This article examines the impact of isolation on human rights and its negative impact on the person convicted to prison. On the basis of analysis of Criminal and Penitentiary Code of the Republic of Kazakhstan the authors examine the opportunities for contact with the outside world convicted, substantiates the relative nature of imprisonment, identify opportunities convicted under existing national legislation for the implementation of their rights for the realization of human rights and on this basis makes proposals with regard to the possibility of the convict with the society.

Keywords: insulation, convicted, contact, date, holiday.

УДК 351.74

***В.Н. Лебедев**, кандидат технических наук, доцент, заместитель начальника кафедры информационных технологий управления органами внутренних дел Академии управления МВД Российской Федерации*
(e-mail: lvn-73@mail.ru)

СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ: ОСНОВНЫЕ ПОЛОЖЕНИЯ И ЭЛЕМЕНТЫ

Рассматриваются вопросы обеспечения безопасности персональных данных в органах внутренних дел РФ. Обеспечение требований законодательства Российской Федерации в области защиты персональных данных, обрабатываемых в информационных системах территориальных органов МВД, является актуальной, сложной и требующей решения задачей.

Ключевые слова: персональные данные, информационная система персональных данных, защита персональных данных, система защиты персональных данных, организация защиты персональных данных, носители информации, способы, техника и средства защиты персональных данных.

Полиция для выполнения возложенных на нее обязанностей имеет право обрабатывать необходимые данные о гражданах с последующим внесением полученной информации в банки данных в соответствии со ст. 17 федерального закона РФ от 7 февраля 2011 г. № 3-ФЗ «О полиции» [1].

Само понятие «данные о гражданах» не имеет законодательного закрепления, однако на основе положений ст. 24 Конституции РФ, федеральных законов РФ «О персональных данных» [2] и «Об информации, информационных технологиях и защите информации» [3] в данное понятие входит в первую очередь информация о частной жизни, личная и семейная тайны, персональные данные [4, 5].

Применительно к деятельности полиции понятие «данные о гражданах» полностью отождествляется с персональными данными (ПДн) граждан и представляются в качестве информации, неразрывно связанной с личностью ее обладателя и относящейся прямо или косвенно к определенному или определяемому физическому лицу (субъекту ПДн) [2].

Министерство внутренних дел Российской Федерации, являясь организующим и осуществляющим обработку ПДн [6] оператором, обязано принимать правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, а также от иных неправомерных действий в отношении данных сведений [2].

Федеральным законом «О персональных данных» закреплено, что перечень мер, направленных на выполнение обязанностей, связанных с обработкой ПДн государственными органами, устанавливает правительство РФ. При этом состав и содержание конкретных требований к защите персональных данных, организационных и технических мер по обеспечению безопасности при их обработке в информационных системах персональных данных (ИСПДн) устанавливается Федеральной службой безопасности Российской Федерации (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в пределах их полномочий.

Для обеспечения реализации требований законодательства РФ в области защиты ПДн при их обработке в ОВД необходимо совершенствование соответствующей системы защиты, т. е. системы защиты ПДн (СЗПДн), призванной обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн территориальных органов МВД России.

Система защиты ПДн в ОВД состоит:

из персональных данных и носителей таких данных;

должностных лиц, подразделений и сотрудников, ответственных за организацию и проведение работ по защите ПДн;

способов, техники и средств защиты ПДн;

мер и мероприятий, проводимых в целях защиты ПДн [6, 7].

В связи с актуальностью изучаемых вопросов перечисленные выше элементы системы требуют отдельного рассмотрения и краткого сопроводительного анализа каждого.

Персональные данные и носители таких данных.

Персональные данные (сведения о гражданах, подлежащие внесению в банки данных), обрабатываемые в ОВД, определены в ч. 3 ст. 17 федерального закона РФ «О полиции» [1]. Также в различных подраз-

делениях и службах ОВД (медицинские учреждения, кадровые, финансово-экономические, тыловые подразделения) обрабатываются ПДн сотрудников, федеральных государственных служащих, работников, стажеров системы МВД России, членов их семей и др. Кроме того, в ОВД обрабатываются ПДн, являющиеся государственной тайной [8]. Защита данной категории ПДн осуществляется в соответствии с нормами и правилами, установленными для сведений, составляющих государственную тайну.

В настоящее время в процессе обработки ПДн используются различные носители. Определение полного перечня носителей ПДн, применяемых в ОВД, является немаловажной задачей, так как именно вид используемого носителя информации во многом определяет угрозы ее безопасности и технические каналы утечки ПДн.

Основной материальный носитель для обработки ПДн в ИСПДн ОВД – магнитный: жесткий диск компьютера, сервера и т. п. Использование флэш-памяти в качестве носителя ПДн возможно после совместной аттестации данного носителя и автоматизированной системы. Для передачи информации ограниченного доступа в ОВД в качестве основного носителя служит оптический диск (CD-R, DVD-R). Это обусловлено фактом, что его использование требует применения только относительно «дешевых» режимных (организационных) мер. Использование электромагнитного излучения или электрических и оптических сигналов как носителя информации является крайне актуальным и необходимым, однако требует создания систем криптографической защиты и электронной подписи, т. е. применения специальных и дорогостоящих средств защиты информации. При этом следует учитывать, что использование в ОВД для обработки ПДн разнообразных носителей приводит к увеличению числа угроз и технических каналов утечки ПДн.

Должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн.

В соответствии с требованиями приказа МВД России [6] руководители (начальники) территориальных органов МВД, руководители структурных подразделений территориальных органов МВД, эксплуатирующие ИСПДн, обеспечивают выполнение правовых, организационных и технических мер, которые направлены на обеспечение безопасности ПДн, и являются ответственными за соблюдение требований по защите ПДн при их автоматизированной обработке в подчиненном органе внутренних дел.

Кроме того, ответственными за соблюдение требований по защите ПДн являются администраторы ИСПДн, пользователи, непосредственно обрабатывающие ПДн, инженерно-технический персонал, имеющий доступ к элементам ИСПДн.

Координацию и контроль деятельности по защите ПДн, содержащихся в информационных системах ОВД, осуществляет Департамент информационных технологий связи и защиты информации МВД России (ДИТСиЗИ МВД России), который выполняет функции головного подразделения МВД России по вопросам защиты ПДн при их автоматизированной обработке.

В территориальных органах МВД России функции защиты ПДн и контроля за проведением мероприятий по защите ПДн возложены на подразделение информационных технологий, связи и защиты информации или на должностных лиц, назначенных ответственными за проведение мероприятий по технической защите информации, а также сотрудников, назначенных ответственными за организацию обработки ПДн.

Таким образом, в территориальных органах МВД России за выполнение мероприятий по обеспечению безопасности ПДн отвечает руководитель (начальник) данного органа и руководитель структурного подразделения, осуществляющего обработку ПДн и (или) эксплуатацию ИСПДн.

Способы, методы, техника и средства защиты ПДн.

К способам и методам защиты персональных данных в ИСПДн ОВД относятся:

способы и методы защиты ПДн, обрабатываемой техническими средствами информационной системы, от несанкционированного доступа к ПДн;

способы и методы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к ПДн (методы и способы защиты информации от утечки по техническим каналам).

В целях защиты ПДн, обрабатываемых в ИСПДн, от несанкционированного доступа применяются средства управления и разграничения доступа пользователей к ПДн; обеспечения регистрации и учета действий с информацией; обеспечивающие целостность данных; антивирусной защиты; межсетевого экранирования; анализа защищенности; обнаружения вторжений; криптографической защиты ПДн.

В целях защиты ПДн, обрабатываемых в ИСПДн, от утечки по техническим каналам применяются генераторы активного акустического, виброакустического и электромагнитного маскирующего зашумления, сетевые помехоподавляющие и телефонные фильтры, а также методы экранирования и заземления и др.

Выбор средств защиты информации для построения системы защиты персональных данных осуществляется в соответствии с нормативными правовыми актами, принятыми ФСТЭК и ФСБ России на основе модели угроз и в зависимости от уровня защищенности ИСПДн.

Для обеспечения защиты ПДн, содержащихся в ИСПДн, применяются только средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации [9, 10].

Меры и мероприятия, проводимые в целях защиты ПДн.

Обязанностью оператора, обрабатывающего ПДн, является применение организационных мер по обеспечению безопасности ПДн. В настоящее время порядок организации защиты ПДн, содержащихся в ИСПДн ОВД, установлен приказами ФСТЭК и МВД России [6, 10].

Особое внимание необходимо обратить на то, что обработка ПДн в ИСПДн ОВД должна осуществляется только после завершения работ по созданию системы защиты ПДн и вводу в эксплуатацию ИСПДн. Ввод в эксплуатацию ИСПДн осуществляется на основе приказа руководителя (начальника) территориального органа внутренних дел после аттестации ИСПДн по требованиям защиты информации.

К основным *мероприятиям, направленным на обеспечение безопасности ПДн* при их автоматизированной обработке и создание системы защиты ПДн в территориальных органах МВД России, относятся следующие:

1. Направление уведомлений об обработке ПДн в ДИТСиЗИ МВД России (проведение данного мероприятия обусловлено требованиями федерального закона и приказа МВД России [2, 6]).

2. Получение территориальным органом МВД России на региональном уровне лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации (получение данной лицензии необходимо для проведения аттестации информационных систем, обрабатывающих ПДн, по требованиям защиты информации, а также мероприятий по их технической защите информации [11]; лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК России).

3. Создание комиссии для определения уровня защищенности ИСПДн (приказом руководителя (начальника) территориального органа МВД России создается комиссия, в состав которой включаются представители структурных подразделений, эксплуатирующих ИСПДн, а также специалисты подразделения (сотрудники) информационных технологий, связи и защиты информации).

4. Планирование мероприятий, направленных на защиту ПДн, обрабатываемых в информационных системах территориального органа МВД России.

5. Проведение мероприятий по обеспечению безопасности ПДн, обрабатываемых в информационных системах территориального органа МВД России.

К основным мероприятиям по обеспечению безопасности ПДн в ОВД относятся мероприятия, направленные на формирование требований к защите ПДн, содержащихся в ИСПДн, разработку и внедрение системы защиты ИСПДн, аттестацию информационной системы по требованиям защиты информации и ввод ее в действие, обеспечение защиты ПДн в ходе эксплуатации и при выводе из эксплуатации аттестованной ИСПДн. Состав и содержание указанных мероприятий определены приказом ФСТЭК России [10].

Наиболее технически сложным мероприятием является аттестация информационной системы на соответствие требованиям защиты информации. Аттестация ИСПДн проводится до начала обработки ПДн в данной информационной системе.

Проведение данного мероприятия, т. е. аттестации ИСПДн, включает три этапа.

Этап 1. Подготовка ИСПДн к аттестации на соответствие требованиям защиты информации:

предпроектное обследование ИСПДн, включающее определение: перечня обрабатываемых ПДн; условий расположения, конфигурации и топологии ИСПДн; перечня технических средств, систем и общесистемных и прикладных программных средств, предполагаемых к использованию в ИСПДн; режимов обработки ПДн и уровня защищенности ИСПДн;

разработка модели угроз безопасности ПДн при их обработке в ИСПДн и перечня актуальных угроз.

Этап 2. Разработка технического проекта на систему защиты ИСПДн.

Этап 3. Создание и аттестация ИСПДн по требованиям защиты информации:

приобретение сертифицированных технических, программных и программно-технических средств защиты информации;

установка и настройка, ввод в эксплуатацию средств защиты ПДн;

подготовка проекта приказа о допуске сотрудников к работам в ИСПДн;

оформление журналов учета эксплуатирующего персонала, администраторов защиты, администраторов, пользователей, непосредственно обрабатывающих ПДн в ИСПДн, и инженерно-технического персонала, имеющего доступ к ИСПДн; учет машинных носителей ПДн и учет их выдачи; проведение инструктажей по обеспечению безопасности ПДн, проверка исправности технических средств и технического обслуживания;

разработка инструкций сотрудникам, обрабатывающим ПДн, технического паспорта на ИСПДн, а также инструкций по эксплуатации средств защиты информации;

проверка соответствия организационно-технических мер защиты требованиям нормативно-методических и руководящих документов ФСБ и ФСТЭК России;

проведение специальных исследований и аттестации ИСПДн и выдача аттестата соответствия ИСПДн требованиям по безопасности информации;

проведение контроля состояния защиты информации в ИСПДн.

6. Организация взаимодействия подразделений, обеспечивающих создание и эксплуатацию ИСПДн, с подразделением по защите ПДн.

В настоящее время данный аспект является самым проблемным и сложным в проведении мероприятий по обеспечению безопасности ПДн в ОВД. В соответствии с положением об аттестации объектов информатизации по требованиям безопасности информации подготовку объекта к аттестации осуществляют подразделения, эксплуатирующее ИСПДн. В этих подразделениях отсутствуют специально подготовленные сотрудники для проведения работ по защите информации, которые могут квалифицированно организовать проведение подготовительных мероприятий.

7. Определение должностных обязанностей лиц, ответственных за организацию обработки ПДн и за эксплуатацию ИСПДн, с внесением соответствующих положений в должностные регламенты (инструкции) сотрудников.

8. Организация и осуществление контроля за выполнением установленных требований по обеспечению безопасности ПДн.

Целью такого контроля является соблюдение структурными подразделениями территориального органа МВД России требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

Ведомственный контроль по определению достаточности принятых мер по обеспечению безопасности ПДн проводится не реже одного раза в два года и осуществляется ДИСТиЗИ МВД России и подразделением информационных технологий, связи и защиты информации.

9. Планирование и организация проведения занятий по изучению требований нормативных правовых актов и методических документов по вопросам обеспечения безопасности ПДн, а также ежегодной проверки их знаний.

Изучение указанных требований с заинтересованными сотрудниками проводится в рамках служебной подготовки в течение года с обязательным приемом зачета на знание требований ФСТЭК и МВД России по защите ПДн.

В статье предпринята попытка системного рассмотрения процесса защиты персональных данных, которые обрабатываются в информационных системах органов внутренних дел Российской Федерации с целью дальнейшего совершенствования и развития данной системы.

1. О полиции : федер. закон Рос. Федерации, 7 февр. 2011 г., № 3-ФЗ : в ред. от 3 февр. 2014 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

2. О персональных данных : федер. закон Рос. Федерации, 27 июля 2006 г., № 152-ФЗ : в ред. от 23 июля 2013 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

3. Об информации, информационных технологиях и защите информации : федер. закон Рос. Федерации, 27 июля 2006 г., № 149-ФЗ : в ред. от 28 дек. 2013 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

4. Баглай, М.В. Конституционное право Российской Федерации / М.В. Баглай. М. : Норма, 2011. 768 с.

5. Зорькин, В.Д. Комментарий к Конституции Российской Федерации / В.Д. Зорькин. М. : Норма, 2011. 1008 с.

6. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации : приказ МВД России, 6 июля 2012 г., № 678 : в ред. от 15 июля 2013 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

7. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения : приказ Федер. агентства по техн. регулированию и метрологии Рос. Федерации, 27 дек. 2006 г., № 373-ст // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

8. Об утверждении Перечня сведений, отнесенных к государственной тайне : указ Президента Рос. Федерации, 30 нояб. 1995 г., № 1203 : в ред. от 26 сент. 2013 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

9. О техническом регулировании : федер. закон Рос. Федерации, 27 дек. 2002 г., № 184-ФЗ : в ред. от 28 дек. 2013 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

10. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ Федер. службы по техн. и экспорт. контролю России, 11 февр. 2013 г., № 17 // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

11. О лицензировании отдельных видов деятельности : федер. закон Рос. Федерации, 4 мая 2011 г., № 99-ФЗ : в ред. от 2 июля 2013 г. // КосультантПлюс : Версия Проф [Электронный ресурс] / ООО «ЮрСпектр». М., 2014.

Дата поступления в редакцию: 07.04.14

***V.N. Lebedev**, PhD of technical sciences, associate professor, deputy chief of the chair of information technologies of management of police of the Academy of Management of the MIA of the Russian Federation*

SYSTEM OF PROTECTION OF PERSONAL INFORMATION IN LAW-ENFORCEMENT BODIES OF THE RUSSIAN FEDERATION: BASIC PROVISIONS AND ELEMENTS

In article questions of safety of personal information are considered actual, now for law-enforcement bodies. It is connected, first of all, by that providing requirements of the legislation of the Russian Federation in the field of protection of personal information territorial bodies of the Ministry of Internal Affairs of Russia processed in information systems is the complex challenge demanding the decision now.

Keywords: personal information, information system of personal information, protection of personal information, system of protection of personal information, organization of protection of personal information, data carriers, ways, equipment and means of protection of personal information.