

Политика в отношении обработки
персональных данных
в учреждении образования
«Пинский государственный
автомеханического колледжа»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика конфиденциальности (далее – Политика) разработана в соответствии с требованиями законодательства Республики Беларусь в области информационной безопасности и письмом Главного управления по образованию.

1.2. Целью настоящей Политики является обеспечение защиты конфиденциальной информации колледжа, предотвращение несанкционированного доступа к информационным системам и данным.

1.3. Положения настоящей Политики обязательны для исполнения всеми работниками, обучающимися, а также иными лицами, имеющими доступ к информационным ресурсам колледжа.

2. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Приказом директора колледжа назначаются ответственные лица за организацию мероприятий по информационной безопасности.

2.2. Ответственные лица обязаны пройти обучение по вопросам информационной безопасности в Национальном центре защиты информации Республики Беларусь и (или) РУП «Национальный центр обмена трафиком».

2.3. Руководитель колледжа несет персональную ответственность за организацию работы по обеспечению информационной безопасности в колледже.

3. ТРЕБОВАНИЯ К ПАРОЛЯМ (обязательный раздел)

3.1. Периодичность изменения паролей:

Пароли от компьютеров, корпоративных учетных записей, сайтов колледжа и других внутренних информационных систем подлежат обязательному изменению ежемесячно.

Изменение паролей осуществляется в первые 5 рабочих дней каждого месяца.

3.2. Уникальность паролей:

Для каждой информационной системы (операционная система компьютера, почтовый ящик, сайт колледжа, база данных, внутренние информационные системы) должен использоваться уникальный пароль.

Запрещается использование одинаковых паролей для разных систем.

3.3. Требования к сложности паролей:

Минимальная длина пароля – не менее 12 символов.

Пароль должен содержать:

буквы верхнего регистра (A-Z)

буквы нижнего регистра (a-z)

цифры (0-9)

специальные символы (!, @, #, \$, % и др.)

Запрещается использование:

простых слов из словарей

последовательных символов (123456, qwerty, abcdef)

личной информации (ФИО, дата рождения, номер телефона)

названий организаций и учреждений

повторяющихся символов

3.4. Хранение паролей:

Запрещается записывать пароли на бумажных носителях и оставлять их на рабочих местах.

Запрещается передавать пароли третьим лицам.

Рекомендуется использование корпоративных менеджеров паролей для безопасного хранения.

4. ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

4.1. Все компьютеры и серверы колледжа должны быть защищены антивирусным программным обеспечением с регулярным обновлением баз.

4.2. Доступ к информационным системам колледжа осуществляется только посредством аутентификации с использованием логина и пароля.

4.3. Регулярно выполняется резервное копирование критически важных данных с проверкой целостности резервных копий.

5. ОБУЧЕНИЕ И ИНФОРМИРОВАНИЕ ПЕРСОНАЛА

5.1. Все работники колледжа обязаны проходить инструктаж по вопросам информационной безопасности при приеме на работу и ежегодно в течение трудовой деятельности.

5.2. Все работники колледжа обязаны ознакомиться с настоящей Политикой конфиденциальности под роспись в специальном журнале.

5.3. Ответственные за информационную безопасность проводят регулярные консультации и разъяснительную работу по вопросам защиты информации.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ

6.1. Нарушение требований настоящей Политики влечет дисциплинарную ответственность в соответствии с Трудовым кодексом Республики Беларусь.

6.2. За преступления против информационной безопасности, совершенные в отношении информационных ресурсов колледжа, предусмотрена уголовная ответственность в соответствии с законодательством Республики Беларусь.

6.3. Лица, виновные в нарушении требований информационной безопасности, несут материальную ответственность за причиненный ущерб в установленном законодательством порядке.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящая Политика вступает в силу с момента ее утверждения директором колледжа.

7.2. Контроль за исполнением настоящей Политики осуществляет назначенный приказом ответственный за информационную безопасность.

7.3. Настоящая Политика подлежит пересмотру не реже одного раза в год или при изменении законодательства в области информационной безопасности.

8. ТРЕБОВАНИЯ К БЕСПРОВОДНЫМ СЕТЯМ (WI-FI) И ТОЧКАМ ДОСТУПА

8.1. Развертывание и авторизация оборудования

8.1.1. Развертывание точек беспроводного доступа (Wi-Fi) в сети колледжа осуществляется только уполномоченными сотрудниками.

8.1.2. Запрещается самостоятельная установка обучающимися, работниками или иными лицами персональных точек доступа, Wi-Fi роутеров и устройств, создающих беспроводные сети, без согласования с ответственным за информационную безопасность.

8.1.3. Все точки доступа должны быть внесены в реестр сетевого оборудования колледжа.

8.2. Настройки безопасности и шифрование

8.2.1. Все беспроводные сети колледжа должны использовать современные протоколы шифрования (не ниже WPA2-AES, рекомендуется WPA3).

8.2.2. Запрещается использование устаревших и небезопасных протоколов шифрования (WEP, WPA-TKIP).

8.2.3. Идентификаторы сетей (SSID) не должны содержать информации, раскрывающей внутреннюю структуру сети, версии оборудования или конфиденциальные данные колледжа.

8.3. Сегментация сети

8.3.1. Доступ к внутренней информационной сети колледжа через Wi-Fi предоставляется только сотрудникам через защищенный сегмент сети с обязательной аутентификацией.

8.3.2. Для обучающихся и гостей должен быть организован изолированный гостевой сегмент сети (Guest Network), не имеющий доступа к внутренним ресурсам колледжа (серверам, базам данных, локальным принтерам).

8.3.3. Трафик в гостевой сети должен подвергаться фильтрации и мониторингу.

8.4. Аутентификация в беспроводной сети

8.4.1. Доступ к корпоративному сегменту Wi-Fi осуществляется с использованием индивидуальных учетных данных (логин/пароль), соответствующих требованиям раздела 3 настоящей Политики.

8.4.2. Запрещается использование единых общих паролей для доступа к защищенному сегменту Wi-Fi для сотрудников.

8.5. Физическая защита точек доступа

8.5.1. Точки доступа должны размещаться в местах, исключающих возможность их физического повреждения, несанкционированного отключения или сброса настроек посторонними лицами.

8.5.2. Доступ к коммутационным шкафам и оборудованию,

обеспечивающему работу Wi-Fi, должен быть ограничен для неуполномоченных лиц.

8.6. Мониторинг и реагирование

8.6.1. Ответственные лица обязаны регулярно проводить мониторинг эфира на предмет наличия несанкционированных точек доступа.

8.6.2. При обнаружении несанкционированной точки доступа должны быть приняты меры по ее локализации и блокировке доступа к сети колледжа.

9. ТРЕБОВАНИЯ К АДМИНИСТРИРОВАНИЮ ОФИЦИАЛЬНОГО САЙТА И НАПОЛНЕНИЮ ИНФОРМАЦИЕЙ

9.1. Доступ к системе управления сайтом (CMS)

9.1.1. Доступ к панели администрирования официального сайта колледжа предоставляется только уполномоченным сотрудникам, назначенным приказом директора.

9.1.2. Учетные записи администраторов сайта должны защищаться паролями, соответствующими требованиям раздела 3 настоящей Политики.

9.1.3. Запрещается передача учетных данных для доступа к CMS третьим лицам, включая обучающихся и посторонних сотрудников.

9.1.4. При увольнении сотрудника, имевшего доступ к сайту, его учетная запись должна быть заблокирована или удалена в тот же день.

9.2. Публикация информации и новостей

9.2.1. Вся информация, размещаемая на сайте, должна быть актуальной, достоверной и соответствовать законодательству Республики Беларусь.

9.2.2. Запрещается публикация сведений, составляющих государственную тайну, коммерческую тайну или иную конфиденциальную информацию колледжа.

9.2.3. Новости и объявления должны проходить предварительную модерацию ответственным лицом перед публикацией.

9.2.4. Не допускается размещение информации, порочащей деловую репутацию колледжа, содержащей призывы к противоправным действиям или экстремизму.

9.3. Защита персональных данных на сайте

9.3.1. Запрещается публикация персональных данных обучающихся и работников (ФИО, фото, контакты, оценки) без их письменного согласия, за исключением случаев, предусмотренных законодательством.

9.3.2. При публикации списков, протоколов или фотографий мероприятий необходимо обезличивание данных и наличие согласий на обработку персональных данных.

9.3.3. Формы обратной связи на сайте должны содержать уведомление о политике обработки персональных данных и ссылку на соответствующий документ.

9.4. Техническая поддержка и резервное копирование

9.4.1. Ответственные лица обязаны регулярно обновлять программное обеспечение сайта (CMS, плагины, темы) для устранения уязвимостей безопасности.

9.4.2. Перед внесением масштабных изменений в структуру или контент сайта должно выполняться резервное копирование данных.

9.4.3. Резервные копии сайта должны храниться на отдельном носителе, не связанном напрямую с веб-сервером.

9.5. Мониторинг и реагирование на инциденты

9.5.1. Ответственный за сайт обязан регулярно проверять работоспособность ресурса и отсутствие несанкционированных изменений (дефейс).

9.5.2. При обнаружении взлома сайта или утечки информации через веб-ресурс необходимо немедленно сообщить ответственному за информационную безопасность и принять меры по восстановлению из резервной копии.

9.5.3. Доступ к сайту должен быть защищен протоколом HTTPS с использованием действительного SSL-сертификата.

10. ТРЕБОВАНИЯ К ВЕДЕНИЮ ОФИЦИАЛЬНЫХ СТРАНИЦ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

10.1. Общие положения

10.1.1. Официальными каналами коммуникации колледжа в сети Интернет являются: официальный сайт, страницы в социальных сетях «ВКонтакте», «Instagram», канал в «Telegram», а также группы в мессенджере «Viber».

10.1.2. Создание, ведение и закрытие официальных страниц в социальных сетях и мессенджерах осуществляется на основании приказа директора колледжа.

10.1.3. За каждым официальным ресурсом закрепляется ответственный сотрудник (контент-менеджер, модератор), назначенный приказом.

10.2. Доступ к учетным записям и защита аккаунтов

10.2.1. Доступ к управлению официальными страницами предоставляется только уполномоченным сотрудникам под индивидуальные учетные записи.

10.2.2. Запрещается использование личных аккаунтов сотрудников для публикации официальной информации от имени колледжа.

10.2.3. Все учетные записи, привязанные к официальным страницам (почта, телефон), должны быть защищены сложными паролями в соответствии с разделом 3 настоящей Политики.

10.2.4. На всех платформах, поддерживающих данную функцию, должна быть включена двухфакторная аутентификация (2FA).

10.2.5. При увольнении сотрудника, имевшего доступ к социальным сетям, необходимо немедленно сменить пароли и отозвать доступы.

10.3. Публикация контента и информационная безопасность

10.3.1. Вся публикуемая информация должна быть достоверной, актуальной и соответствовать законодательству Республики Беларусь.

10.3.2. Запрещается размещение в официальных аккаунтах: сведений, составляющих государственную тайну или конфиденциальную информацию колледжа;

материалов, содержащих призывы к экстремизму, насилию, противоправным действиям;

информации, порочащей деловую репутацию колледжа, работников или

обучающихся;

нецензурной лексики и материалов, не соответствующих этическим нормам.

10.3.3. Перед публикацией новостей, фотографий с мероприятий, списков обучающихся или работников необходимо получить письменное согласие на обработку и распространение их персональных данных и изображений.

10.3.4. Не допускается публикация служебной информации: расписаний с персональными данными, внутренних приказов, протоколов с оценками, информации о системе безопасности колледжа.

10.4. Модерация и взаимодействие с пользователями

10.4.1. Ответственные лица обязаны осуществлять регулярный мониторинг комментариев и сообщений в официальных сообществах.

10.4.2. Запрещается вступать в конфликтные дискуссии от имени колледжа, использовать некорректные формулировки в ответах пользователям.

10.4.3. Сообщения, содержащие спам, оскорбления, призывы к противоправным действиям или распространение ложной информации, подлежат удалению с фиксацией факта в журнале инцидентов.

10.4.4. На обращения граждан и организаций в официальных аккаунтах должны даваться ответы в сроки, установленные законодательством об обращениях граждан.

10.5. Техническая безопасность и резервное копирование

10.5.1. Устройства, с которых осуществляется публикация материалов в официальные аккаунты, должны быть защищены антивирусным ПО и иметь актуальные обновления безопасности.

10.5.2. Не рекомендуется осуществлять вход в аккаунты колледжа с общественных компьютеров или через незащищенные сети Wi-Fi.

10.5.3. Ответственные лица обязаны регулярно создавать резервные копии опубликованного контента (тексты, медиафайлы) на внешних носителях колледжа.

10.6. Реагирование на инциденты

10.6.1. При подозрении на взлом официального аккаунта, публикацию несанкционированной информации или утечку данных ответственный сотрудник обязан немедленно:

ограничить доступ к аккаунту (сменить пароль, включить режим ограничения);

сообщить ответственному за информационную безопасность колледжа; сохранить доказательства инцидента (скриншоты, логи).

10.6.2. Восстановление доступа к аккаунтам осуществляется только через официальные процедуры поддержки платформ с участием уполномоченного сотрудника колледжа.