УТВЕРЖДАЮ
Директор
_____ А.А.Ишмухамбетов
«___» _____ 2021 г.

Политика информационной безопасности

КГКП «Рудненского политехнического колледжа» Управления образования акимата Костанайской области

1. Общие положения

1.1. Политика информационной безопасности КГКП «Рудненского политехнического колледжа» Управления образования акимата Костанайской области (далее – колледж), определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее – ИБ), которыми руководствуются работники колледжа при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности колледжа является защита информации колледжа при осуществлении образовательной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.

1.3. Политика информационной безопасности разработана в соответствии с Законом Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности», Законом Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации», Законом Республики Казахстан от 15 марта 1999 года № 349-I «О государственных секретах», Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите», Законом Республики Казахстан от 7 января 2003 года № 370 «Об электронном документе и электронной цифровой подписи», Законом Республики Казахстан от 5 июля 2004 года № 567-II «О связи», Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник колледжа.

2. Цель и задачи политики информационной безопасности

2.1. Основными целями политики ИБ являются:

-сохранение конфиденциальности критичных информационных ресурсов;

-обеспечение непрерывности доступа к информационным ресурсам колледжа;

-защита целостности информации с целью поддержания возможности колледжа по оказанию услуг высокого качества и принятию эффективных управленческих решений;

-повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами колледжа;

-определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности.
-повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
-предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2. Основными задачами политики ИБ являются:
-разработка требований по обеспечению ИБ;
-контроль выполнения установленных требований по обеспечению ИБ;
-повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
-разработка нормативных документов для обеспечения ИБ колледжа;
-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ колледжа;
-организация антивирусной защиты информационных ресурсов колледжа;
-защита информации колледжа от несанкционированного доступа (далее – НСД) и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору колледжа.

3. Концептуальная схема обеспечения информационной безопасности

3.1. 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 и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал колледжа. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Стратегия обеспечения ИБ колледжа заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников колледжа.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения ИБ:
-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;
-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.

5.Объекты защиты

5.1. Объектами защиты с точки зрения ИБ в управлении являются:

-информационный процесс профессиональной деятельности;

-информационные активы колледжа.

5.2. Защищаемая информация делится на следующие виды:

- 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;

- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

6.1. В отношении всех собственных информационных активов колледжа, активов, находящихся под контролем колледжа, а также активов, используемых для получения доступа к инфраструктуре колледжа, должна быть определена 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.

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

6.3. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну колледжа и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

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

6.5. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

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

6.7. Рекомендованные правила:

- сотрудникам колледжа разрешается использовать сеть Интернет только в служебных целях;

- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

- работа сотрудников колледжа с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации колледжа в сеть Интернет;

- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем колледжа;
- сотрудники колледжа перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещено использование сторонних почтовых служб (зарубежных служб @mail.ru, @gmail.com и т.д.) в служебной деятельности. В работе разрешается использовать почтовые службы такие как mail.kz, post.kz, nur.kz;
- запрещена передача служебной информации без пометки, с пометкой ДСП, с грифом «секретно» по средствам мессенджеров WhatsApp, Telegram, Viber, Vk.com, Facebook и другие;
- запрещена фото и видеосъемка проектов документов, а также самих документов (без пометки, с пометкой ДСП, с грифом);
- запрещено подключение смартфонов к рабочим компьютерам для зарядки, передачи файлов, фото и другое;
- запрещено использование программ удалённого доспупа (TeamViewer, Radmin, AnyDesk, Supremo и т.д.;
- запрещен доступ в Интернет через сеть колледжа для всех лиц, не являющихся сотрудникамиколледжа, включая членов семьи сотрудников.

6.8. Администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.9. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация колледжа.

6.10. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит инженер по ПО или лицо его заменяющее.

6.11. Все 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 (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное колледжем, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

6.13. Все компьютеры могут быть защищены паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. 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.

6.14. При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

6.15. Порты передачи данных, в том числе CD дисководы в стационарных компьютерах

сотрудников колледжа блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

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

6.17. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственно директору колледжа.

6.18. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;

6.19. Сотрудники колледжа не должны:

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

6.20. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Конфиденциальная информация колледжа, ни при каких обстоятельствах, не подлежит пересылке третьим лицампо электронной почте.

6.21. Использование сотрудниками колледжа публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации.

6.22. Сотрудники колледжа для обмена документами должны использовать только свой официальный адрес электронной почты.

6.23. 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.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой 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.

6.24. Не допускается при использования электронной почты:

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

6.25. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.26. В случае кражи переносного компьютера следует незамедлительно сообщить администратору и/или директору колледжа.

6.27. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
-проинформировать инженера по ПО или лицо его заменяющее;
- не использовать и не включать 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 инженером по ПО или лицом его заменяющим.

6.28. 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;
- передавать информацию о сотрудниках или списки сотрудников колледжа посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

6.31. Все заявки на проведение технического обслуживания компьютеров должны направляться инженеру по ПО или лицу его заменяющему.

7.Управление информационной безопасностью

7.1. 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.

8. Реализация политики информационной безопасности

8.1. Реализация Политики ИБ колледжа осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

9.Порядок внесения изменений и дополнений в политику информационной безопасности

9.1. Внесение изменений и дополнений в Политику информационной безопасности

производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10.Контроль за соблюдением политики информационной безопасности

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности колледжа возлагается на заместителя директора по информационным технологиям.

10.2. Директор колледжа на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.