должно использоваться исключительно в производственных целях.

3.1.18. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию колледжа по электронной почте без

использования систем шифрования. Конфиденциальная информация колледжа, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

3.1.19. Использование сотрудниками колледжа публичных почтовых ящиков электронной почты осуществляется только при согласовании с заведующим сектором по информационнотехническому обеспечению.

3.1.20. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

3.1.21. Перед отправкой сообщений пользователи должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать заведующего сектором по информационно-техническому обеспечению.

3.1.22. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

3.1.23. Не допускается при использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

- рассылка рекламных материалов не связанных с производственной деятельностью;

- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

- поиск и чтение сообщений, направленных другим лицам (независимо

от способа их хранения);

- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

3.1.24. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с заведующим сектором по информационно-техническому обеспечению.

3.2. **Права, обязанности и ответственность**

3.2.1. Руководители структурных подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

3.2.2. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

3.2.3. В процессе своей работы сотрудники обязаны контролировать и предотвращать вероятную возможность утечки данных.

3.2.4. Каждый сотрудник обязан немедленно уведомить заведующего сектором по информационно-техническому обеспечению обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

3.2.5. Сотрудникам, использующим в работе портативные компьютеры колледжа, может быть предоставлен удаленный доступ к сетевым ресурсам колледжа в соответствии с правами в корпоративной информационной системе.

3.2.6. Сотрудникам, работающим за пределами колледжа с использованием компьютера, не принадлежащего колледжу, запрещено

копирование данных на компьютер, с которого осуществляется удаленный доступ.

3.2.7. Сотрудники, имеющие право удаленного доступа к информационным ресурсам колледжа, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети колледжа и к каким-либо другим сетям, не принадлежащим колледжу.

3.2.8. Заведующий сектором по информационно-техническому обеспечению имеет право:

- контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях;

- на создание и удаление совместно используемых сетевых ресурсы и папок общего пользования, а также управление полномочиями доступа к ним;

3.2.9. Сотрудники должны обеспечивать физическую безопасность оборудования, на котором хранится информация колледжа.

3.2.10. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит заведующий сектором по информационно-техническому обеспечению.

3.2.11. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

3.2.12. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности.

3.2.13. При выявлении вирусов или иных разрушительных компьютерных кодов, сотрудник обязан незамедлительно:

- проинформировать сектор информационно-технического обеспечения колледжа в установленном порядке;

- не пользоваться и не выключать зараженный компьютер;

- не подсоединять этот компьютер к компьютерной сети колледжа до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование сектором информационно-технического обеспечения.

3.2.14. Сотрудникам колледжа запрещается:

- нарушать информационную безопасность и работу сети колледжа;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников колледжа посторонним лицам;

создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

3.2.16. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

3.2.17. Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

4. Ответственность и полномочия

4.1. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

4.2. Ответственность за управлением информационной безопасностью лежит на заведующем секторе по информационно-техническому обеспечению.

4.3. Текущий контроль за соблюдением выполнения требований настоящего локальнонормативного акта возлагается на заведующего сектором по информационно-техническому обеспечению.

5. Нормативные документы

5.1 Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».

5.2 Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных».

5.3 Федеральный закон от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи».

5.4 Указ Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

5.5 Постановление Правительства РФ №781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»,

5.6 Постановление Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

5.7 Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

5.8 Иные нормативные правовые акты в сфере защиты информации.

6. Лист регистрации изменений

Номер изменения	Номера листов			Основание для внесения изменений	Подпись	Расшифровка подписи	Дата	Дата введения изменения
	замененных	новых	аннулированных					