АДМИНИСТРАЦИЯ ГУБЕРНАТОРА ЗАБАЙКАЛЬСКОГО КРАЯ

ПРИКАЗ

16 октября 2012 года ~ 991

г. Чита

Об утверждении Политики информационной безопасности в Администрации Губернатора Забайкальского края

Во исполнение пунктов 2, 4, 6 части 1 и части 2 статьи 18^1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», пункта 2 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, пункта 2.7 Типовой программы аудита организации и состояния работы по защите конфиденциальной информации в исполнительных органах государственной власти Забайкальского края, утвержденной решением Совета информационной безопасности Забайкальского края 31 октября 2011 года №1 **приказываю:**

1. Утвердить прилагаемую Политику информационной безопасности в Администрации Губернатора Забайкальского края (далее – Политика).
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 и Политики «постоянно».
3. Руководителям структурных подразделений Администрации Губернатора Забайкальского края:

3.1. изучить лично и организовать изучение прилагаемой Политики подчиненными государственными гражданскими служащими и работниками, допущенными в установленном порядке к работе с персональными данными

как с информацией, в отношении которой установлено требование об обеспечении ее конфиденциальности;

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

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

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

4.1. руководителей структурных подразделений Администрации Губернатора Забайкальского края за организацию контроля выполнения требований настоящего приказа и прилагаемой Политики в возглавляемых ими структурных подразделениях;

4.2. государственных 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 прилагаемой Политики в части, их касающейся.

5. Возложить на заместителя руководителя Администрации Губернатора Забайкальского края – начальника управления организационной работы и развития местного самоуправления Губернатора Забайкальского края, контроль за исполнением настоящего приказа и прилагаемой Политики.

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

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

УТВЕРЖДЕНА

приказом Администрации
Губернатора Забайкальского края
от 16.10.2012 года № 991

ПОЛИТИКА
информационной безопасности в 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. **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.

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

1.6. **Замысел защиты информации** – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

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. **Компьютерный вирус (КВ)** – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

1.9. **Криптографическое средство защиты информации** – а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении; б) средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы

криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации; в) средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи; г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций; д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации); е) ключевые документы (независимо от вида носителя ключевой информации).

1.10. **Межсетевой экран (МЭ) (средство межсетевого экранирования)** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС.

1.11. **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.

1.12. **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.

1.13. **Объект защиты информации** – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

1.14. **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.

1.15. **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.

1.16. **Ответственный за организацию обработки персональных данных** – должностное лицо оператора ПДн, осуществляющее:

– внутренний контроль за соблюдением государственными гражданскими служащими и работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доведение до сведения государственных гражданских служащих и работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов;

– контроль организации допуска государственных гражданских служащих и работников Администрации к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

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

1.18. **Политика безопасности (информации в организации)** – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

1.19. **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. Так

как Администрация не издает ни законов, ни иных нормативных правовых актов в области защиты информации, то правовые методы защиты информации для Администрации заключаются в применении существующих законов и иных нормативных правовых актов, а также в контроле за их исполнением.

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

1.21. **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.

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

1.23. **Цель защиты информации** – заранее намеченный результат защиты информации.

1.24. **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. Общие положения

2.1. Настоящая Политика информационной безопасности в Администрации Губернатора Забайкальского края (далее – Политика) определяет общую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется Администрация в своей деятельности.

2.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, при их обработке в Администрации, изложенных в Техническом задании и Техническом проекте на создание СЗПДн.

2.3. Политика разработана в соответствии с требованиями:

– Конституции Российской Федерации;

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

– Трудового кодекса Российской Федерации;

– Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности»;

– Указа Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

– Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № Пр-1895;

– постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

– постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– постановления Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации»;

– Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;

– Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 №58;

– Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-662;

– Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;

– ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;

– ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем;

– ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство;

– Положения об Администрации Губернатора Забайкальского края, утвержденного постановлением Правительства Забайкальского края от 16.02.2010 № 40, и иными правовыми актами Российской Федерации и Забайкальского края.

2.4. Целью настоящей Политики является определение основных правил обеспечения безопасности объектов защиты Администрации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизации ущерба от возможной реализации угроз безопасности ПДн.

2.5. Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления конкретных мероприятий по обеспечению безопасности персональных данных в Администрации.

2.6. 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.

2.7. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных.

2.8. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2.9. Состав объектов защиты представлен в техническом проекте на создание СЗПДн.

2.10. Состав ИСПДн подлежащих защите, представлен в паспорте ИСПДн и Правилах обработки персональных данных в Администрации Губернатора Забайкальского края.

2.11. В Политике определены общий замысел защиты информации Администрации, требования к пользователям ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности лиц, ответственных за обеспечение безопасности персональных данных в ИСПДн Администрации.

2.12. Требования Политики обязательны для всех государственных гражданских служащих и работников Администрации, представителей контрольно-надзорных органов, допущенных к защищаемой информации на

законных основаниях, а также индивидуальных лиц и работников иных организаций допущенных к защищаемой информации для проведения работ по гражданско-правовым договорам.

2.13. В соответствии с ч. 2. ст. 18^1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», п. 2 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211, Администрация обязана опубликовать, разместить на официальном сайте или иным образом обеспечить неограниченный доступ к настоящей Политике.

3. Система защиты персональных данных Администрации

3.1. Система защиты персональных данных (СЗПДн), строится на основании применения правовых, организационных и технических мер по обеспечению безопасности персональных данных.

3.2. Указанные в п. 3.1. настоящей Политики меры по обеспечению безопасности персональных данных регламентированы следующими внутренними организационно-распорядительными и инструктивно-технологическими документами Администрации:

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

– приказ Администрации от 16.10.2012 № 992 «Об утверждении Положения об ответственном за организацию обработки персональных данных в Администрации Губернатора Забайкальского края»;

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

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

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

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

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

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

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

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

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

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

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

3.3. В п. 2.3., п. 3.2. нормативных правовых и организационно-распорядительных документов определяется необходимый уровень защищенности ПДнИСПДн Администрации. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, сделано заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые технические мероприятия отражены в Техническом проекте и в Плане мероприятий по обеспечению защиты ПДн.

3.4. Для ИСПДн в разработанном Паспорте ИСПДн составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке персональных данных в ИСПДн.

3.5. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн включает следующие технические средства:

– антивирусные средства для рабочих станций пользователей и серверов;

– средства межсетевого экранирования;

– средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

3.6. Разработанная в Техническом проекте СЗПДн включает функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты:

– управление и разграничение доступа пользователей;

– регистрацию и учет действий с информацией;

– обеспечение целостности данных;

– обнаружение вторжений.

3.7. Список используемых технических средств отражается в Техническом проекте на создание СЗПДн. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Технический проект по согласованию с разработчиком.

3.8. В соответствии с реализуемыми функциями защиты СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

3.9. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в акте классификации информационной системы персональных данных.

3.10. Подсистемы СЗПДн, указанные в п. 3.8. настоящей Политики подробно разработаны для ИСПДн в Техническом проекте.

4. Пользователи ИСПДн

4.1. В Техническом проекте определены следующие категории пользователей ИСПДн:

- администратор ИСПДн;
- администратор безопасности информации;
- оператор.

4.2. В Паспортах каждой ИСПДн указанного Технического проекта разработаны матрицы доступа для каждого вида пользователей к ресурсам информационной системы.

4.3. Данные о группах пользователях, уровне их доступа и информированности отражены также в Положении о разрешительной системе допуска пользователей к ИСПДн.

4.4. Администратор ИСПДн:

4.4.1. Администратор ИСПДн – государственный гражданский служащий или работник Администрации, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора) к элементам, хранящим персональные данные.

4.4.2. Администратор ИСПДн обладает следующим уровнем доступа и знаний:

– обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

– обладает полной информацией о технических средствах и конфигурации ИСПДн;

– имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

– обладает правами конфигурирования и административной настройки технических средств ИСПДн.

4.5. Администратор безопасности информации:

4.5.1. Администратор безопасности информации – государственный гражданский служащий или работник Администрации, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

4.5.2. Администратор безопасности информации обладает следующим уровнем доступа и знаний:

– обладает правами администратора ИСПДн;

– обладает полной информацией об ИСПДн;

– имеет доступ к средствам защиты информации и протоколирования, а также к части ключевых элементов ИСПДн;

– не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

4.5.3. Администратор безопасности информации уполномочен:

– реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор) получает возможность работать с элементами ИСПДн;

– осуществлять аудит средств защиты;

– устанавливать доверительные отношения своей защищенной сети с сетями других органов власти и организаций.

4.6. Оператор:

4.6.1. Оператор – государственный гражданский служащий или работник Администрации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

4.6.2. Оператор обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

5. Требования к пользователям по обеспечению защиты персональных данных

5.1. Требования к государственным гражданским служащим и работникам Администрации, допущенным в установленном порядке к персональным данным, их права и обязанности установлены в:

– 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», утвержденной приказом Администрации Губернатора Забайкальского края от 16.10.2012 № 1001;

– Положении об администраторе безопасности информации, утвержденном приказом Администрации от 16.10.2012 №999;

– Инструкции по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности, утвержденной приказом Администрации от 16.10.2012 № 1000;

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

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

– Правилах обработки персональных данных в Администрации Губернатора Забайкальского края, утвержденных приказом Администрации от 16.10.2012 №993.

5.2. Все государственные гражданские служащие и работники Администрации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

5.3. До пользователей должны быть доведены под роспись в листе ознакомления требования нормативных правовых и внутренних организационно-распорядительных актов в области защиты информации, в части их касающейся.

5.4. Пользователи надлежащим образом должны быть извещены об ответственности за нарушение требований нормативных правовых и внутренних организационно-распорядительных актов в области защиты информации.

6. Лицо, ответственное за организацию обработки персональных данных

6.1. Заместитель председателя Правительства Забайкальского края – руководитель Администрации Губернатора Забайкальского края своим приказом назначает лицо, ответственное за организацию обработки персональных данных.

6.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от заместителя председателя Правительства Забайкальского края – руководителя Администрации Губернатора Забайкальского края и подотчетно ему.

6.3. Должностные лица Администрации обязаны предоставлять лицу, ответственному за организацию обработки персональных данных, следующие сведения:

– наименование, адрес 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 статьями 18^1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ «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.

6.4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

– осуществлять внутренний контроль за соблюдением государственными гражданскими служащими и работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доводить до сведения гражданских служащих и работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов;

– осуществлять контроль организации допуска гражданских служащих и работников Администрации Губернатора Забайкальского края к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

7. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства и подзаконных актов

7.1. Внутренний контроль 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 оператора в Администрации осуществляют:

– лицо, ответственное за организацию обработки персональных данных, назначаемое приказом Администрации;

– администратор безопасности информации, исполнение обязанностей которого дополнительно возложены на существующего штатного работника.

7.2. Внутренний контроль соответствия обработки персональных данных требованиям законодательства и подзаконных актов осуществляется в соответствии с планами, разработанными на отчетный период.

7.3. По результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства и подзаконных актов оператора лица, указанные в п. 7.1 настоящей Политики, докладывают заместителю председателя Правительства Забайкальского края – руководителю Администрации Губернатора Забайкальского края о выявленных нарушениях и принятых мерах.