Приложение №1
к Приказу ГБУ КО ПОО «КИТиС»
от 21.05 2015 года № 198

ПОЛОЖЕНИЕ
об обработке и защите персональных данных государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»

***Оглавление*:**

1. Общие положения

1.1. Настоящее Положение имеет своей целью закрепление механизмов обеспечения прав субъекта персональных данных на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Настоящее Положение об обработке и защите персональных данных (далее – Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников (сотрудников), обучающихся в **государственном бюджетном учреждении Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»** (далее – образовательная организация) в соответствии с законодательством Российской Федерации и гарантии конфиденциальности предоставленных сведений.

1.3. Данное Положение разработано в соответствии с Конституцией РФ, ст. 86 – 90 Трудового кодекса Российской Федерации, Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ, Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 г. № 188, Устава Государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства».

1.4. В рамках настоящего Положения ***Оператором*** персональных данных является **государственное бюджетное учреждение Калининградской области профессиональная образовательная организация «Колледж информационных технологий и строительства»**.

2. Цель и задачи в области защиты персональных данных

2.1. Целью и задачами в области защиты персональных данных в образовательной организации в соответствии с законодательством Российской Федерации является:

- обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- защита персональных данных, содержащихся в документах, полученных в обращениях субъектов персональных данных и других документах.

2.2. Персональные данные могут обрабатываться только для целей, непосредственно связанных с Уставной деятельностью образовательной организации.

3. Понятие и состав персональных данных

3.1. Для целей настоящего Положения используются следующие понятия:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Обучающийся – лицо, проходящее обучение в образовательной организации, и являющееся субъектом персональных данных.

Оператор персональных данных (далее – Оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Работник (сотрудник) – физическое лицо, состоящее в трудовых отношениях или иных договорных отношениях с оператором и являющееся субъектом персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных определенному кругу лиц.

Субъект персональных данных – физическое лицо, которому принадлежат те или иные персональные данные (*обучающиеся, родители (опекуны), сотрудники и т.д. и т.п.*).

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.

3.2. При обработке персональных данных образовательная организация устанавливает следующие категории персональных данных, в том числе:

а) персональные данные работников (сотрудников):

• фамилия; имя; отчество;

• число, месяц, год рождения;
• паспортные данные (номер, серия, кем и когда выдан);
• адрес постоянной регистрации;
• адрес фактического проживания;
• контактный телефон (домашний, мобильный, рабочий);
• свидетельство государственного пенсионного страхования;
• начисления по заработной плате;
• сведения о льготах;
• данные о вычетах и взносах;
• национальность;
• сведения о ближайших родственниках;
• социальный пакет;
• код по диагнозу заболевания;
• сведения об опекунах (фамилия, имя, отчество, социальное положение, место работы, должность, место проживания в настоящее время, контактные телефоны);
• номер банковского счета для перечисления стипендии и денежных компенсаций для детей-сирот;
• фотография;
• данные свидетельства о постановке на налоговый учет ИНН;
• данные о трудовом стаже;
• номер полиса ОМС;
• начисления по заработной плате;
• сведения о льготах;
• место рождения;
• гражданство;
• сведения по инвалидности;
• количество и возраст детей;
• сведения об образовании, повышении квалификации, аттестации;
• справка о наличии судимости;
• сведения о награждениях;
• сведения о почетных званиях и степенях.

в) персональные данные обучающихся:

• фамилия; имя; отчество;
• число, месяц, год рождения;
• паспортные данные (номер, серия, кем и когда выдан);
• адрес постоянной регистрации;
• адрес фактического проживания;
• место рождения;
• контактный телефон (домашний, мобильный, рабочий);
• гражданство;
• сведения о ближайших родственниках (фамилия, имя, отчество, контактные телефоны, данные свидетельства о смерти, данные о составе семьи);

• сведения об опекунах (фамилия, имя, отчество; социальное положение, место работы, должность, место проживания в настоящее время, контактные телефоны);
• данные свидетельства о постановке на налоговый учет ИНН;
• свидетельство государственного пенсионного страхования;
• сведения о льготах;
• номер полиса ОМС;
• социальный пакет;
• сведения по инвалидности;
• количество и возраст детей;
• сведения об образовании, повышении квалификации, аттестации;
• данные о состоянии здоровья (диагноз);
• данные о трудовом стаже;
• сведения о наградах, ученой степени, званиях;
• сведения о социальном статусе;
• сведения об опекунах;
• сведения об обучающихся с ограниченными возможностями здоровья

4. Обработка персональных данных

4.1. В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных образовательная организация как Оператор **ОБЯЗАНА** соблюдать следующие требования:
• осуществлять обработку персональных данных с согласия субъекта персональных данных;
• осуществлять обработку персональных данных на законной и справедливой основе и исключительно в целях обеспечения соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов РФ;
• не использовать персональные данные в целях причинения имущественного и (или) морального вреда гражданам, затрудняющего реализацию прав и свобод граждан Российской Федерации;
• не принимать решений, затрагивающих интересы субъекта персональных данных, основываясь на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения;
• обеспечивать, при обработке субъекта персональных данных, точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
• принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных субъекта персональных данных;
• ознакомить субъектов персональных данных, не являющихся работниками (сотрудниками), или их законных представителей с документами образовательной организации, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

4.2. Содержание и объем обрабатываемых персональных данных субъекта должны соответствовать заявленным целям обработки персональных данных в образовательной организации.
4.3. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки в образовательной организации.
4.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4.5. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту информации, касающихся персональных данных; частной жизни, личной и семейной тайны.

5. Получение персональных данных

5.1. Все персональные данные, обрабатываемые в образовательной организации, следует получать непосредственно от субъекта персональных данных.
5.2. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.
5.3. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.
5.4. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой, позволяющей подтвердить факт его получения, форме, если иное не установлено федеральным законодательством
5.5. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законодательством - электронной подписью.
5.6. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные данные субъекта следует получать от его законных представителей (родителей, попечителей, опекунов и т.д.). Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на обработку их и своих персональных данных образовательной организации.
Полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются образовательной организацией как Оператором.
5.7. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:
• фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

• фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
• наименование, адрес образовательной организации или фамилию, имя, отчество, адрес получающего согласие субъекта персональных данных;
• цель обработки персональных данных;
• перечень персональных данных, на обработку которых, дается согласие субъекта персональных данных;
• наименование, адрес образовательной организации или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу или образовательной организации;
• перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
• срок, в течение которого, действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
• подпись субъекта персональных данных.

5.8. Письменное согласие на обработку персональных данных **НЕ ТРЕБУЕТСЯ** в случаях:
• если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого, является субъект персональных данных.

5.9. Согласие на обработку персональных данных может быть отозвано субъектом и (или) его законным представителем.

5.10. В случаях, когда образовательная организация как Оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

В уведомлении образовательная организация как Оператор **ОБЯЗАНА** сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение.

Согласие оформляется в письменной форме в 2 (двух) экземплярах: один – предоставляется субъекту, второй – хранится в образовательной организации.

5.11. Обязанность представить доказательства получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований на обработку его персональных данных, возлагается на образовательную организацию как на Оператора.

5.12. Образовательная организация, как образовательное учреждение,

в соответствии с федеральным законодательством Российской Федерации в области образования обеспечивает открытость и доступность сведений о персональном составе педагогических работников с указанием уровня образования и квалификации.

5.13. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации образовательная организация как Оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

5.14. В трудовые, в гражданско-правовые договоры с работниками (сотрудниками) образовательной организации вносятся условия об обработке персональных данных работников (сотрудников),

5.15. В договоры по оказанию услуг вносятся условия по соблюдению конфиденциальности представляемой информации в соответствии с действующим законодательством Российской Федерации.

5.16. **ЗАПРЕЩАЕТСЯ** получать и обрабатывать персональные данные субъекта персональных данных о его частной жизни, а также политических, религиозных и иных убеждениях, о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

6. Хранение персональных данных

6.1. Хранение персональных данных субъектов персональных данных в образовательной организации осуществляется как на бумажных, так и на электронных носителях с ограниченным доступом.

6.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому, является субъект персональных данных.

6.3. Работники (сотрудники) образовательной организации, хранящие персональные данные на электронных носителях, в электронных базах данных, обеспечивают их защиту от несанкционированного доступа и копирования.

6.4. Работники (сотрудники) образовательной организации, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному Постановлением Правительства Российской Федерации 15 сентября 2008 г. № 687.

7. Передача персональных данных

7.1. При передаче персональных данных субъектов персональных данных образовательная организация как Оператор **ОБЯЗАНА** соблюдать следующие требования:

• не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в случаях, предусмотренных Трудовым кодексом и федеральным законодательством Российской Федерации;
• предупреждать лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;
• не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
• не запрашивать информацию о состоянии здоровья субъекта персональных данных за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции;
• передавать персональные данные субъекта персональных данных представителям субъекта персональных данных в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;
• регистрировать все сведения о передаче персональных данных субъекта в «*Журнале учета входящих или исходящих документов*» в целях контроля правомерности использования данной информации получившими ее лицами. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

7.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта персональных данных распространяются как на **бумажные**, так и на **электронные (автоматизированные)** носители информации.

8. Внутренний доступ (доступ внутри образовательной организации) к персональным данным субъекта

8.1. Право доступа к персональным данным субъекта персональных данных имеют:
• директор образовательной организации;
• определенные перечнем работники (сотрудники) образовательной организации, доступ которых к персональным данным необходим для выполнения своих должностных обязанностей;
• сам субъект, носитель данных;
• представители субъекта персональных данных.

8.2. Все работники (сотрудники) образовательной организации, имеющие доступ к персональным данным субъектов персональных данных, обязаны подписать соглашение о неразглашении персональных данных.

8.3. К числу массовых потребителей персональных данных, вне образовательной организации, относятся государственные и негосударственные функциональные структуры; налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления.

Контрольные и надзорные органы имеют доступ к информации в сфере своей компетенции.

8.4. Учреждения, в которые субъект персональных данных может осуществлять перечисления денежных средств (страховые организации, негосударственные пенсионные фонды, благотворительные и кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

8.5. Процедура оформления доступа к персональным данным работников (сотрудников), обучающихся включает в себя ознакомление лиц, осуществляющих обработку персональных данных или имеющих к ним доступ, с настоящим Положением, в листе ознакомлений, под роспись (п.8 ст.86 ТК РФ).

8.6. Обязанность ознакомления работников (сотрудников) и обучающихся с настоящим Положением лежит на директоре образовательной организации.

Примечание:

При наличии иных нормативных актов (приказов, распоряжений), регулирующих обработку персональных данных работников (сотрудников), обучающихся также производится ознакомление лиц, осуществляющих обработку персональных данных или имеющих к ним доступ, под роспись.

8.7. Управление и разграничение доступа к электронным базам данных образовательной организации, содержащим персональные данные работников (сотрудников) и обучающихся образовательной организации в образовательной организации, обеспечивается техническими средствами защиты информации, сертифицированными ФСТЭК России как средства защиты информации, использующиеся при построении системы защиты информационных систем персональных данных соответствующего класса.

8.8. Пользователи информационных систем персональных данных должны быть ознакомлены с правилами работы с персональными данными и проинструктированы о необходимых мерах, обеспечивающих безопасность персональных данных при их обработке в информационных системах персональных данных.

9. Уничтожение персональных данных

9.1. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки.

9.2. Уничтожение персональных данных осуществляется:

• по достижении цели обработки персональных данных;

• в случае утраты необходимости в достижении целей обработки

персональных данных;
• в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
• по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов в случае
выявления фактов совершения образовательной организацией неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.
9.3. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.
9.4. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
9.5. Уничтожение персональных данных должно быть осуществлено в течение 3 (трех) дней с указанных в **п.9.2** моментов. Факт уничтожения персональных данных субъекту персональных данных, проводится актом уничтожения, с подписью ответственных(ого) лиц(а) за уничтожение.
9.6. После уничтожения образовательная организация направляет уведомление об уничтожении персональных данных субъекту персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, направляет уведомление об уничтожении персональных данных в уполномоченный орган.

10. Права и обязанности субъектов персональных данных

10.1. В целях обеспечения защиты персональных данных субъект персональных данных **ИМЕЕТ ПРАВО:**
• получать информацию, касающуюся 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 образовательной организации как 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 образовательной организацией 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 о состоявшейся или предполагаемой трансграничной

передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению образовательной организации, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими Федеральными законами.
• получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
• требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;
• заявлять в письменной форме о своем несогласии, предоставив соответствующее обоснование, при отказе образовательной организации как Оператора или уполномоченного им лица исключить или исправить персональные данные субъекта;
• дополнять персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;
• требовать от образовательной организации как от Оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;
• на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
10.2. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

11. Обязанности образовательной организации как Оператора при работе с персональными данными субъектов персональных данных

11.1. В целях обеспечения защиты персональных данных образовательная организация как Оператор **ОБЯЗАНА** принимать меры, необходимые и достаточные для обеспечения защиты персональных данных, предусмотренных Федеральным законодательством.
11.2. Образовательная организация как Оператор самостоятельно определяет перечень мер, необходимых и достаточных для обеспечения защиты персональных данных, предусмотренных Федеральным законодательством.
11.3. Для защиты персональных данных субъектов персональных данных образовательная организация как Оператор **ОБЯЗАНА**:
• назначить ответственного за организацию обработки персональных данных в образовательной организации из числа сотрудников;
• ознакомить работников (сотрудников), обучающихся с настоящим Положением, его правами в области защиты персональных данных под расписку;
• применить правовые, организационные и технические меры по обеспечению безопасности персональных данных;

• за свой счет обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;
• по запросу ознакомить субъекта персональных данных или его законных представителей с настоящим Положением, а также с другими документами образовательной организации, устанавливающими порядок обработки персональных данных, правами субъекта персональных данных в области защиты персональных данных, с соответствующим заполнением граф в *«Журнале учета обращений граждан (субъектов персональных данных) о выполнении их законных прав в области защиты персональных данных»*;
• осуществлять передачу персональных данных субъекта персональных данных только в соответствии с настоящим Положением и законодательством Российской Федерации;
• предоставлять персональные данные субъекта персональных данных только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим положением и законодательством Российской Федерации;
• обеспечить субъекту персональных данных свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;
• по требованию субъекта персональных данных или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

11.4. Актом директора образовательной организации необходимо

УТВЕРДИТЬ:

• правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами образовательной организации;
• перечень информационных систем персональных данных;
• перечни персональных данных, обрабатываемых в образовательной организации в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;
• перечень должностей работников образовательной организации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
• должностную инструкцию ответственного за организацию обработки персональных данных в образовательной организации;
• типовое обязательство сотрудников образовательной организации, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ними трудового договора прекратить обработку

персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

• типовая форма согласия на обработку персональных данных работников образовательной организации, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

• порядок доступа работников образовательной организации в помещения, в которых ведется обработка персональных данных.

11.5. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуется проведение периодических проверок условий обработки персональных данных в образовательной организации.

11.6 Журнал внутренних проверок режима защиты персональных данных, содержит перечень внутренних проверок, проводимых в образовательной организации.

Журнал составляется для мероприятий в соответствии с Планом мероприятий по обеспечению защиты персональных данных и определяет периодичность проведения проверок.

Журнал внутренних проверок содержит следующую информацию:

• название проверяемого мероприятия.

• периодичность проведения проверки.

• исполнитель мероприятия.

Журнал внутренних проверок распространяется на все информационные системы персональных данных образовательной организации.

11.7. Проверки осуществляются ответственным за организацию обработки персональных данных в образовательной организации либо комиссией, утвержденной директором образовательной организации. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору образовательной организации докладывает ответственный за организацию обработки персональных данных в образовательной организации либо председатель комиссии.

11.8. При получении персональных данных не от субъекта персональных данных образовательная организация как Оператор до начала обработки таких персональных данных **ОБЯЗАНА** предоставить субъекту персональных данных следующую информацию:

• наименование либо фамилию, имя, отчество и адрес оператора или его представителя;

• цель обработки персональных данных и ее правовое основание;

• предполагаемые пользователи персональных данных; • установленные настоящим Федеральным законом права субъекта
персональных данных;

• источник получения персональных данных.

11.9. Срок хранения документов, указанных в п.п. **11.3; 11.4; 11.6; 11.8** зависит от того, какие юридические последствия могут возникнуть для образовательной организации как Оператора осуществляющей обработку

персональных данных, если образовательная организация как Оператор не будет обладать информацией содержащейся в вышеуказанных документах.
11.10. Образовательная организация как Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. **11.8** настоящего Положения в случаях, если:
• субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим Оператором;
• персональные данные получены Оператором на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных • персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
• Оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных.
11.11. Образовательная организация обязуется обеспечить неограниченный доступ к настоящему Положению, определяющему политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.
11.12. Образовательная организация как Оператор осуществляет сбор персональных данных с использованием информационно телекоммуникационных сетей и обязуется опубликовать на официальном сайте образовательной организации документы, определяющие политику в отношении обработки персональных данных, в течение 10 (десяти) дней после их утверждения.
11.13. Образовательная организация как Оператор при обработке персональных данных **ОБЯЗАНА** принимать необходимые **правовые, организационные и технические меры** или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных:
• устанавливать правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
• обеспечивать регистрацию и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных образовательной организации;
• учитывать материальные носители персональных данных образовательной организации.
11.14. Образовательной организации как Оператору при обработке персональных данных субъекта **ЗАПРЕЩАЕТСЯ** принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и

законные интересы на основании исключительно автоматизированной обработки персональных данных. Любые решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных могут быть приняты только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных Федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

11.15. Образовательная организация как Оператор **ОБЯЗАНА**:

- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения;
- предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;
- рассмотреть возражение в течение 30 (тридцати) дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

11.16. Образовательная организация как Оператор **ОБЯЗАНА** разъяснить субъекту персональных данных **юридические последствия отказа предоставить его персональные данные**, если предоставление персональных данных является обязательным в соответствии с Федеральным законом.

12. Общедоступные источники персональных данных

12.1. В целях информационного обеспечения в образовательной организации могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги).

12.2. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его:

- фамилия, имя, отчество;
- год и место рождения;
- адрес;
- абонентский номер;
- сведения о профессии;
- иные персональные данные, сообщаемые субъектом персональных данных.

12.3. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

13. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

13.1. Образовательная организация как Оператор **ОБЯЗАНА** назначить лицо ответственное за организацию обработки персональных данных.

13.2. Лицо, ответственное за организацию обработки персональных данных, подчиняется директору образовательной организации и получает указания непосредственно от него.
13.3. Лицо, ответственное за организацию обработки персональных данных в образовательной организации, **ОБЯЗАНО**:
• осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской
Федерации о персональных данных, в том числе требований к защите персональных данных;
• доводить до сведения работников (сотрудников) образовательной организации положения: законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (приказы, инструкции); требования к защите персональных данных;
• организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.
13.4. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации.
Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.
13.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.
13.6. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных изложена в:
• Кодексе об административных правонарушениях Российской Федерации (КоАП РФ) – статьи **13.11, 13.14, 5.39, 19.7;**
• Уголовном Кодексе Российской Федерации (УК РФ) – статьи **137, 140, 272; 81,90, 237.**
• Трудовом Кодексе Российской Федерации (ТК РФ) – статьи **14. Подача уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Управление Роскомнадзора по Калининградской области)**
14.1. До начала обработки персональных данных образовательная организация как Оператор **ОБЯЗАНА** уведомить уполномоченный орган по защите прав субъектов персональных данных **(Управление Роскомнадзора по Калининградской области)** о своем намерении осуществлять обработку

персональных данных.
14.2. Образовательная организация как Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:
• обрабатываемых в соответствии с трудовым законодательством;
• полученных Оператором в связи с заключением договора,
стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
• относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без письменного согласия субъектов персональных данных;
• включающих в себя только фамилии, имена и отчества субъектов персональных данных;
• необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится образовательная организация, или в иных аналогичных целях;
• включенных в информационные системы персональных данных, имеющих в соответствии с Федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
• обрабатываемых без использования средств автоматизации в соответствии с Федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.
14.3. Уведомление, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается директором образовательной организации или уполномоченным лицом.
14.4. Уведомление должно содержать следующие сведения:
• наименование образовательной организации;
• адрес образовательной организации как Оператора;
• цель обработки персональных данных;
• категории персональных данных;
• категории субъектов, персональные данные которых обрабатываются;
• правовое основание обработки персональных данных;

• перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
• описание мер, предусмотренных ст. 18.1 и ст.19 ФЗ-152 «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
• фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
• дата начала обработки персональных данных;
• срок или условие прекращения обработки персональных данных;
• сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
• сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

14.5. В случае изменения сведений, указанных в **п. 14.4** настоящей статьи, а также в случае прекращения обработки персональных данных образовательная организация как Оператор **ОБЯЗАНА** уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение 10 (десяти) рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

15. Заключительные положения

15.1. Настоящее Положение не заменяет собой действующего законодательства Российской Федерации, регулирующего общественные отношения в сфере обработки персональных данных и обеспечения их безопасности и конфиденциальности.

15.2. При изменении Федеральных законов и иных нормативных правовых актов отдельные требования настоящего Положения вступят в противоречие с указанными законами и нормативными правовыми актами, соответствующие требования Положения не будут подлежать применению.

Приложение №2
к Приказу ГБУ КО ПОО «КИТиС»
от 21.05 2015 года № 198

Инструкция
пользователя информационных систем
персональных данных

1. Общие положения

1.1. Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в информационной системе персональных данных (далее – ИСПДн).

1.2. Пользователь информационных систем персональных данных (далее – Пользователь) осуществляет обработку персональных данных (далее – ПДн) в ИСПДн.

1.3. Пользователями являются сотрудники **государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»** (далее – образовательная организация), имеющие доступ к программному обеспечению, средствам защиты и участвующие, в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации, содержащей ПДн, допущенные к работе в ИСПДн, в соответствии с приказом «Об утверждении списка лиц, которым необходим доступ к ПДн, обрабатываемым в ИСПДн, для выполнения своих служебных (трудовых) обязанностей».

1.4. Пользователь несет персональную ответственность за свои действия при обработке ПДн на средствах вычислительной техники (далее – СВТ).

1.5. Пользователь в своей работе руководствуется настоящей Инструкцией, утвержденным Положением по обработке персональных данных, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю России и регламентирующими документами образовательной организации.

1.6. Методическое руководство работой пользователя осуществляется ответственным лицом за организацию обработки ПДн и выполнение мероприятий по обеспечению безопасности ПДн в образовательной организации.

2. Обязанности пользователя

2.1. При обработке ПДн пользователь **ОБЯЗАН**:

• знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите персональных данных и распоряжений, регламентирующих порядок действий по защите персональных данных;

• выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены для него в соответствии со списком постоянных пользователей и разграничение прав доступа к обрабатываемым ПДн в ИСПДн;
• знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно распорядительных документов;
• знать и соблюдать установленные требования по учету и хранению съемных носителей информации. Проверять перед началом работы файлы, хранящиеся на съемных носителях информации, на наличие компьютерных вирусов. Антивирусный контроль на СВТ должен осуществляться пользователем не реже 1 (одного) раза в неделю;
• соблюдать установленный режим разграничения доступа к информационным ресурсам: иметь пароль безопасности, надежно его запоминать и хранить в тайне, выполняя требования парольной политики образовательной организации;
• помнить личные пароли и идентификаторы;
• соблюдать установленную технологию обработки информации;
• соблюдать правила при работе в сетях общего доступа и международного обмена (сеть Интернет);
• соблюдать правила при использовании электронной почты;
• располагать экран монитора в помещении во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами. Шторы на оконных проемах должны быть завешаны (жалюзи закрыты);
• руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники и средств защиты информации;
• обо всех выявленных нарушениях, связанных с информационной безопасностью образовательной организации, необходимо обратиться к администратору информационной безопасности (далее – Администратор ИБ) или к директору образовательной организации;
• блокировать ввод-вывод информации на своем рабочем месте ИСПДн в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИСПДн;
• блокировать вывод информации на монитор СВТ. 2.2. Для получений консультаций по вопросам информационной безопасности необходимо обращаться к специалистам отдела защиты информации обособленного подразделения закрытого акционерного общества « КАЛУГА АСТРАЛ» в г . Калининграде и Калининградской области и сотрудникам отдела защиты информации: общества с ограниченной ответственностью «И-Сервис», по электронной почте: **astral@inok.ru** или по телефону **777-155 доп. 230,232,233.**

2.3. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИБ образовательной организации.

2.4. Пользователям **ЗАПРЕЩАЕТСЯ**:

• разглашать защищаемую информацию третьим лицам;

• записывать и хранить информацию на неучтенных съемных носителях информации;

• оставлять во время работы съемные носители информации (или СВТ со съемными носителями информации) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

• производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

• самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

• несанкционированно открывать общий доступ к папкам на своей рабочей станции;

• подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

• отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на данные СВТ;

• обрабатывать на СВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

• сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

• производить копирование отдельных файлов с учтенных носителей информации на неучтенные носители информации, в том числе для временного хранения информации;

• работать на СВТ при обнаружении каких-либо неисправностей;

• хранить носители информации вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

• привлекать посторонних лиц для производства ремонта или настройки СВТ, без согласования с ответственным лицом за обеспечение защиты ПДн;

• при отсутствии визуального контроля за СВТ доступ к ним должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

• принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью ликвидации их последствий в рамках возложенных на него функций.

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором ИБ.

3.2. Смена паролей пользователей в ИСПДн проводится самостоятельно, не реже одного раза в 10 (десять) дней. 3.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 (три) месяца.

3.4. Правила формирования пароля:

• пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

• пароль должен состоять не менее чем из шести буквенно- цифровых символов;

• в пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;

2) строчные буквы английского алфавита от a до z;

3) десятичные цифры (от 0 до 9);

4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

3.5. При формировании пароля **ЗАПРЕЩАЕТСЯ:**

• использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

• использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

• использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

• выбирать пароли, которые уже использовались ранее.

3.6. Правила ввода пароля:

• ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

• во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.7. Правила хранения пароля:

• запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

• запрещается сообщать другим пользователям личный пароль и регистрироваться в системе под своим паролем.

3.8. Лица, использующие паролирование, **ОБЯЗАНЫ**:

• четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

• своевременно сообщать Администратору ИБ об утере, компрометации, несанкционированном изменении паролей• ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
• во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
3.7. Правила хранения пароля:
• запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
• запрещается сообщать другим пользователям личный пароль и регистрироваться в системе под своим паролем.
3.8. Лица, использующие паролирование, **ОБЯЗАНЫ**:
• четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
• своевременно сообщать Администратору ИБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Общие обязанности пользователей по обеспечению информационной безопасности при работе в ИСПДн

4.1. Каждый пользователь образовательной организации, участвующий в рамках своих функциональных обязанностей в процессе автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным несет персональную ответственность за свои действия и обязан:
• строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами;
• знать и строго выполнять правила работы со средствами защиты информации, установленными на объекте информатизации;
• выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей;
• выполнять требования «Инструкции по организации парольной защиты», хранить в тайне свой пароль (пароли), с установленной периодичностью менять свой пароль (пароли);
• хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу).
4.2. Немедленно проверять свое рабочее место в случаях обнаружения:
• нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах персонального компьютера (далее – ПК) или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (далее – НСД) к защищенным СВТ;
• несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств СВТ;
• отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или

неустойчивого функционирования узлов СВТ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
• некорректного функционирования установленных на СВТ технических средств защиты;
• непредусмотренных отводов кабелей от СВТ и подключенных к нему устройств.

5. Порядок работы с персональными данными

5.1. Перед началом работы с ПДн:
• исключить несанкционированное пребывание в помещениях образовательной организации, где обрабатываются ПДн посторонних лиц;
• ознакомиться с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации;
• изучить Инструкцию пользователя по системе защиты от несанкционированного доступа (если такое программное оборудование установлено);
• закрыть окна помещения непрозрачными шторами или жалюзи;
• иметь необходимые учтенные документы и (или) сменные носители информации (флеш-карта, СЖД, CD-R, CD-RW).
5.2. В процессе работы с ПДн **НЕОБХОДИМО**:
• обрабатывать информацию в соответствии с технологическим процессом обработки информации, имея права доступа к обрабатываемой в системе информации и настройкам системы в соответствии с правами доступа и настройками, установленными Администратором ИБ; • результаты работы (готовые данные) записываются только на учтенный жесткий диск СВТ в папку пользователя. При возникновении необходимости записи учтенной информации на сменный носитель (флеш-карта, СЖД, CD-R, CD-RW) обратиться к Администратору ИБ.
5.3. Постановка на учет распечатанных конфиденциальных документов производится в установленном порядке.

6. Правила работы в сетях общего доступа и (или) международного обмена

6.1. Работа в сетях общего доступа и (или) международного обмена (далее – сеть Интернет) на элементах ИСПДн должна проводиться при служебной необходимости.
6.2. Сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Образовательная организация как оператор ПДн оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых, запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство

других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе, разъясняющие порядок применения взрывчатых веществ и иного оружия.

6.3. При работе с ресурсами сети Интернет **НЕДОПУСТИМО**:

• разглашение служебной информации образовательной организации, ставшей известной сотрудникам образовательной организации по служебной необходимости либо иным путем;

• распространение коммерческой тайны;

• публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения, либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения НСД к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

6.4. При работе в Сети Интернет **ЗАПРЕЩАЕТСЯ:**

• загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

• использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой образовательной организации;

• осуществлять работу при отключенных средствах защиты (антивирус и других);

• передавать по Сети защищаемую информацию без использования средств шифрования;

• запрещается скачивать из Сети программное обеспечение и другие файлы;

• запрещается посещение сайтов с сомнительной репутацией (сайты порнографического содержания, сайты, содержащие нелегально распространяемое программное обеспечение и другие); • запрещается нецелевое использование подключения к Сети.

7. Правила работы с электронной почтой образовательной организации

7.1. При работе с корпоративной системой электронной почты сотрудникам образовательной организации ЗАПРЕЩАЕТСЯ:

• использовать адрес электронной почты для оформления подписок, без предварительного согласования с директором образовательной организации;

• публиковать свой адрес, либо адреса других сотрудников образовательной организации на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

• отправлять сообщения с вложенными файлами, общий объем которых превышает 5 Мегабайт;
• открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
• осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
• осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с Директором образовательной организации;
• рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения НСД к платным ресурсам в сети Интернет, а также ссылки на вышеуказанную информацию;
• распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и (или) авторские и смежные с ним права третьей стороны;
• распространять информацию, содержание и направленность которой, запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе, разъясняющие порядок применения взрывчатых веществ и иного оружия;
• распространять информацию ограниченного доступа, представляющую коммерческую тайну образовательной организации;
• предоставлять пароли доступа к своему почтовому ящику, лицам, не имеющим доступа к информационным системам образовательной организации.

8. Ответственность

8.1. Пользователь несет персональную ответственность:
• за соблюдение установленной технологии обработки информации;
• за соблюдение режима конфиденциальности ПДн при их обработке и хранении в ИСПДн;
• за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

• за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с ПДн;
• за несоблюдение правил осуществления обработки персональных данных сотрудников в соответствии с положением Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».
8.2. Все сотрудники образовательной организации, обрабатывающие ПДн, должны быть предупреждены об ответственности.

9. Заключительные положения

9.1. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным в образовательной организации.
9.2. Вся информация о ресурсах, посещаемых сотрудниками образовательной организации, протоколируется и, при необходимости, может быть предоставлена директору образовательной организации для детального изучения.
9.3. Сотрудники, определенные приказом директора образовательной организации как пользователи, участвующие в обработке ПДн, должны ознакомиться с настоящей Инструкцией.
9.4. Обязанность ознакомления пользователей с настоящей Инструкцией лежит на ответственном лице за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в образовательной организации.

Приложение №3
к Приказу ГБУ КО ПОО «КИТиС»
от «21» 05 2015 года № 198

Инструкция
по организации режима доступа в помещения
1. Общие положения

1.1. Защита от проникновения посторонних лиц в помещения **государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»** (далее – образовательная организация) обеспечивается организацией режима доступа, а также соответствующей инженерно-технической защитой помещений образовательной организации с установленными в них средствами электронно-вычислительной техники (далее – ЭВТ), которые предусматривают проведение следующих мероприятий:

• инженерно-техническая защита (наличие охранной сигнализации);

• защита технических средств ЭВТ и носителей информации от несанкционированного доступа, повреждения или хищения.

2. Пропускной режим предусматривает:

• определение перечня должностных лиц, имеющих право доступа в определенные зоны (технологические, административные и др.) образовательной организации.

3. Внутриобъектовый режим предусматривает:

• определение круга должностных лиц, имеющих право на работу с документами конфиденциального характера и лиц, допускаемых к той или иной конфиденциальной информации;

• определение категории и правил работы с информацией;

• обеспечение установленного порядка работы с конфиденциальной информацией;

• осуществление контроля использования технических средств, предназначенных для обработки конфиденциальной информации.

3.1. Помещения, в которых устанавливаются средства ЭВТ, должны надежно охраняться и иметь:

• прочные двери, оборудованные замками повышенной надежности и, при необходимости, замки с контролерами доступа;

• технические средства охраны, связанные с центральным пультом охраны, осуществляющим охрану здания и помещений образовательной организации.

3.2. Выдачу ключей от помещений образовательной организации осуществлять должностным лицам, ответственным за данное помещение.
3.3. Уборка этих помещений должна производиться в присутствии лиц, ответственных за эти помещения. В случае ухода из помещений в рабочее время необходимо закрывать их на ключ.
3.4. В нерабочее время помещения должны закрываться и сдаваться под охрану либо охраняться сотрудниками образовательной организации на основании внутренних приказов директора ГБУ КО ПОО «КИТиС».

4. Защита технических средств ЭВТ и носителей информации от несанкционированного доступа, повреждения или хищения

4.1. Во время эксплуатации средств ЭВТ, предназначенных для обработки конфиденциальной информации, должны быть предусмотрены меры по исключению случаев несанкционированного вскрытия средств ЭВТ при проведении ремонтных, профилактических и других видов работ.
4.2. Порядок допуска к узлам, блокам и другим составным элементам средств ЭВТ определяет администратор информационной безопасности.
4.3. В случае необходимости проведения ремонтных работ на средствах ЭВТ с привлечением специализированных ремонтных организаций или передачи им оборудования **обеспечивается обязательное гарантированное уничтожение (стирание) конфиденциальной информации на жестких дисках** под контролем администратора информационной безопасности образовательной организации, о чем составляется протокол (акт).

5. Заключительные положения

5.1. Сотрудники ГБУ КО ПОО «КИТиС», должны ознакомиться с настоящей Инструкцией.
5.2. Обязанность ознакомления пользователей с настоящей Инструкцией лежит на ответственном лице за выполнение мероприятий по обеспечению безопасности персональных данных в ГБУ КО ПОО «КИТиС.

Приложение №4
к Приказу ГБУ КО ПОО «КИТиС»
от 21.05 2015 года № 198

Инструкция
о порядке планирования и проведения проверок информационной безопасности в информационных системах персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет порядок планирования и проведения проверок информационной безопасности от несанкционированного доступа, распространения, искажения и утраты в информационных системах персональных данных **государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»** (далее – образовательная организация).

1.2. Проверка информационной безопасности в информационных системах персональных данных (далее – ИСПДн) образовательной организации осуществляется не реже 1 (одного) раза в год.

1.3. В ходе проверки осуществляется контроль эффективности внедренных на объекте защитных мер, средств защиты информации в соответствии с требованиями предписаний на эксплуатацию технических средств и средств защиты информации.

Обязательным является контроль:

- при вводе ИСПДн в эксплуатацию;
- после ремонта технических средств, входящих в состав ИСПДн и средств защиты информации;
- при изменении условий эксплуатации ИСПДн и размещения технических средств.

2. Контроль аппаратного обеспечения

2.1. Контроль работоспособности аппаратных компонентов ИСПДн, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

2.2. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности, должны контролироваться постоянно в рамках работы администраторов информационной безопасности соответствующих ИСПДн.

3. Контроль парольной защиты

3.1. Контроль парольной защиты и контроль надежности пользовательских паролей проводится на основе Инструкции по организации парольной защиты и предусматривает:

• установление сроков действия паролей;

• периодическую проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4. Контроль целостности

4.1. Контроль целостности программного обеспечения включает следующие действия:

• проверка контрольных сумм и цифровых подписей каталогов и файлов, сертифицированных программных средств при загрузке операционной системы;

• обнаружение дубликатов идентификаторов пользователей; • восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Контроль попыток несанкционированного доступа

5.1. Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы, специальных программных средств и предусматривает:

• фиксацию неудачных попыток входа в систему в системном журнале;

• протоколирование работы сетевых сервисов;

• выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимость.

6. Контроль производительности

6.1. Контроль производительности ИСПДн производится по обращениям пользователей в ходе администрирования системы и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности системы.

7. Контроль защищенности системного и прикладного программного обеспечения

7.1. Контроль защищенности системного и прикладного программного обеспечения производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

7.2. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния ИСПДн уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют цель: выявление всех несоответствий между текущим состоянием ИСПДн и состоянием, соответствующему специально составленному списку для проверки.

7.3. Обзоры безопасности должны включать:
• отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
• проверку содержимого файлов конфигурации на соответствие списка для проверки;
• обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
• проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
• проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
• проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).
7.4. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).
7.5. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо или изменить конфигурацию системы (для ликвидации условий проявления уязвимости), или установить программные коррекции, или установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.
7.6. Внесение изменений в системное программное обеспечение осуществляется ответственным лицом за выполнение мероприятий по обеспечению безопасности персональных данных в образовательной организации с обязательным уведомлением сотрудника, на рабочем месте которого производилось изменение, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.
7.7. Ответственность за организацию планирования и проверок информационной безопасности ИСПДн несет ответственное лицо за выполнение мероприятий по обеспечению безопасности персональных данных в образовательной организации.

Приложение №5
к Приказу ГБУ КО ПОО «КИТиС»
от 21.05 2015 года № 192

Инструкция
о порядке организации учета, хранения и выдачи машинных носителей персональных данных информационных систем персональных данных

1. Общие положения

1.1. Настоящая инструкция устанавливает организацию учета, хранения и выдачи машинных носителей персональных данных в информационных системах персональных данных **государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»** (далее – образовательная организация).

2. Организация учета машинных носителей персональных данных

2.1. Учет, хранение и выдачу машинных носителей персональных данных в образовательной организации осуществляет ответственный за выполнение мероприятий по обеспечению безопасности персональных данных либо сотрудники структурных подразделений, на которых возложены функции учета, хранения и выдачи носителей персональных данных:

• данные сотрудники несут персональную ответственность за сохранность персональных данных;

• при увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов, который утверждается директором ГБУ КО ПОО «КИТиС».

2.2. Все находящиеся на хранении и в обращении машинные носители персональных данных (далее – носители) подлежат учету. Учет всех видов и типов носителей производится в Журнале учета съемных электронных носителей персональных данных.

2.3. Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемную часть носителя персональных данных наносятся:

• учетный номер;
• отметка «Персональные данные»;
• дата регистрации (день, месяц, год);
• ФИО, должность, подпись сотрудника, выполнившего учет.

3. Организация выдачи машинных носителей персональных данных.

3.1. Пользователи (сотрудники) получают учтенный съемный носитель от ответственного лица за выполнение мероприятий по обеспечению

безопасности персональных данных в ГБУ КО ПОО «КИТиС» на конкретный срок. При получении делаются соответствующие записи в Журнале учета съемных электронных носителей персональных данных.

3.2. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета съемных электронных носителей персональных данных.

4. Организация хранения машинных носителей персональных данных

4.1. Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение конфиденциальной информации, а также хищение носителей. Носители должны храниться в служебных помещениях, в сейфе – установленным порядком. Запрещается хранить машинные носители персональных данных вместе с носителями открытой информации на рабочих столах либо оставлять их без присмотра, или передавать на хранение другим лицам.

4.2. Действия при утрате или уничтожении съемных носителей персональных данных:

• в случае утраты носителей, содержащих персональные данные либо разглашения, содержащихся в них сведений, немедленно поставить в известность ответственного за обеспечение безопасности персональных данных соответствующие отметки вносятся в Журнал учета съемных электронных носителей персональных данных.

4.3. Носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение носителей осуществляется комиссией ГБУ КО ПОО «КИТиС». По результатам уничтожения носителей составляется Акт уничтожения съемных электронных носителей персональных данных.

4.4. При передаче средств вычислительной техники ГБУ КО ПОО «КИТиС» сторонним организациям для проведения ремонтно-восстановительных или иных работ несъемные машинные носители изымаются из состава средств вычислительной техники.

5. Заключительные положения

5.1. Ответственность за выполнение правил эксплуатации машинных носителей персональных данных при выполнении непосредственных работ с носителями несет пользователь информационных систем персональных данных образовательной организации.

5.2. Контроль выполнения пользователями установленных правил эксплуатации машинных носителей персональных данных осуществляют ответственный за эксплуатацию объекта информатизации, ответственный за обеспечение безопасности персональных данных и администратор информационной безопасности в рамках своих должностных обязанностей.

5.3. Обязанность ознакомления пользователей с настоящей Инструкцией лежит на ответственном лице за выполнение мероприятий по обеспечению безопасности персональных данных в ГБУ КО ПОО «КИТиС».

Приложение №6
к Приказу ГБУ КО ПОО «КИТиС»
от 21.05. 2015 года № 192

Инструкция
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации определяет действия, связанные с функционированием информационных систем персональных данных **государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Колледж информационных технологий и строительства»** (далее – образовательная организация), меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем персональных данных.

1.2. Целью настоящей Инструкции является превентивная защита элементов информационных систем персональных данных (далее – ИСПДн) образовательной организации от предотвращения потери защищаемой информации.

1.3. Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех сотрудников (пользователей) образовательной организации, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций в том числе на:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Пересмотр настоящей Инструкции осуществляется по мере необходимости, но не реже 1 (одного) раза в 2 (два) года.

1.6. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается администратор информационной безопасности, назначенный приказом по ГБУ КО ПОО «КИТиС».

2. Порядок реагирования на инцидент

2.1. В настоящей Инструкции под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

Технические меры

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

• системы жизнеобеспечения;
• системы обеспечения отказоустойчивости;
• системы резервного копирования и хранения данных;
• системы контроля физического доступа.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

• пожарные сигнализации и системы пожаротушения;
• системы вентиляции и кондиционирования;
• системы резервного питания.

3.1.3. Все помещения образовательной организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации, а при необходимости и охранной сигнализации.

3.1.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

3.1.6. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

• локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
• источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

• резервные линии электропитания в пределах комплекса зданий;
• аварийные электрогенераторы.
Системы обеспечения отказоустойчивости;
• кластеризация;
технология RAID.
3.1.7. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации:
• для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров;
• для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.
3.1.8. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (флэш-карту, диск, жесткий диск и т.п.).

3. Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:
• для обрабатываемых персональных данных – не реже 1 (одного) раза в неделю;
• для технологической информации – не реже 1 (одного) раза в месяц;
• эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже 1 (одного) раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4. Учет, регистрация и выдача резервных копий

4.1. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования. Для учета процесса создания резервных копий информации ведется «Журнал учета резервных копий конфиденциальной информации».
4.2. «Журналу учета резервных копий конфиденциальной информации» присваивается номер, согласно номенклатуре, утвержденной директором ГБУ КО ПОО «КИТиС». Страницы журнала нумеруются, скрепляются печатью ГБУ КО ПОО «КИТиС».
4.3. Все резервные копии конфиденциальной информации записываются на учтенные и зарегистрированные в «Журнале учета съемных электронных носителей персональных данных» носители.
4.4. Сотрудник образовательной организации, ответственный за создание резервных копий конфиденциальной информации, после изготовления резервной копии обязан:
зарегистрировать сделанную копию информации в

«Журнале учета резервных копий информации» с указанием номера сменного носителя;

• резервную копию с отметкой о сдаче в «Журнале учета резервных копий конфиденциальной информации» хранить в сейфе;

• при создании резервной копии информации с использованием программ архивирования и шифрования данных, применяемых при этой процедуре, пароль должен быть записан в запечатанном конверте и храниться в сейфе.

4.5. Носители должны храниться в несгораемом шкафу (сейфе).

4.6. Носители должны храниться не менее 1 (одного) года, для возможности восстановления данных.

5. Ответственные лица

5.1. Ответственность за резервирование конфиденциальной информации и ведение «Журнала учета резервных копий конфиденциальной информации» возлагается на администраторов информационной безопасности ИСПДн.

5.2. Ответственность за ведение «Журнала учета съемных электронных носителей персональных данных» возлагается на администратора информационной безопасности (далее – Администратор ИБ), назначенного приказом директора ГБУ КО ПОО «КИТиС».

5.3. Контроль соблюдения правильности политики резервирования данных и учета носителей информации, предназначенных для создания резервных копий конфиденциальной информации, возлагается на Администратора ИБ образовательной организации.

5.4. Ответственность за ввод в действие, установку и обновление необходимого программно-аппаратного обеспечения технологии резервирования данных возлагается на Администратора ИБ образовательной организации.

5.5. Ответственность за своевременное уничтожение пришедших в негодность носителей резервных копий несут сотрудник отдела, ответственный за резервирование информации и Администратор ИБ.

6. Правила работы и обязанности должностных лиц по процедуре резервирования конфиденциальной информации, ее хранению и уничтожению

6.1. Носители, предназначенные для хранения копий, пришедших в негодность, снимаются с эксплуатации путем физического разрушения (разлома или разрезания). Уничтожение информации производится администратором информационной безопасности в присутствии сотрудника отдела, ответственного за резервное копирование конфиденциальной информации, о чем производится соответствующая запись в «Журнале учета съемных электронных носителей персональных данных» за подписями:

• администратора информационной безопасности;

• ответственного за резервное копирование конфиденциальной информации в структурном подразделении образовательной организации.

6.2. Все факты разрушения данных на рабочих местах, с использованием средств вычислительной техники, классифицируются как «значимые

нарушения информационной безопасности» и должны анализироваться через процедуру служебного расследования.

6.3. Категорически **ЗАПРЕЩАЕТСЯ:**

• копирование и обработка любой информации, переносимой с помощью сменных носителей без служебной необходимости;

• производить резервное копирование информации на неучтенные носители.

7. Требования к оборудованию помещений для хранения резервных копий

7.1. Помещение должно оборудоваться сейфом или металлическим хранилищем, имеющим резервные ключи и устройства для опечатывания.

7.2. Должностное лицо, осуществляющее хранение резервных копий, должно иметь печать для опечатывания сейфа или металлического хранилища.

8. Заключительные положения

8.1. Сотрудники (пользователи) образовательной организации, ответственные за создание резервных копий конфиденциальной информации должны ознакомиться с настоящей Инструкцией.

8.2. Обязанность ознакомления сотрудников с настоящей Инструкцией лежит на ответственном лице за выполнение мероприятий по обеспечению безопасности персональных данных в ГБУ КО ПОО «КИТиС».

Приложение №7
к Приказу ГБУ КО ПОО «КИТиС»
от 21.05. 2015 года № 198

ЖУРНАЛ
учета обращений граждан (субъектов персональных данных) о выполнении их законных прав в области защиты персональных данных

№п/п	Дата обращения	Ф.И.О. заявителя	Должность заявителя или наименование организации запрашивающих документы	Домашний адрес (или адрес организации) заявителя	Цель ознакомления с запрашиваемыми документами	Роспись заявителя в ознакомлении или получении	Приложение
1	2	3	4	5	6	7	8