Автономная некоммерческая организация профессионального обучения
«Колледж предпринимательских и цифровых технологий»
(АНО ПО «Колледж предпринимательских и цифровых технологий»)

650000, г. Кемерово, ул. Н. Островского, д. 12, Тел. 89511607451
e-mail: zifra42@mail.ru; https://zifra42.ru
ОКПО 54572550; ОГРН 1204200005195; ИНН/КПП 4205388631/420501001

ПРИНЯТО
на Педагогическом совете
протокол № 9 от 28.06.2024 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 02A9735C009AB14CB14191A4FCB8807A7E
Владелец: НЕВЕДРОВА ОЛЬГА МИХАЙЛОВНА
Действителен: с 25.06.2024 до 25.09.2025

ПРИЛОЖЕНИЕ №3
К приказу директора колледжа
от 09.07.2024 № 41

УТВЕРЖДАЮ
Директор АНО ПО «Колледж предпринимательских и цифровых технологий»

_____О.М. Неведрова
09 июля 2024 года

ПОЛОЖЕНИЕ
О порядке обработки и по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации и с использованием автоматизированной информационной системы АНО ПО «Колледж предпринимательских и цифровых технологий»

Кемерово 2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке обработки и по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации и с использованием автоматизированной информационной системы АНО ПО «Колледж предпринимательских и цифровых технологий» (далее — Положение) определяет особенности и порядок обработки персональных данных при их обработке без использования средств автоматизации и с использованием автоматизированной информационной системы в АНО ПО «Колледж предпринимательских и цифровых технологий» (далее — Колледж).

1.2. Настоящее Положение также определяет требования по обеспечению безопасности автоматизированной информационной системы (далее - АИС) АНО ПО «Колледж предпринимательских и цифровых технологий» (далее – Оператор).

1.3. Положение разработано во исполнение Политики в отношении обработки персональных данных и в соответствии с Федеральным законом от 27 июля 2006 г.№ 152-ФЗ «О персональных данных», Федеральным законом от 20 февраля 1995 года № 24-ФЗ « Об информации, информатизации и защите информации», Законом Российской Федерации от 19 февраля 1993 года N 4524-1 "О федеральных органах правительственной связи и информации" и Положением о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденным Приказом ФАПСИ от 23 сентября 1999 года N 158, с целью определения порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

1.3. Все работники Колледжа, непосредственно осуществляющие обработку персональных данных без использования средств автоматизации и с использованием автоматизированной информационной системы, должны быть ознакомлены с настоящим Положением под роспись.

2. ОСОБЕННОСТИ И ПОРЯДОК ОБРАБОТКИ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Оператор обеспечивает раздельное хранение персональных данных, обрабатываемых без использования средств автоматизации с разными целями.

2.2. Для обработки каждой категории персональных данных используется отдельный материальный носитель.

2.3. При необходимости уничтожение или обезличивание части персональных данных, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на том же материальном носителе (удаление, вымарывание).

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), соблюдаются условия:

— типовая форма или связанные с ней документы содержат сведения о цели обработки персональных данных, наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

— типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, при необходимости получения такого согласия;

— типовая форма составлена таким образом, что каждый из субъектов персональных данных, содержащихся в документе, имеет возможность ознакомиться со своими персональными

данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

— типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

Перечень типовых форм, использующихся Оператором, приведён в Приложении 1.

2.5. Работники Оператора, осуществляющие обработку персональных данных без использования средств автоматизации, информируются о факте такой обработки, об особенностях и правилах.

2.6. Оператор принимает организационные и физические меры, обеспечивающие сохранность материальных носителей персональных данных и исключающие возможность несанкционированного доступа к ним.

2.7. Документы и внешние электронные носители информации, содержащие персональные данные, могут храниться в служебных помещениях Оператора в запираемых шкафах, в сейфах.

2.8. Перечень лиц, имеющих доступ к персональным данным, обрабатываемым без использования средств автоматизации, в помещения и к местам хранения носителей, ограничен работниками, работающими в указанных помещениях на постоянной основе. Исключена возможность доступа в помещения, где обрабатываются персональные данные без использования средств автоматизации, посторонних лиц без сопровождения допущенного работника.

2.9. Работа с материальными носителями, содержащими персональные данные, организовывается следующим образом. Материальные носители могут находиться на рабочем месте работника в течение времени, необходимого для обработки персональных данных, но не более одного рабочего дня. При этом должна быть исключена возможность просмотра персональных данных посторонними лицами. В конце рабочего дня все материальные носители, содержащие персональные данные, должны быть убраны в запираемые шкафы, сейфы. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются.

3. ОСОБЕННОСТИ И ПОРЯДОК ОБРАБОТКИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности Оператора.

Основными функциональными возможностями АИС Оператора являются:

- формирование, хранение и обновление сведений о структуре учебных подразделений Оператора;
- формирование, хранение и обновление сведений о преподавательском составе и сотрудниках учебных подразделений Оператора;
- формирование, хранение и обновление сведений об индивидуальных планах работы преподавательского состава;
- формирование, хранение и обновление сведений об учебном (учебно-производственном) плане Оператора;
- формирование, хранение и обновление сведений об учебной нагрузке преподавательского состава;
- формирование, хранение и обновление сведений о научной и учебно-методической продукции (методические рекомендации, учебные пособия, монографии, публикации) преподавательского состава;
- формирование, хранение и обновление сведений об обучающихся, проходящих обучение у Оператора;
- формирование, хранение и обновление сведений о результатах учебного процесса (итоги тестирования, экзаменов);
- аналитическая обработка информации о проведении учебного процесса как за отчётный период, так и о текущей деятельности учебных подразделений Оператора.

3.2. В качестве информации, подлежащей защите в АИС Оператора, рассматриваются:

– персональные данные преподавательского состава и сотрудников учебных подразделений;

– персональные данные обучающихся, проходящих и прошедших обучение;

– персональные данные административно-хозяйственных подразделений.

При обеспечении безопасности персональных данных в информационной системе Оператор руководствуется следующим: выбор средств защиты информации для системы защиты персональных данных; определение типа угроз безопасности персональных данных, актуальных для информационной системы; установление и обеспечение уровня защищённости персональных в информационной системе производится Оператором в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

– угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и обучающихся, при ее обработке и хранении;

– угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и обучающихся;

– угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и обучающихся, без разрешения на то ее владельца (субъекта персональных данных);

– угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и обучающихся, передаваемой заинтересованным лицам;

– угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и обучающихся, из каналов передачи данных с использованием специализированных программно-технических средств;

– угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и обучающихся, вследствие сбоев (отказов) программного и аппаратного обеспечения;

– угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;

– угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

3.2. Функциональные требования безопасности охватывают:

– требования к осуществлению аудита безопасности;

– требования к обеспечению подлинности субъектов обмена информацией;

– требования к криптографической поддержке;

– требования к защите информации, содержащей сведения о персональных данных работников и обучающихся;

– требования к идентификации и аутентификации пользователей АИС;

– требования к управлению безопасностью;

– требования к защите системы безопасности.

4. ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ И ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АИС, СВЯЗАННЫЕ С ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ (ЗАЩИТОЙ ИНФОРМАЦИИ)

4.1.Защита данных пользователя:

- АИС осуществляет функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом предоставляет возможность ограничивать и

контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, пытающийся получить доступ к АИС, сначала проходит процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, авторизацию, т.е. проверку разрешений Пользователя по отношению к какому-либо защищаемому активу.

В АИС доступ к информации разрешен только уполномоченным на это Пользователям. Модель защиты АИС включает компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в АИС, ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов формируется при создании объекта и впоследствии может меняться. Изменение их значений обеспечивается только Пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту определяются посредством списка управления доступом. Список управления доступом включает перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

4.2. Аудит событий безопасности:

- АИС обеспечивает набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий позволяет обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к АИС или доступа к защищаемой информации. В частности, определяя политику аудита;

- уполномоченный администратор АИС имеет возможность осуществлять аудит только необходимых типов событий безопасности, таких как неудачные попытки подключения пользователей к АИС;

- запись результатов аудита событий безопасности осуществляется в журналы регистрации событий аудита, доступ к которому разрешен только уполномоченному администратору АИС;

- просмотр журналов регистрации событий аудита выполняется с использованием средств АИС (специализированных инструментальных средств). Данные средства предоставляют возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

4.3. Идентификация и аутентификация:

- АИС обеспечивает хранение паролей в преобразованном формате. АИС предоставляет средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля.

- АИС предоставляет механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором АИС или по истечении времени действия, заданного для счетчика блокировки.

4.4. Защита системы безопасности:

- изоляция процессов и поддержания домена безопасности обеспечивает безопасное выполнение функций системы безопасности АИС.

5. ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПОВЫШЕНИЯ НАДЕЖНОСТИ

АИС обеспечивает надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

5.1. Резервное копирование данных

В АИС входят стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования предоставляют Пользователям возможность выбора различных стратегий резервного копирования,

обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям предоставляется возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.

6. СРЕДА БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

6.1. Модели угроз, характерные для АИС

6.1.1. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся.

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

Используемые уязвимости – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемое свойство безопасности – конфиденциальность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба образовательному учреждению.

6.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся и их модификация (в том числе подмена).

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.

Используемые уязвимости – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемые свойства безопасности – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба образовательному учреждению.

6.1.3. Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения.

Источники угрозы – программное и аппаратное обеспечение.

Способ (метод) реализации угрозы – сбои (отказы) программного и аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучаемых.

Нарушаемое свойство безопасности – доступность, достоверность.

Возможные последствия реализации угрозы – нарушение со стороны образовательного учреждения взятых на себя обязательств по обработке персональных данных работников и обучающихся и может привести к прямому или косвенному материальному ущербу образовательному учреждению.

6.1.4. Нарушение согласованности данных в персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок персонала образовательного учреждения.

Источники угрозы – программное и аппаратное обеспечение, персонал образовательного учреждения.

Способ (метод) реализации угрозы – сбои (отказы) программного обеспечения и ошибки персонала образовательного учреждения.

Используемые уязвимости – недостатки механизмов обеспечения согласованности данных в БД АИС, связанные с возможностью нарушения согласованности.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемые свойства безопасности активов – достоверность, целостность.

Возможные последствия реализации угрозы – рассогласование в персональных данных работников и обучаемых, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесения морального и/или материального ущерба образовательному учреждению.

6.1.5. Осуществление доступа (ознакомления) с персональными данными обучающегося, хранимыми и обрабатываемыми в АИС, без согласия субъекта персональных данных или окончания срока действия такого согласия.

Источники угрозы – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

Способ (метод) реализации угрозы – осуществление доступа к персональным данным обучающихся с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.

Используемые уязвимости – недостатки механизмов защиты персональных данных обучающегося, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.

Вид информации, потенциально подверженной угрозе – персональные данные обучающихся.

Нарушаемые свойства безопасности – конфиденциальность.

Возможные последствия реализации угрозы – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба обучающемуся из-за несанкционированного раскрытия конфиденциальной информации.

6.2. Политика и цели безопасности для АИС

АИС обеспечивает следование приведенным ниже правилам безопасности:

6.2.1. обеспечена регистрация и учет получения (включая указание срока действия) согласия обучающегося на обработку предоставленных им в образовательное учреждение своих персональных данных.

6.2.2. обеспечена возможность надежного хранения персональных данных работников и обучающихся (в течение действия срока трудового договора и разрешения на обработку персональных данных соответственно).

6.2.3. обеспечена возможность безопасного восстановления АИС после сбоев и отказов программного обеспечения и оборудования.

6.2.4. обеспечена защита информации, составляющей персональные данные работников и обучающихся, при ее обработке, хранении и передаче специализированными средствами защиты.

6.2.5. обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора АИС о любых событиях, относящихся к безопасности АИС.

6.2.6. обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы образовательного учреждения, доступных только уполномоченным администраторам.

6.2.7. предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.

6.2.8. обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы функционируют в соответствии с сертифицированными алгоритмами.

6.3. Политика и цели безопасности

6.3.1. Среда функционирования АИС обеспечивает следование приведенным ниже правилам безопасности:

- обеспечена инженерно-техническая укреплённость объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.

- объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, оборудованы системой охранной сигнализации.

- исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.

- на объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности, обеспечено регулярное обновление антивирусных баз.

- объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.

- на объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, обеспечено отсутствие нештатных программных средств, не имеющих отношение к процессу функционирования образовательного учреждения.

- обеспечены установка, конфигурирование и управление программно- аппаратными средствами АИС в соответствии с руководствами и согласно оцененным конфигурациям.

- персонал, ответственный за администрирование АИС, благонадежен и компетентен.