



ФЕДЕРАЛЬНАЯ СЛУЖБА ИСПОЛНЕНИЯ НАКАЗАНИЙ

**УПРАВЛЕНИЕ ПО АСТРАХАНСКОЙ ОБЛАСТИ
(УФСИН РОССИИ ПО АСТРАХАНСКОЙ ОБЛАСТИ)**

П Р И К А З

Астрахань

А.А. Киктев

№ 50

**Об утверждении Политики
УФСИН России по Астраханской области в отношении обработки
и защиты персональных данных**

В соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», п р и к а з ы в а ю :

1. Утвердить прилагаемую Политику УФСИН России по Астраханской области в отношении обработки и защиты персональных данных (приложение).
2. Ответственность за организацию обработки персональных данных в ходе трудовых и иных непосредственно связанных с ними отношений, в которых УФСИН России по Астраханской области выступает в качестве работодателя, возложить на временно исполняющего обязанности заместителя начальника УФСИН России по Астраханской области майора внутренней службы Михайлюка М.Е.
3. Ответственность за организацию обработки персональных данных осужденных возложить на начальника оперативного отдела УФСИН России по Астраханской области полковника внутренней службы Вардакова С.Н.
4. Контроль за исполнением приказа оставляю за собой.

Начальник
подполковник внутренней службы

А.А. Киктев

ПОЛИТИКА
УФСИН России по Астраханской области в отношении обработки
и защиты персональных данных

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом УФСИН России по Астраханской области (далее - УФСИН), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является УФСИН.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в УФСИН, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных УФСИН как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

2. Основания обработки и состав персональных данных,
обрабатываемых в УФСИН

2.1. Обработка ПДн в УФСИН осуществляется в связи с выполнением возложенных на УФСИН функций, определяемых:

2.1.1. Уголовно-исполнительным Кодексом Российской Федерации от 08.01.1997 № 1-ФЗ;

2.1.2. Законом РФ от 21.07.1993 № 5473-1 «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы»;

2.1.3. Федеральным законом от 15.07.1995 № 103-ФЗ «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений»;

Кроме того, обработка ПДн в УФСИН осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых УФСИН выступает в качестве работодателя (Трудовой Кодекс РФ, Положение о службе в органах внутренних дел Российской Федерации, утвержденное Постановлением Верховного Совета Российской Федерации от 23.12.1992 № 4202-1), в связи с реализацией УФСИН своих прав и обязанностей как юридического лица.

2.2. В связи с реализацией своих прав и обязанностей, УФСИН обрабатываются ПДн физических лиц, являющихся контрагентами УФСИН по гражданско-правовым договорам, физических лиц, ПДн которых используются для осуществления пропускного режима в занимаемых УФСИН помещениях, а также граждан, письменно обращающихся в УФСИН по вопросам его деятельности.

2.3. ПДн получают и обрабатываются УФСИН на основании федеральных законов, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.4. УФСИН предоставляет обрабатываемые им ПДн государственным органам

и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.5. В УФСИН не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в УФСИН, в том числе при достижении целей их обработки или утраты необходимости

в достижении этих целей, обрабатывавшиеся УФСИН ПДн уничтожаются или обезличиваются.

2.6. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. УФСИН принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в УФСИН является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн УФСИН руководствуется следующими принципами:

3.2.1. законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

3.2.2. системность: обработка ПДн в УФСИН осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3.2.3. комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах УФСИН (далее - ИС) и других имеющихся в УФСИН систем и средств защиты;

3.2.4. непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

3.2.5. своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

3.2.6. преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в УФСИН с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

3.2.7. персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

3.2.8. минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

3.2.9. гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных УФСИН (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

3.2.10. открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн УФСИН (далее - СЗПДи)

не дают возможности преодоления имеющихся в УФСИН систем защиты возможными нарушителями безопасности ПДн;

3.2.11. научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

3.2.12. специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

3.2.13. эффективность процедур отбора кадров и выбора контрагентов: кадровая политика УФСИН предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах УФСИН до заключения договоров;

3.2.14. наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

3.2.15. непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в УФСИН ПДн имеют лица, уполномоченные на то в установленном порядке, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством функции УФСИН закрепляются за соответствующими структурными подразделениями УФСИН.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением УФСИН, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения» только для чтения и подготовки обобщенных материалов в части вопросов» касающихся структурного подразделения этих Работников.

4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями. Допущенные к обработке ПДн Работник под роспись знакомятся с документами УФСИН, устанавливающими порядок обработки ПДн.

4.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым УФСИН, осуществляется в соответствии с Законом о ПДн.

5. Реализация Политики

5.1. УФСИН принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в ходе трудовых и иных непосредственно связанных с ними отношений, в которых УФСИН России по Астраханской области выступает в качестве работодателя, несет заместитель начальника УФСИН, курирующий работу с кадрами.

Ответственность за организацию обработки ПДн осужденных несет начальник оперативного отдела УФСИН.

Ответственный за организацию обработки ПДн в УФСИН, в частности, обязан:

5.2.1. осуществлять внутренний контроль за соблюдением в УФСИН требований нормативных правовых актов и внутренних регулятивных документов УФСИН в области обработки и защиты ПДн;

5.2.2. доводить до сведения Работников положения нормативных правовых актов и внутренних регулятивных документов УФСИН в области обработки и защиты ПДн;

5.2.3. организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. УФСИН осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.4. При обработке ПДн без использования средств автоматизации УФСИН, в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн, реализует комплекс организационных и технических мер, обеспечивающих:

5.4.1. обособление ПДн от информации» не содержащей ПДн;

5.4.2. отдельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

5.4.3. соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;

5.4.4. соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения, занимаемые УФСИН, или в иных аналогичных целях;

5.4.5. сохранность материальных носителей ПДн;

5.4.6. условия хранения, исключая несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

5.4.7. надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. Обработка ПДн в УФСИН с использованием средств автоматизации ведется только в ИСПДн. В УФСИН запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.6. В целях обеспечения управления информационной безопасностью ПДн в УФСИН создается СЗПДн.

Объектами защиты СЗПДн являются информация, обрабатываемая УФСИН и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

5.7. СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

5.7.1. подготовку внутренних регулятивных документов УФСИН по вопросам обработки и защиты ПДн, контроль за исполнением в УФСИН требований нормативных правовых актов и внутренних регулятивных документов УФСИН в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

5.7.2. оформление письменных обязательств Работников о неразглашении ПДн;

5.7.3. доведение до сведения Работников информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

5.7.4. разработку и введение в действие внутренних регулятивных документов УФСИН по обеспечению информационной безопасности ИСПДн;

5.7.5. регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

5.7.6. ознакомление Работников с положениями нормативных правовых актов и внутренних регулятивных документов УФСИН в области обработки и защиты ПДн, а также обучение Работников правилам обработки и защиты ПДн;

5.7.7. проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

- физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;

- защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

- организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

- организацию необходимых мероприятий с Работниками, а также собеседование с лицами, претендующими на работу в УФСИН, изучение их биографии и проверку предоставляемых сведений; обучение Работников требованиям информационной безопасности;

- осуществление контроля эффективности организационных мер защиты;

5.8. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций ИСПДн разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в квартал проходят актуализацию. Работники проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нештатных ситуациях.

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПДн реализуются в УФСИН в следующих направлениях:

6.1.1. предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

6.1.2. предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

6.1.3. защита от вредоносных программ;

6.1.4. обеспечение безопасного межсетевого взаимодействия;

6.1.5. обеспечение безопасного доступа к сетям международного информационного обмена;

6.1.6. анализ защищенности ИСПДн;

6.1.7. обеспечение защиты информации с использованием шифровальных (криптографических) средств при передаче ПДн по каналам связи;

6.1.8. обнаружение вторжений и компьютерных атак;

6.1.9. осуществления контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

6.2.1. предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

6.2.2. ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

6.2.3. размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

6.2.4. организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

6.2.5. учет и хранение съемных носителей информации и их обращение, исключая хищение, подмену и уничтожение;

6.2.6. резервирование технических средств, дублирование массивов и носителей информации;

6.2.7. использование защищенных каналов связи, защита информации при ее передаче по каналам связи;

6.2.8. периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

6.3. С целью поддержания состояния защиты ПДн на надлежащем уровне в УФСИН осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.

Внутренний контроль включает:

- мониторинг состояния технических и программных средств» входящих в состав СЗПДн;

- контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн, требований договоров);

6.4. В целях осуществления внутреннего контроля в УФСИН проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в УФСИН.