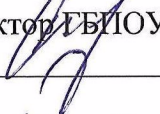
	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ		
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ		
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»		
	Версия 1	Изменения 0	Экземпляр 1
			Стр. 1 из 12

**ПРИНЯТО**

На Педагогическом совете  
ГБПОУ «БРИТ»  
протокол № 3  
« 27 » мая 2021 г.

**УТВЕРЖДАЮ**

Директор ГБПОУ «БРИТ»  
  
Ю.Ф. Сындыева  
Пр. № 43 от « 27 » мая 2021 г.

**СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА**

**ПОЛОЖЕНИЕ  
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ  
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО  
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ  
«БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»**

г. Улан-Удэ  
2021 г.

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ		
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ		
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»		
Версия 1	Изменения 0	Экземпляр 1	Стр. 2 из 12

## 1 Наименование

В целях обеспечения правильной классификации документации для включения в Перечень нормативной документации Техникума принято следующее наименование данного документа: Положение о защите персональных данных в системах персональных данных государственного бюджетного профессионального образовательного учреждения «Бурятский республиканский индустриальный техникум» (далее по тексту Положение).

Документ вводится в действие с момента утверждения.

## 2 Область применения

Настоящее Положение разработано в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных ГБПОУ «БРИТ». Данное Положение используется в организации работы библиотеки в Техникуме.

## 3 Нормативные ссылки

Настоящее Положение в соответствии с нормативными документами:

- Закон Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных»;
- Методические рекомендации ФСТЭК России и ФСБ России;
- Устав ГБПОУ «БРИТ».

## 4 Обозначения и сокращения

В настоящем документе использованы следующие сокращения:

**ПДн** - персональных данных;

**ИСПДн** - информационных системах персональных данных

**ГБПОУ «БРИТ»** - государственное бюджетное профессиональное образовательное учреждение «Бурятский республиканский индустриальный техникум»;

## 5 Общие положения

5.1 Положение определяет:

5.1.1 порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке;

5.1.2 порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений;

5.1.3 порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке;

5.1.4 порядок обучения персонала практике работы в ИСПДн;

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 3 из 12

5.1.5 порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией;

5.1.6 правила обновления общесистемного и прикладного программного обеспечения;

5.1.7 правила организации антивирусной защиты и парольной защиты ИСПДн;

5.1.8 порядок охраны и допуска посторонних лиц в защищаемые помещения.

5.2 Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих персональные данные. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

## **6 Порядок предоставления допуска пользователей к работе в ИСПДн**

6.1 Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается руководителем образовательного учреждения (далее Руководитель). В приказе определяется список сотрудников, допущенных к работе в ИСПДн;

6.2 С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн руководителем назначается администратор безопасности;

6.3 С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИСПДн.

6.4 Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

6.5 Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя запрещено.

## **7 Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн**

7.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн;

7.2 Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн;

7.3 Перед началом работы в ИСПДн, сотрудники учреждения, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных (Приложение 1);

7.4 Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю;

7.5 Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтенные в Журнале учета носителей персональных данных. Ответственным за ведение Журнала учета является администратор безопасности;

7.6 При работе со съемными машинными носителями информации пользователь каждый раз

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	<i>Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»</i>			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 4 из 12

перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения;

7.7 Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

7.7.1 строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

7.7.2 знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

7.7.3 хранить в тайне свой пароль (пароли);

7.7.4 хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;

7.7.5 выполнять требования антивирусной защиты в полном объеме.

7.8 Немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

7.8.1 фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;

7.8.2 несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;

7.8.3 некорректного функционирования установленных на компьютеры технических средств защиты;

7.8.4 непредусмотренных отводов кабелей и подключенных устройств.

7.9 **Пользователю категорически запрещается:**

7.9.1 использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

7.9.2 самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

7.9.3 осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

7.9.4 записывать и хранить ПДн на неучтенных машинных носителях информации;

7.9.5 оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

7.9.6 оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;

7.9.7 умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;

7.9.8 размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 5 из 12

## **8 Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации**

8.1 Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители.

8.2 Администратор информационной системы обязан осуществлять периодическое резервное копирование персональных данных.

8.3 При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов.

8.4 При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

8.5 При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

8.6 Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора информационной системы.

## **9 Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных**

9.1 Перед началом работы в ИСПДн пользователи должны ознакомиться с требованиями настоящего Положения под роспись;

9.2 Пользователи должны продемонстрировать администратору безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения;

9.3 Ответственным за организацию обучения и оказание методической помощи в учреждении является администратор безопасности.

## **10 Правила антивирусной защиты**

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

10.1 К использованию на компьютерах допускаются только лицензионные антивирусные средства;

10.2 Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором информационной системы;

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 6 из 12

10.3 Администратор информационной системы осуществляет периодическое обновление антивирусных средств и контроль их работоспособности;

10.4 Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы;

10.5 Ежедневно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров;

10.6 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель);

10.7 Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль;

10.8 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн;

10.9 На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации;

10.10 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором информационной системы) должен провести внеочередной антивирусный контроль компьютера.

10.11 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

10.11.1 приостановить обработку данных в ИСПДн;

10.11.2 немедленно поставить в известность о факте обнаружения зараженных вирусом файлов информационной системы, а также смежные подразделения, использующие эти файлы в работе;

10.11.3 совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

10.11.4 провести лечение или уничтожение зараженных файлов.

10.12 Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора информационной системы;

10.13 Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора информационной системы и всех пользователей данной ИСПДн.

## 11 Правила парольной защиты

Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

11.1 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора информационной системы;

11.2 При доступе пользователя в систему должна осуществляться идентификация и проверка

	<b>МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ</b>			
	<b>ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ</b>			
СМК ПЛ 03-02/1-2021	<i>Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»</i>			
	<b>Версия 1</b>	<b>Изменения 0</b>	<b>Экземпляр 1</b>	<b>Стр. 7 из 12</b>

подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов;

11.3 Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

11.3.1 пароль должен быть длиной не менее шести буквенно-цифровых символов;

11.3.2 символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

11.3.3 пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

11.3.4 при смене пароля новое значение должно отличаться от предыдущих;

11.3.5 пользователь не имеет права сообщать личный пароль другим лицам;

11.4 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 365 дней;

11.5 Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании указания руководителя или начальника отдела кадров.

11.6 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Учреждения и другие обстоятельства) администратора безопасности.

11.7 В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля.

11.8 Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

## **12 Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн**

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

12.1 Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется администратору информационной системы.

12.2 Право внесения изменений в конфигурацию аппаратно-программных средств защиты информации предоставляется администратору информационной системы.

12.3 Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора информационной системы запрещено.

12.4 Заявку на внесение изменений в конфигурацию аппаратно-программных средств защищенных рабочих мест ИСПДн, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

12.5 После чего заявка передается администратору информационной системы для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке.

12.6 Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	<i>Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»</i>			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 8 из 12

подсистем.

12.7 Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).

12.8 Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

12.9 При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор информационной системы обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

### **13 Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления.**

13.1 Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

13.2 Основными задачами контроля являются:

13.2.1 проверка организации выполнения мероприятий по защите информации в учреждении, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

13.2.2 выявление демаскирующих признаков объектов ИСПДн;

13.2.3 уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

13.2.4 проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

13.2.5 проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

13.2.6 проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

13.2.7 проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;


13.2.8 оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

13.2.9 разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

### **14 Порядок охраны и допуска посторонних лиц в помещения ИСПДн**

14.1 В учреждении должна быть предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного



	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 9 из 12

проникновения в помещения и хранилище носителей информации;

14.2 В помещениях должна быть установлена пожарная сигнализация;

14.3 Серверное и коммутационное оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора безопасности;

14.4 Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях;

14.5 При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, убираются для хранения в запираемый ящик стола или сейф;

14.6 При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и(или) ответственному за защиту информации;

14.7 При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или руководителю, или администратору безопасности.

## 15 Корректирующие действия по внесению изменений и дополнений в НД

По мере внесения изменений и дополнений в Федеральный Закон от 27 июля 2006 года №152-ФЗ «О персональных данных», Методические рекомендации ФСТЭК России и ФСБ России, Устав ГБПОУ «БРИТ» в настоящий документ необходимо вносить дополнения и изменения.

Разработчик(и): юрист



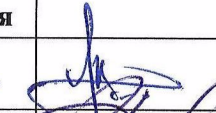
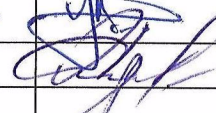
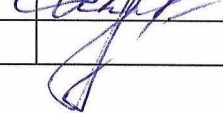
Баторов Д.О.


Проверил: Специалист управления процессами



Назарова Н.В.

## 16 ЛИСТ СОГЛАСОВАНИЯ

№	Должность	ФИО	Дата согласования	Подпись
	1-й заместитель директора	Нехуров А.Л.	27.05.21	
	Заместитель директора по ПР	Алонова О.С.	/	
	Заместитель директора по ВР	Аникьева М.В.		

	<b>МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ</b>		
	<b>ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ</b>		
СМК ПЛ 03-02/1-2021	<i>Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»</i>		
	Версия 1	Изменения 0	Экземпляр 1
			Стр. 10 из 12

**17 Лист внесения изменений и дополнений в НД**

Номер измене- ния	Номера листов			Основани е для внесения измени й	Подпись	Расшифровка подписи	Дата введени я измени я
	замене нных	новых	аннули рованы х				

	МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ			
	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ			
СМК ПЛ 03-02/1-2021	Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 11 из 12

## Приложение А

Обязательство о неразглашении информации,  
содержащей персональные данные

### ОБЯЗАТЕЛЬСТВО о неразглашении информации, содержащей персональные данные

Я, \_\_\_\_\_,  
(ФИО сотрудника)  
исполняющий(ая) должностные обязанности по замещаемой должности \_\_\_\_\_

(должность, наименование структурного подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей мне будет предоставлен доступ к персональным данным, обрабатываемым в ГБПОУ «Бурятский республиканский индустриальный техникум».

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.


5. В течение года после прекращения права на доступ к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_  
(ФИО сотрудника)

\_\_\_\_\_  
(подпись)

« \_\_\_\_ » \_\_\_\_\_ 202\_\_ г.

	<b>МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ</b>			
	<b>ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ</b>			
СМК ПЛ 03-02/1-2021	<i>Положение о защите персональных данных в системах персональных данных ГБПОУ «БРИТ»</i>			
	Версия 1	Изменения 0	Экземпляр 1	Стр. 12 из 12

## ЛИСТ ОЗНАКОМЛЕНИЯ

№	ФИО	Должность	Дата	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				
31.				
32.				
33.				
34.				
35.				
36.				
37.				
38.				
39.				
40.				
41.				