МИНИСТЕРСТВО ТУРИЗМА РЕСПУБЛИКИ БУРЯТИЯ
БУРЯАД УЛАСАЙ АЯНШАЛГЫН ЯАМАН

ПРИКАЗ

«16» мая 2025 года № 85

г. Улан-Удэ

О внесении изменений в приказ Министерства туризма Республики Бурятия от 18.03.2020 № 21 «О мерах, направленных на реализацию постановления Правительства Российской Федерации от 21.03.2012 № 211»

В целях приведения нормативного правового акта Министерства туризма Республики Бурятия в соответствие с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и соблюдения требований нормативных правовых актов в сфере информационных технологий **п р и к а з ы в а ю:**

1. Внести в приказ Министерства туризма Республики Бурятия от 18.03.2020 № 21 «О мерах, направленных на реализацию постановления Правительства Российской Федерации от 21.03.2012 № 211» (зарегистрирован в реестре нормативных правовых актов исполнительных органов государственной власти Республики Бурятия 08.04.2020 № 032020138) следующие изменения:

1.1. Дополнить пунктом 1.16 следующего содержания:

«1.16. Регламент осуществления мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак и по реагированию на компьютерные инциденты в Министерстве туризма Республики Бурятия согласно приложению 16 к настоящему приказу.».

1.2. В пунктах 2, 3 слова «кадровой работы, организационного, правового и финансового обеспечения» заменить словами «финансового и правового обеспечения».

1.3. В приложении № 3:

1.3.1. Абзац второй пункта 4 изложить в следующей редакции:

«Должностным лицом, ответственным за организацию обработки персональных данных в Министерстве, является консультант отдела финансового и правового обеспечения.».

1.3.2. Абзац второй пункта 6 исключить.

1.4. Приложение № 5 дополнить строкой 6 следующего содержания:

6.	Информационная система «Официальный сайт Республики Бурятия в сфере туризма «Байкал-Бурятия: туризм и отдых»

1.5. В приложении № 6:

1.5.1. Наименование изложить в следующей редакции:

«Перечень персональных данных, обрабатываемых в Министерстве туризма Республики Бурятия в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственной услуги и осуществлением государственной функции».

1.5.2. В пункте 1 после слов «трудовых отношений,» дополнить словами «а также в связи с оказанием государственной услуги и осуществлением государственной функций,».

1.6. Приложение № 7 изложить в новой редакции согласно приложению № 1 к настоящему приказу.

1.7. Приложение № 8 изложить в новой редакции согласно приложению № 2 к настоящему приказу.

1.8. В пункте 1 приложения № 9 слова «кадровой работы, организационного, правового и финансового обеспечения» заменить словами «финансового и правового обеспечения».

1.9. В пункте 11 приложения № 13 слова «начальником отдела кадровой работы, организационного, правового и финансового обеспечения» заменить словами «консультантом отдела финансового и правового обеспечения».

1.10. Приложение № 15 изложить в новой редакции согласно приложению № 3 к настоящему приказу.

1.11. Дополнить приложением № 16 согласно приложению № 4 к настоящему приказу.

2. Контроль за исполнением настоящего приказа возложить на начальника отдела финансового и правового обеспечения.

3. Настоящий приказ вступает в силу со дня его официального опубликования.

И. о. министра Б. Б. Цыдыпова

Исп. Манзаева Д. А., 21-07-57

Приложение № 1
к приказу Министерства туризма
Республики Бурятия
от «16» мая 2025 г. № 85

Приложение № 7
к приказу Министерства туризма
Республики Бурятия
от «18» марта 2020 г № 21

ПЕРЕЧЕНЬ
должностей государственных гражданских служащих Республики Бурятия в Министерстве туризма Республики Бурятия,
ответственных за проведение мероприятий по обезличиванию персональных данных, в случае обезличивания персональных данных

№ п/п	Наименование структурного подразделения Министерства туризма Республики Бурятия	Наименование должности
1.	Комитет стратегического управления развитием туризма	Заместитель председателя комитета - начальник отдела координации туристских проектов
2.	Отдел финансового и правового обеспечения	Консультант (юрист)
		Консультант (специалист по кадрам)
		Консультант (бухгалтер)
3.	Отдел управления развитием туризма	Консультант
4.	Сектора регионального контроля в сфере туристской индустрии	Консультант

Приложение № 2
к приказу Министерства туризма
Республики Бурятия
от «26» мая 2025 г. № 85

Приложение № 8
к приказу Министерства туризма
Республики Бурятия
от «18» марта 2020 г № 21

Перечень
должностей в Министерстве туризма Республики Бурятия, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1) Министр туризма Республики Бурятия;
2) Заместитель министра – председатель Комитета стратегического управления развитием туризма;
3) Заместитель министра – председатель Комитета продвижения туристского продукта и поддержки субъектов туристской индустрии;
4) Заместитель председателя комитета - начальник отдела координации туристских проектов;
5) Заместитель председателя комитета - начальник отдела поддержки субъектов туристской индустрии;
6) Начальник отдела финансового и правового обеспечения;
7) Начальник отдела управления развитием туризма;
8) Начальник отдела продвижения туристского продукта;
9) Консультант отдела финансового и правового обеспечения;
10) Консультант отдела координации туристских проектов;
11) Консультант отдела управления развитием туризма;
12) Консультант отдела поддержки субъектов туристской индустрии;
13) Консультант отдела продвижения туристского продукта;
14) Консультант сектора регионального контроля в сфере туристской индустрии;
15) Главный специалист отдела поддержки субъектов туристской индустрии;
16) Старший аналитик отдела финансового и правового обеспечения;
17) Старший аналитик отдела продвижения туристского продукта.

Приложение № 3
к приказу Министерства туризма
Республики Бурятия
от «16» мая 2025 г. № 85

Приложение № 15
к приказу Министерства туризма
Республики Бурятия
от «18» марта 2020 г № 21

СОСТАВ
комиссии в Министерстве туризма Республики Бурятия
по осуществлению внутреннего контроля
за обработкой персональных данных (далее – Комиссия)

Председатель Комиссии - Заместитель председателя комитета - начальник отдела координации туристских проектов;

Секретарь Комиссии - Консультант отдела финансового и правового обеспечения (специалист по закупкам);

Члены Комиссии:

Консультант отдела финансового и правового обеспечения (юрист);

Консультант отдела финансового и правового обеспечения (специалист по кадрам);

Консультант управления развитием туризма;

Консультант сектора регионального контроля в сфере туристской индустрии.

Приложение № 4
к приказу Министерства туризма
Республики Бурятия
от «16» мая 2025 № 85

Приложение № 16
к приказу Министерства туризма
Республики Бурятия
от «18» марта 2020 г. № 21

Регламент осуществления мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак и по реагированию на компьютерные инциденты в Министерстве туризма Республики Бурятия

1. Общие сведения

1.1. Настоящий Регламент разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет порядок действий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и по реагированию на компьютерные инциденты в Министерстве туризма Республики Бурятия (далее – Министерство).

1.2. В настоящем Регламенте используются следующие понятия:

Инцидент информационной безопасности - непредвиденное или нежелательное событие, которое может нарушить деятельность информационных систем или информационную безопасность;

Информационная безопасность – аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств её обработки;

Событие информационной безопасности – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

Конфиденциальность – свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц;

Целостность – неизменность информации в процессе ее передачи или хранения;

Доступность – свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц;

Информационное взаимодействие - процесс взаимодействия двух и более участников, целью которого является обработка информации в общих информационных системах и сетях;

Участники информационного взаимодействия - пользователи информационных систем (далее - пользователи) Министерства.

1.3. Действие положений настоящего Регламента распространяется на деятельность Министерства и обязательны к соблюдению всеми сотрудниками Министерства, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4. Источниками информации об инцидентах информационной безопасности в Министерстве являются:

факты, выявленные сотрудниками Министерства;

результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

обращения субъектов персональных данных с указанием инцидента информационной безопасности;

сообщения Федеральной службы технического и экспортного контроля России;

сообщения Федеральной службы безопасности Российской Федерации;

сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

иные источники информации.

1.5. Основными видами инцидентов информационной безопасности в Министерстве являются:

- нарушение конфиденциальности, целостности или доступности конфиденциальной информации, в том числе персональных данных;

- несанкционированный доступ к информационным ресурсам Министерства;

- превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников Министерства;

- отказ оборудования, сервисов, средств обработки и (или) защиты информации;

- несоблюдение требований внутренней организационно-распорядительной документации и действующего законодательства Российской Федерации в области защиты информации;

- вирусная атака или вирусное заражение;

- сетевые атаки.

К инцидентам информационной безопасности также относятся попытки и факты получения несанкционированного доступа к информационным системам персональных данных (ИСПДн):

- сеансы работы в ИСПДн незарегистрированных пользователей;

- сеансы работы Пользователей ИСПДн, срок действия полномочий которых истёк, либо в состав полномочий которых не входит обработка персональных данных;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учётной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учётной записи;

- совершение попыток несанкционированного доступа к АРМ, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

- несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты персональных данных.

1.6. В соответствии с частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в случае выявления инцидента Министерство обязано уведомить уполномоченный орган по защите прав субъектов персональных данных – Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

1.7. В соответствии с частью 12 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Министерство обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России), обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

2. Порядок реагирования на инциденты информационной безопасности

2.1. Последовательность действий работника в случае выявления инцидента информационной безопасности (ИБ):

- прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

- оповестить непосредственного руководителя о факте выявления инцидента ИБ;

- непосредственный руководитель работника должен оповестить ответственного за организацию обработки персональных данных о факте выявления инцидента ИБ;

- ответственный за организацию обработки персональных данных и администратор информационной безопасности (далее – администратор ИБ) собирают всю необходимую информацию для анализа инцидента ИБ.

2.2. Ответственный за организацию обработки персональных данных проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его наступлению, и составляет краткую справку, в которой описываются произошедший инцидент ИБ, его последствия (при наличии) и оценка необходимости проведения расследования инцидента ИБ, возможные меры для устранения последствий инцидента.

3. Порядок действий в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

3.1. В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов персональных данных, необходимо немедленно прекратить обработку персональных данных этих субъектов и по возможности блокировать доступ к этим данным до устранения причин, повлекших

наступление инцидента ИБ и его последствий. Решение о блокировании доступа к персональным данным принимает ответственный за организацию обработки персональных данных. Производится анализ ситуации и реализуются оперативные контрмеры, которые можно применить для локализации инцидента.

3.2. Ответственный за организацию обработки персональных данных в Учреждении уведомляет субъекта персональных данных об инциденте и принятых мерах блокирования доступа к его персональным данным.

3.3. Ответственный за организацию обработки персональных данных обязан уведомить Роскомнадзор в течение 24 (двадцати четырех) часов о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента.

Ответственное лицо должно подать уведомление о данном инциденте на сайте Роскомнадзора, пройдя верификацию через сервис ЕСИА.

3.4. Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ. Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Ответственный за организацию обработки персональных данных и администратор ИБ обеспечивают немедленное уничтожение персональных данных.

3.5. Ответственный за организацию обработки персональных данных оповещает субъекта персональных данных о прекращении обработки и уничтожении его персональных данных.

3.6. В порядке, определённом нормативными документами ФСБ России, необходимо обеспечить взаимодействие с ГосСОПКА и передать информацию об инцидентах ИБ, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, в Национальный координационный центр по компьютерным инцидентам (НКЦКИ). В случае возникновения инцидента в НКЦКИ должна быть направлена следующая информация:

- дата, время, место происшествия;
- наличие связи между инцидентом и компьютерной атакой;
- связь с другими происшествиями – при наличии;
- технические параметры компьютерного инцидента;
- последствия.

Передать информацию об инциденте возможно через техническое подключение к ГосСОПКА или путём отправки информации по E-mail, телефону, факсу на контакты НКЦКИ, указанные на их сайте http://cert.gov.ru.

Срок передачи информации об инциденте ИБ – 24 часа с момента происшествия.

4. Порядок расследования инцидента

4.1. Разбирательство и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;

- халатность и несоблюдение требований по обеспечению безопасности персональных данных;

- несоблюдение условий хранения носителей персональных данных;

- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

4.2. В случае установления неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, ответственный за организацию обработки персональных данных обязан уведомить Роскомнадзор в течение 72 (семидесяти двух) часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии). Ответственный за организацию обработки персональных данных должен подать уведомление о результатах внутреннего расследования на сайте Роскомнадзора (https://pd.rkn.gov.ru/incidents/), пройдя верификацию через сервис ЕСИА.

4.3. Проведение внутреннего расследования инцидента возлагается на комиссию по осуществлению внутреннего контроля за обработкой персональных данных.

4.4. Комиссия собирает и анализирует все данные об обстоятельствах инцидента (электронные письма, логи информационных систем, показания сотрудников и др.). Проверяются все собранные данные о том, что произошло, когда произошло, кто совершил неприемлемые действия, и как все это может быть предупреждено в будущем.

4.5. Комиссия обязана установить имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

4.6. По окончании внутреннего расследования комиссия представляет Министру заключение, в котором излагаются:

- основания и время проведения расследования;

- проделанная работа (кратко);

- время, место и обстоятельства факта нарушения;

- причины и условия совершения нарушения;

- виновные лица и степень их вины;

- наличие умысла в действиях виновных лиц;

- предложения по возмещению ущерба;

- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;

- рекомендации по исключению подобных нарушений;

- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т.д.).

К заключению прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;

- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.;

- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба (убытков).

Заключение должно быть подписано всеми членами комиссии. При несогласии с выводами или содержанием отдельных положений член комиссии, подписывая заключение, приобщает к нему своё особое мнение (в письменном виде). Заключение по результатам расследования подлежит утверждению Министром.

4.7. Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с заключением по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

5. Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение

5.1. Мероприятия, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе персональных данных;

- восстановление операционной системы рабочей станции, на которой произошел инцидент ИБ, на заводские настройки;

- своевременное удаление неиспользуемых учётных записей;

- контроль и мониторинг действий пользователей в информационной системе персональных данных;

- проведение обучения (повторного обучения) пользователей правилам обработки и защиты персональных данных;

- ознакомление пользователей с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм и правил обработки персональных данных, а также за разглашение полученных данных.

6. Пересмотр и внесение изменений в организационные документы по обеспечению безопасности информации

6.1. Пересмотр положений настоящего и иных локальных документов Министерства, касающихся вопросов обработки и обеспечения безопасности персональных данных, проводится в следующих случаях, если иное не установлено в пересматриваемых документах:

- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти Российской Федерации;

- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;

- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;

- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

6.2. Внесение изменений производится на основании соответствующего приказа Министра.

7. Контроль исполнения настоящего положения

7.1. Контроль надлежащего исполнения требований настоящего Положения осуществляется консультантом отдела финансового и правового обеспечения, ответственным за организацию обработки персональных данных.