ПРИНЯТА
на Совете учреждения
протокол № 1 от «27» июня 2019 г

УТВЕРЖДЕНА
приказом
от «28» июня 2019 г. № 157-ОП

СОГЛАСОВАНО
Первичная профсоюзная организация профсоюза работников народного образования и науки БПОУ ВО «ВТК»
Протокол от «17» июня 2019 г № 16

ПОЛОЖЕНИЕ
о порядке обработки и защите персональных данных в БПОУ ВО «Вологодский технический колледж»

1. Общие положения

1.1. Настоящим Положением регулируются отношения, связанные с обработкой персональных данных, осуществляемых БПОУ ВО «Вологодский технический колледж (далее – Колледж, оператор) с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированным на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

1.2. Целью настоящего Положения является обеспечения защиты прав и свобод работников и обучающихся Колледжа, персональные данные которых подлежат обработке Колледжем на основании полномочий оператора.

1.3. Настоящее Положение разработано в соответствии с требованиями законодательства РФ:

1.3.1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);

1.3.2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

1.3.3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных» (далее – Постановление Правительства от 01.11.2012 № 1119);

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

1.3.5. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. В настоящем Положении используются следующие основные понятия:

- ***персональные данные*** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- ***оператор*** - бюджетное профессиональное образовательное учреждение Вологодской области «Вологодский технический колледж», самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- ***обработка персональных данных*** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- ***автоматизированная обработка персональных данных*** - обработка персональных данных с помощью средств вычислительной техники;

- ***распространение персональных данных*** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- ***предоставление персональных данных*** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- ***блокирование персональных данных*** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- ***уничтожение персональных данных*** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- ***обезличивание персональных данных*** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- ***информационная система персональных данных*** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- ***трансграничная передача персональных данных*** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Принципы и условия обработки персональных данных

2.1. Основные принципы работы Колледжа с персональными данными:

2.1.1. Персональные данные получаются и обрабатываются добросовестным и законным образом.

2.1.2. Персональные данные собираются для точно определенных, объявленных и законных целей, не используются в противоречии с этими целями и в дальнейшем не обрабатываются каким-либо образом, не совместимым с данными целями.

2.1.3. Персональные данные должны соответствовать целям, для которых они собираются и обрабатываются, и не быть избыточными в отношении этих целей.

2.1.4. Сбор и обработка персональных данных в Колледже производится в целях реализации следующих задач:

- реализация трудовых договорных отношений с работниками, а также функционирование бухгалтерского и налогового учета в соответствии с действующим законодательством;

- реализация образовательных программ, учебного процесса, в том числе по оказанию платных услуг, связанных с обучением в соответствии с действующим законодательством.

2.2. Персональные данные должны быть точными, т.е. не допускать ошибок и искажений в сведениях о личности, регулярно обновляться и актуализироваться.

2.3. Персональные данные хранятся не дольше, чем это требуют цели их обработки и подлежат уничтожению по достижению данных целей, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных (перечень ИСПД Колледжа, с указанием объема обрабатываемых персональных данных, целей обработки и сроков хранения приведен в документе «Перечень информационных систем персональных данных БПОУ ВО «Вологодский технический колледж»).

2.4. Обработка персональных данных Колледжем осуществляется в следующих, предусмотренных ФЗ «О персональных данных», случаях:

2.4.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2.4.2. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а так же для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

2.5. Колледж ведет обработку персональных данных, относящихся к специальным категориям персональных данных только с письменного согласия субъекта персональных данных.

2.6. Колледж ведет обработку биометрических персональных данных только с письменного согласия субъекта персональных данных.

2.7. Колледжем не осуществляется трансграничная передача персональных данных.

2.8. Колледж вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных (пп.2 п.2 ст.22 ФЗ «О персональных данных»), поскольку данные получены оператором в связи с заключением договора, стороной которого является субъект персональных данных. В процессе обработки персональные данные не распространяются, а так же не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных.

2.9. Колледж в ряде случаев поручает обработку персональных данных третьим лицам (Перечень информации, передаваемой для обработки третьим лицам, с указанием объема передаваемой информации, основания для передачи, устанавливается локальным актом Колледжа).

2.10. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным (типовая форма согласия на обработку персональных данных субъекта персональных данных для работников и обучающихся утверждается локальным актом Колледжа).

2.11. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Колледж вправе продолжить обработку

персональных данных без согласия субъекта персональных данных на основании ч.2 ст.9 ФЗ «О персональных данных».

3. Права субъекта персональных данных

3.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

3.2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.3. В случае обращения субъекта персональных данных к Колледжу за предоставлением ему вышеуказанных сведений, данные сведения предоставляются ему в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных. Сведения предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Колледжем (номер и дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данным Колледжем, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3.4. В случае, если вышеуказанные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Колледжу или направить ему повторный запрос в целях получения вышеназванных сведений и ознакомления с ними не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

3.5. Субъект персональных данных вправе обратиться к оператору повторно или направить ему повторный запрос в целях получения вышеназванных сведений, а так же в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Колледж вправе мотивированно отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным ФЗ «О персональных данных».

3.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4. Обязанности оператора

4.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную п.3.1 настоящего Положения.

4.2. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 ФЗ «О персональных данных».

4.3. Поскольку предоставление персональных данных является обязательным в соответствии с ФЗ «О персональных данных», Колледж должен разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

4.4. Колледжем определяется состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и утверждаются в соответствии с ним следующие правовые акты:

4.4.1. назначение лица, ответственного за организацию обработки персональных данных.

4.4.2. издание локальных актов, определяющих политику Колледжа в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствие таких нарушений (Комплект организационно-распорядительной документации, регламентирующей деятельность Колледжа в отношении обработки персональных данных субъектов персональных данных утверждается приказом директора Колледжа).

4.4.3. применение правовых, организационных и технических мер по обеспечению персональных данных в соответствии со статьей 19 ФЗ «О персональных данных) для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а так же от иных неправомерных действий в отношении персональных данных, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (содержится в документе «Частная модель угроз безопасности персональных данных»);

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровне защищенности персональных данных (перечень применяемых мер содержится в пунктах 6 и 7 настоящего Положения).

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

- учетом машинных носителей персональных данных (учет машинных носителей ведется в соответствующем журнале по типовой форме).

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер (обнаруженные факты несанкционированного доступа к персональным данным и перечень принятия мер определяется инструкцией администратора безопасности).

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (перечень мероприятий по резервному копированию и восстановлению данных в случае несанкционированного доступа к ним определяется инструкцией администратора безопасности).

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных (обеспечивается средствами защиты, а так же мерами, регламентированными принятой организационно-распорядительной документацией).

4.4.4. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Колледжа в отношении обработки персональных данных, локальным актам Колледжа (перечень мероприятий по внутреннему контролю и проведению проверок приведен в документе «План проведения внутренних проверок режима защиты персональных данных»).

4.4.5. Ознакомление работников Колледжа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Колледжа в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) обучение указанных работников (ознакомление указанных работников с данными документами проводится ответственным за защиту информации, отметка об ознакомлении проставляется в «Журнале ознакомления»).

4.5. Колледж обязан предоставить вышеуказанные документы и локальные акты по запросу уполномоченного органа по защите прав субъектов персональных данных.

4.6. Колледж обязан сообщить в порядке, предусмотренном ст.14 ФЗ «О персональных данных» субъекту персональных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

4.7. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя, Колледж обязан дать в письменной форме мотивированный ответ, являющийся основанием для отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса персональных данных или его представителя.

4.8. Колледж обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителя сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Колледж обязан внести в него соответствующие изменения.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Колледж обязан уничтожить такие персональные данные.

Колледж обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4.9. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Колледж обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу уполномоченного органа по защите прав субъектов персональных данных, Колледж обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

4.10. В случае подтверждения факта неточности персональных данных Колледж на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов

персональных данных, или иных необходимых документов, обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Колледжа) в течение семи рабочих дней со дня предоставления таких сведений и снять блокирование персональных данных.

4.11. В случае выявления неправомерной обработки персональных данных, осуществляемой Колледжем или лицом, действующим по поручению Колледжа, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Колледж в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Колледж обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлен уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

4.12. В случае достижения целей обработки персональных данных Колледж прекращает обработку персональных данных и уничтожает их в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, или действующим законодательством.

5. Ответственность за нарушение пунктов настоящего положения

5.1. Лица, которым персональные данные стали известны в силу их служебного положения, принимают на себя обязательства по следующим направлениям:

5.1.1. обеспечение конфиденциальности этих персональных данных;

5.1.2. обеспечение сохранности, целостности и достоверности данных, в том числе и при передаче по международным информационно-телекоммуникационным системам;

5.1.3. обеспечение надлежащего правового режима этих данных при работе с ними на уровне держателя этих данных или при выдаче их работнику.

5.2. Виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

6. Дополнительные положения по защите персональных данных, обрабатываемых в информационных системах

6.1. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные, в соответствии с ч.5 ст.19 ФЗ «О персональных данных».

6.2. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности

персональных данных и информационных технологий, используемых в информационных системах.

6.3. Безопасность персональных данных при их обработке в ИСПДн обеспечивает Колледж, или лицо, осуществляющее обработку персональных данных по поручению Колледжа на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между Колледжем и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в ИСПДн.

6.4. Выбор средств технической защиты информации для системы защиты персональных данных осуществляется Колледжем в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности РФ и Федеральной службой по техническому и экспортному контролю во исполнение ч.4 ст.19 ФЗ «О персональных данных».

6.5. Согласно Постановлению Правительства РФ от 01.11.2012 № 1119:

6.5.1. информационные системы персональных данных, эксплуатируемые в Колледже, являются информационными системами, обрабатывающими персональные данные лиц, являющихся и не являющихся сотрудниками оператора;

6.5.2. актуальными угрозами безопасности персональных данных для ИСПДн, эксплуатируемых Колледжем, являются угрозы 3-го типа, т.е. угрозы. Не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

6.5.3. для ИСПДн, эксплуатируемых Колледжем, необходимо обеспечить 4-й уровень защищенности персональных данных при их обработке в ИСПДн (согласно акту классификации (определения уровня защищенности)).

6.6. Для обеспечения 4-го уровня защищённости персональных данных при их обработке в информационных системах Колледжа, необходимо выполнение следующих требований:

6.6.1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (определено в документе «Перечень мер, направленных на организацию режима обеспечения безопасности помещений в БПОУ ВО «Вологодский технический колледж»).

6.6.2. обеспечение сохранности носителей персональных данных.

6.6.3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей (определено в документах «Перечень лиц, допущенных к обработке персональных данных в БПОУ ВО «Вологодский технический колледж» и «Перечень лиц, осуществляющих техническое обслуживание информационных систем БПОУ ВО «Вологодский технический колледж»).

6.6.4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6.7. Контроль за выполнением настоящих требований организуется и проводится Колледжем самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление

деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже одного раза в 3 года в сроки, определяемые Колледжем.

6.8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий входят:

6.8.1. идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ):

- идентификация и аутентификация пользователей, являющихся работниками;
- управление идентификаторами, в т.ч. создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в т.ч. хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификации информации;
- идентификации и аутентификации пользователей, не являющихся работниками оператора (внешних пользователей).

6.8.2. Управление доступом субъектов доступа к объектам доступа (УПД):

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в т.ч. внешних пользователей;
- реализация необходимых методов(дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы а также между информационными системами;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- регламентация и контроль использования в информационной системе беспроводного доступа;
- регламентация и контроль использования в информационной системе мобильных технических средств;
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

6.8.3. Регистрация событий безопасности (РСБ):

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

- защита информации о событиях безопасности.

6.8.4. Антивирусная защита (АВЗ):

- реализация антивирусной защиты;

- обновление базы данных признаков вредоносных компьютерных программ (вирусов).

6.8.5. Контроль (анализ) защищенности персональных данных (АНЗ):

- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

6.8.6. Защита среды виртуализации (ЗСВ):

- идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в т.ч. администраторов управления средствами виртуализации;

- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в т.ч. внутри виртуальных машин.

6.8.7. Защита технических средств (ЗТС):

- контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

6.8.8. Защита информационной системы, ее средств, систем связи и передачи данных (СИЗ):

- обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в т.ч. беспроводным каналам связи.

6.9. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а так же с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер, могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

7. Дополнительные положения по защите персональных данных, обрабатываемых без использования средств автоматизации

7.1. Лица, осуществляющие обработку персональных данных без использования средств автоматизации в Колледже, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Колледжа (отметка о

прохождении инструктажа проставляется в журнале ознакомления работников с документами по обработке персональных данных).

7.2. В случае необходимости, уничтожение персональных данных проводится путем уничтожения материального носителя персональных данных способом, исключающим дальнейшую обработку этих персональных данных и использования материального носителя. По факту уничтожения составляется акт уничтожения персональных данных субъекта персональных данных.

7.3. Колледж принимает следующие меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации:

7.3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (определяется документами: «Перечень мест хранения материальных носителей персональных данных», «Перечень лиц, допущенных к обработке персональных данных»).

7.3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7.4. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ (Перечень принятых мер по охране материальных носителей персональных данных определяется документом «Перечень мер, направленных на организацию режима обеспечения безопасности помещений»).