АДМИНИСТРАЦИЯ ГУБЕРНАТОРА ЗАБАЙКАЛЬСКОГО КРАЯ

ПРИКАЗ

1 сентября 2012 года № 997

г. Чита

Об утверждении Положения о порядке организации и проведении работ по защите конфиденциальной информации в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности управления финансово-экономической и договорной работы Администрации Губернатора Забайкальского края»

В соответствии с пунктами 2, 6 части 1 и частью 2 статьи 18^1 Федерального закона «О персональных данных», пунктом 3.5. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30 августа 2002 года № 282, пунктом 3.2. Типовой программы аудита организации и состояния работы по защите конфиденциальной информации в исполнительных органах государственной власти Забайкальского края, рекомендованной решением Совета информационной безопасности Забайкальского края от 31 октября 2011 года № 1, **приказываю**:

1. Утвердить Положение о порядке организации и проведении работ по защите конфиденциальной информации в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности управления финансово-экономической и договорной работы Администрации Губернатора Забайкальского края».
2. В соответствии со статьей 655 Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденного приказом Министерства культуры Российской Федерации от 25 августа 2010 года № 558,установить срок хранения настоящего приказа «постоянно».
3. Руководителям структурных подразделений Администрации Губернатора Забайкальского края:

3.1. изучить лично и организовать изучение прилагаемого Положения подчиненными гражданскими служащими и работниками, допускаемыми в установленном порядке к работе с персональными данными как с конфиденциальной информацией;

3.2. довести до указанных в пункте 3.1. гражданских служащих и работников требования настоящего приказа и Положения под роспись в ведомости ознакомления;

3.3. взять под личный контроль исполнение подчиненными гражданскими служащими и работниками требований настоящего приказа и Положения.

4. Персональную ответственность за исполнение требований настоящего приказа и Положения возложить на:

4.1. руководителей структурных подразделений Администрации Губернатора Забайкальского края за организацию контроля выполнения требований настоящего приказа и прилагаемого Положения в вверенных им подразделениях;

4.2. гражданских служащих и работников Администрации Губернатора Забайкальского края, допущенных в установленном порядке к персональным данным как информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, за неисполнение требований настоящего приказа и прилагаемого Положения в части, их касающейся.

5. Возложить на заместителя руководителя Администрации Губернатора Забайкальского края – начальника управления организационной работы и развития местного самоуправления Губернатора Забайкальского края, ответственного за организацию обработки персональных данных в Администрации Губернатора Забайкальского края, общий контроль исполнения настоящего приказа и прилагаемого Положения.

6. Приказ довести до заинтересованных лиц под роспись в ведомости ознакомления.

Заместитель председателя Правительства
Забайкальского края – руководитель
Администрации Губернатора
Забайкальского края Г.П.Чупин

Приложение к приказу
Администрации Губернатора
Забайкальского края
от 16.10.2012 г. № 997

ПОЛОЖЕНИЕ

о порядке организации и проведении работ по защите конфиденциальной информации в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности управления финансово-экономической и договорной работы Администрации Губернатора Забайкальского края»

1. Термины и определения

1.1. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

1.2. **Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.3. **Администрация**- Администрация Губернатора Забайкальского края.

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

1.5. **Безопасность информации [данных]**- 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

1.6. **Доступность (санкционированная доступность) информации** - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

1.7. **Информационная система персональных данных (ИСПДн)**- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.8. **Несанкционированный доступ (несанкционированные действия) (НСД)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.9. **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.

1.10. **Объект защиты информации**- информация или носитель информации, или информационный процесс, которые необходимо защищать

в соответствии с целью защиты информации.

1.11. **Организационные меры защиты информации (оргмеры)**- под организационными мерами (оргмерами) понимаются организационные мероприятия по обеспечению физической защиты информации, предусматривающие установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты. Организационные меры по защите персональных данных включают в себя:
1. Разработку организационно – распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных;
2.Перечень мероприятий по защите персональных данных: определение круга лиц, допущенного к обработке персональных данных; организация доступа в помещения, где осуществляется обработка ПДн; разработка должностных инструкций по работе с персональными данными; установление персональной ответственности за нарушения правил обработки ПДн; определение продолжительности хранения ПДн и т.д.

1.12. **Оператор персональных данных (оператор ПДн)** - 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.

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

1.14. **Правовые меры защиты информации**- под правовыми мерами понимается защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. Т.к. Администрация Губернатора Забайкальского края не издает ни законов, ни иных нормативно- правовых актов в области защиты информации, то правовые методы защиты информации для данной Администрации заключаются в применении существующих законов и иных нормативных правовых актов, а также в контроле за их исполнением.

1.15. **СЗПДн** – система (подсистема) защиты персональных данных.

1.16. **Технические меры защиты информации**- под техническими мерами защиты информации в узком смысле слова понимается защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением

технических, программных и программно-технических средств. В широком смысле слова под техническими средствами защиты информации понимается защита информации как некриптографическими методами, так и методами преобразования при помощи шифрования.

1.17. **Целостность информации** - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1.18. **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

2. Цель и правовые основания

2.1. Настоящее Положение о порядке организации и проведении работ по защите конфиденциальной информации в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края» (далее - Положение) разработано в соответствии с:

– Федеральным законом от 27.07.2006 №149-ФЗ (ред. от 06.04.2011) "Об информации, информационных технологиях и о защите информации";

– Федеральным законом от 27.07.2006 № 152-ФЗ (в ред. от 25.07.2011) «О персональных данных»;

– Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;

– Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденным постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;

– Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденным приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456);

– приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», (зарегистрирован в Минюсте РФ 03.04.2008г. №1146);

– Базовой моделью угроз безопасности персональных данных при их

обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008;

– Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008;

– Типовой программой аудита организации и состояния работы по защите конфиденциальной информации в исполнительных органах государственной власти Забайкальского края, рекомендованной решением Совета информационной безопасности Забайкальского края от 31.10.2011 №1 и др.

2.2. В соответствии с ч.2. ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ (в ред. от 25.07.2011) «О персональных данных»Администрация Губернатора Забайкальского краяобязана опубликовать, разместить на официальном сайте или иным образом обеспечить неограниченный доступ к настоящему Положению.

3. Меры по обеспечению безопасности персональных данных при их обработке в ИСПДнАдминистрации Губернатора Забайкальского края

3.1. Общие положения:

3.1.1. Администрация Губернатора Забайкальского края при обработке персональных данных в ИСПДн принимает необходимые правовые, организационные и технические меры 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.

3.1.2. Обеспечение безопасности персональных данных при обработке в ИСПДн Администрации Губернатора Забайкальского краядостигается, в частности:

– определением угроз безопасности персональных данных при их обработке в ИСПДн Администрации;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн Администрации, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в ИСПДн Администрации Губернатора Забайкальского края, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн Администрации;

– контролем принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности ИСПДн Администрации Губернатора Забайкальского края.

3.1.3. В настоящем Положении под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3.1.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

3.1.5. Предпринимаемые правовые, организационные и технические меры направлены на защиту персональных данных при обработке в электронной форме на средствах автоматизации, при передаче по каналам связи или на отчуждаемых машинных носителях информации, а также при обработке персональных данных без средств автоматизации.

3.2. Правовые и организационные меры

3.2.1. Администрация Губернатора Забайкальского края осуществляет следующие правовые и организационные меры, направленные на защиту персональных данных в ИСПДнАдминистрации:

– ведет перечень персональных данных, обрабатываемых в ИСПДн«Информационная система отдела бухгалтерского учета и отчетности

Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– классифицирует ИСПДнАдминистрации;

– определяет угрозы безопасности персональных данных при их обработке в ИСПДн«Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края» и формирует на их основе модели угроз;

– разрабатывает на основе моделей угроз систему защиты персональных данных, обеспечивающую нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– разрабатывает внутренние организационно - распорядительные документы, доводит их до сведения гражданских служащих и работников под роспись, а также контролирует их исполнение;

– контролирует правильность функционирования и использования средств защиты информации, применяемых для защиты ПДн;

– контролирует неизменность состава программных и технических средств, определенных проектной документацией на систему защиты персональных данных;

– осуществляет контроль лиц, допущенных к работе с персональными данными;

– осуществляет контроль применяемых средств защиты информации и ведет их реестр;

– организует надежную охрану в нерабочее время средств защиты информации и средств вычислительной техники, на которыхобрабатываются персональные данные;

– проводит контроль состояния системы защиты персональных данных с установленными в проектной документации интервалами.

3.2.2. Комплекс внутренней организационно - распорядительной и технической документации в области защиты персональных данных включает в себя:

– Проект «Система защиты персональных данных информационных систем персональных данных Департамента управления делами Губернатора Забайкальского края». Том 4. Паспорт информационной системы персональных данных «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края». СЗПД-ДУДГЗК.ПС.03-ОР;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №991 «Об утверждении Политики информационной безопасности в Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №992 «Об утверждении Положения об ответственном за

организацию обработки персональных данных в Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №993 «Об утверждении Правил обработки персональных данных в Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №994 «Об утверждении Инструкции по конфиденциальному делопроизводству в Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 № 995 «Об утверждении Положения об архиве Администрации Губернатора Забайкальского края и Положения о Постоянно действующей экспертной комиссии Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №996 «Об утверждении сроков и мест хранения материальных носителей персональных данных»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №997 «Об утверждении Положения о порядке организации и проведении работ по защите конфиденциальной информации в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №998 «Об утверждении Положения о разрешительной системе допуска пользователей к ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №999 «Об утверждении Положения об администраторе безопасности информации»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1000 «Об утверждении Инструкции по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1001 «Об утверждении Инструкции пользователям по обеспечению правил информационной безопасности при работе в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1002 «Об утверждении Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации»;

– приказ Администрации Губернатора Забайкальского края от

16.10.2012 №1003 «Об утверждении Инструкции по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1004 «Об утверждении Регламента безопасного функционирования подсистемы криптографической защиты информации»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1005 «Об утверждении Инструкции по организации антивирусной защиты в ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1006 «Об утверждении Инструкции по организации парольной защиты ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1007 «Об утверждении Инструкции по обеспечению физической защиты помещений контролируемой зоны»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1008 «Об утверждении Плана внутренних проверок состояния защиты персональных данных»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1009 «Об утверждении Плана мероприятий по защите персональных данных»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1010 «Об утверждении Инструкции по внесению изменений в конфигурацию ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1011 «Об утверждении Инструкции о порядке действий в нештатных ситуациях»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1012 «Об утверждении Инструкции по резервному копированию информационных ресурсов ИСПДн «Информационная система отдела бухгалтерского учета и отчетности Управления финансово – экономической и договорной работы Администрации Губернатора Забайкальского края»;

– приказ Администрации Губернатора Забайкальского края от 16.10.2012 №1013 «О форме регистрации в Системе электронного документооборота «ДЕЛО» обращений субъектов персональных данных о соблюдении их законных прав».

3.2.3. Контроль исполнения требований организационно-

распорядительных и технических документов осуществляет ответственный за организацию обработки персональных данных.

3.3. Технические меры

3.3.1. Для обеспечения безопасности персональных данных в ИСПДн Администрация Губернатора Забайкальского края применяет следующие средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и определенные проектной документацией:

- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- средства обнаружения вторжений и анализа защищенности
- средства антивирусной защиты;
- криптографические средства.

3.3.2. Обслуживание средств защиты информации в ходе их эксплуатации возлагается на администратора безопасности информации.