УДК 681.3.06(075)

А.С. Басан, О.Б. Макаревич

ВНЕДРЕНИЕ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РАМКАХ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ЮФУ В ОРГАНИЗАЦИЯХ ГОРОДА ТАГАНРОГА

Рассматривается организация инновационной деятельности Южно-Российского регионального центра по проблемам информационной безопасности ЮФУ (ЮР РУНЦ ИБ ЮФУ) в сфере внедрения систем защиты персональных данных в организациях и предприятиях во исполнение закона № 152-ФЗ «О персональных данных», а также проведения обучающих курсов и семинаров. Рассмотрены основные требования со стороны государственных регуляторов к организациям – операторам персональных данных, а также вопросы, возникающие в процессе создания систем защиты, а также способы их решения. Рассмотрена деятельность центра по переподготовке специалистов и повышению квалификации в области защиты конфиденциальной информации.

Защита персональных данных; закон № 152-ФЗ; конфиденциальная информация; персональные данные; технические средства защиты.

A.S. Basan, O.B. Makarevich

EXECUTION WORKS FOR THE IMPLEMENTATION OF THE PROTECTION OF PERSONAL DATA IN THE ORGANIZATIONS IN THE INNOVATION OF SRRCIS

The organization of innovative activities of the South Russian Regional Centre for Information Security SFEDU in the introduction of systems of personal data protection in organizations and enterprises, pursuant to Law № 152-FZ "On personal data" as well as holding training courses and seminars. The main requirement on the part of state regulators to organizations - operators of personal data, as well as issues arising in the process of establishing security systems, as well as their solutions. We consider the activities of the center for the retraining and further training in the protection of confidential information.

Protection of personal data, federal law number 152-FZ; confidential information, personal data; means of protection.

Вопросу защиты персональных данных (ПДн), обрабатываемых практически всеми организациями России, в настоящее время уделяется много внимания как на государственном уровне, так и на многочисленных практических семинарах и научных конференциях. Такой интерес к этой теме вызван необходимостью абсолютно всех организаций (операторы ПДн), бюджетных или коммерческих, обеспечивать адекватную защиту персональных данных, которые они обрабатывают. Требования к защите достаточно чётко изложены законодательными актами, нормативными и методическими документами ФСТЭК (Федеральная служба технического и экспортного контроля) и ФСБ (Федеральная служба безопасности). Несмотря на то, что требования к защите известны и доступны, грамотно выполнить их достаточно сложно – необходима квалификация в этой области знаний. Кроме того, создание системы защиты потребует значительных расходов на приобретение средств защиты. За нарушение законодательства в области персональных данных определены достаточно суровые меры наказания – от административной до уголовной ответственности. Типовыми случаями ответственности являются штрафы должностного лица, его увольнение, приостановление обработки персональ-

ных данных в организации, а также лишение лицензии на основной вид деятельности. Сложившаяся ситуация показывает реальную заинтересованность операторов ПДн в создании надежной системы защиты ПДн, удовлетворяющей актуальным требованиям законодательства.

Статус персональных данных в качестве конфиденциальной информации был определен Указом Президента РФ от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

Принятие Федерального Закона № 152-ФЗ «О персональных данных» явилось логическим следствием ратификации Российской Федерацией «Европейской конвенции о защите физических лиц при автоматизированной обработке персональных данных», которая состоялась 25 ноября 2005 г. С этого момента контроль за защитой персональных данных, как вида конфиденциальной информации, заметно усилился.

В первую очередь увеличилось количество контролирующих организаций, теперь регулировать обработку персональных данных на различных уровнях призваны 3 структуры:

1. РКН (Роскомнадзор), на который возложены функции по ведению реестра операторов, обработке уведомлений, ведению плановых и внеплановых проверок выполнения требований федеральных законов (организационные меры защиты ПДн). РКН уже провёл сотни проверок практически во всех субъектах РФ. Большая часть проверок оканчивалась предписаниями на устранение выявленных недостатков. Некоторые предписания были направлены в Прокуратуру РФ.

2. ФСБ, которая регулирует вопросы защиты персональных данных в части применения сертифицированных криптографических средств защиты информации (СКЗИ). Средства криптографической защиты информации должны применяться при передаче персональных данных по внешним каналам связи.

3. ФСТЭК, которая вырабатывает технические требования к системам защиты персональных данных, а также регламентирует процедуры оценки соответствия средств защиты информации (сертификация) и информационных систем (аттестация) требованиям руководящих документов.

Ст. 19 закона № 152-ФЗ обязала операторов персональных данных независимо от формы собственности принимать меры по защите персональных данных, в том числе с помощью технических средств защиты информации.

Методы и способы защиты информации с использованием сертифицированных средств защиты информации определяются приказом ФСТЭК от 05.02.10 г. № 58.

В соответствии с Постановлением Правительства Российской Федерации от 17.11.2007 г. № 781, средства защиты информации, применяемые в информационных системах, в установленном порядке должны пройти процедуру оценки соответствия, т.е. сертификацию.

В настоящее время, по разным объективным и субъективным причинам, срок действия закона № 152-ФЗ в части *разработанных ранее* ИСПДн перенесен сначала до 1 января 2011 г., а затем и до 1 июля 2011 г. (закон № 444277-5). Однако все разрабатываемые (модернизированные) с начала 2011 г. ИСПДн уже должны соответствовать закону.

Факт соответствия ИСПДн действующему законодательству устанавливается в специальном документе – «Аттестате соответствия», который выдается Заказчику по результатам комплекса специальных работ, проведенных Исполнителем, имеющим лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

Операторы персональных данных, не сумевшие выполнить требования ФЗ-152, с 1 июля 2011 года понесут соответствующую гражданскую, административную, дисциплинарную и уголовную ответственность.

Для решения актуальных задач и проблем в области защиты информации был создан Южно-Российский региональный учебно-научный центр по проблемам информационной безопасности в системе высшей школы ЮФУ (ЮР РУНЦ ИБ). Он основан приказом ректора ТРТУ от 17.07.98 г. № 257 во исполнение приказа Министерства общего и профессионального образования РФ от 20.08.97 г. № 1781. Центр является структурным подразделением Южного федерального университета. В своей основе он опирается на кафедру безопасности информационных технологий (БИТ) ТТИ ЮФУ, учебно-научный центр систем информационной безопасности кафедры БИТ и кафедры вузов региона Юга России.

Плотное взаимодействие ЮР РУНЦ ИБ с кафедрой БИТ позволяет объединять значительный штат квалифицированных инженеров в области защиты информации и научных работников.

ЮР РУНЦ ИБ имеет все необходимые лицензии ФСТЭК и ФСБ, которые необходимы для выполнения работ по защите персональных данных и конфиденциальной информации. В их число входят:

- лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации;
- лицензия ФСБ на распространение шифровальных (криптографических) средств;
- лицензия ФСБ на техническое обслуживание шифровальных (криптографических) средств.

В итоге выполняются следующие важные и взаимосвязанные задачи:

1. Выполнение работ по созданию систем защиты конфиденциальной информации и персональных данных.

2. Проведение обучающих курсов и семинаров по вопросам защиты информации.

3. Проведение научно-исследовательских и конструкторских работ в области защиты информации.

В рамках заданной темы статьи будут рассмотрены две первые задачи, как наиболее близкие к потребностям реальных организаций.

Начиная с конца 2009 г., когда проблема защиты персональных данных приобрела действительную актуальность, и у организаций возникала острая потребность в квалифицированных специалистах по безопасности, в ЮР РУНЦ ИБ стали проводиться обучающие семинары и курсы, посвященные этой решению этой проблемы.

Основываясь на лицензии Министерства образования (регистрационный № 0229, свидетельство о государственной аккредитации № 0680), были организованы курсы повышения квалификации специалистов по защите информации «Техническая защита конфиденциальной информации» (72 часа), а также семинарские занятия (8 часов) по теме «Защита персональных данных. Новое в законодательстве. Построение системы защиты».

Обучающимся на курсах повышения квалификации выдаются удостоверения государственного образца (рис. 1.)

РОССИЙСКАЯ ФЕДЕРАЦИЯ

УДОСТОВЕРЕНИЕ

О КРАТКОСРОЧНОМ ПОВЫШЕНИИ КВАЛИФИКАЦИИ

Настоящее удостоверение выдано

в том, что он(а) с „05" сентября 2011 г. по „13" сентября 2011 г.

прошел(а) краткосрочное обучение в (на) Южно-Российском региональном учебно-научном центре по проблемам информационной безопасности Южного федерального университета

по программе «Администрирование информационно-вычислительных сетей»

в объеме 72 часа.

Ректор (директор)

Секретарь

Город Таганрог год 2011

Рис. 1. Пример выдаваемых удостоверений государственного образца

Таблица 1

Виды организаций	Место проведения занятий	Число слушателей
Интеграторы программного обеспечения и средств защиты информации (ООО «Орбита», г. Таганрог, ООО «Орбита», г. Краснодар, ООО «СандСофт-Новороссийск» и другие)	г. Таганрог	50
Медицинские учреждения г. Таганрога	г. Таганрог	2
Образовательные учреждения (Дагестанский государственный институт народного хозяйства при Правительстве Республики Дагестан», Невинномысский государственный гуманитарно-технический институт)	г. Таганрог	8
Пенсионный фонд РФ, г. Москва	г. Таганрог	40
Предприятия Росрезерва	г. Таганрог	3
Филиал «Аэронавигация Юга» ФГУП «Госкорпорация по ОрВД»; ГУП КК "ЦИТ" Центр информационных технологий, г. Краснодар; ФГНУ НИИ "Спецвузавтоматика", г. Ростов; Северная Алания IR-0283 Комитет лесного хозяйства	г. Таганрог	9
ГУП КК "ЦИТ" для служащих органов власти (58)	Краснодар	58
Институт экономики и ВЭС ЮФУ для служащих органов власти (65)	Ростов-на-Дону	65
Всего		235

Помимо 72-часовых курсов, для всех желающих организаций был проведен ряд семинарских занятий по теме «Защита персональных данных. Новое в законодательстве. Построение системы защиты». Слушателям семинара выдаются сертификаты Южного федерального университета о том, что они прошли обучение по курсу семинара (рис 2).


Федеральное государственное автономное образовательное учреждение высшего профессионального образования
"Южный федеральный университет"

СЕРТИФИКАТ

Настоящий сертификат выдан

в том, что он(а) с "18" октября 2010 г. по "31" мая 2011 г.
прошел(ла) обучение в (на) ЮР РУНЦ ИБ
Южного федерального университета
по программе Организация и технология защиты информации
в объеме 330 часов.

М.П. Ректор

город Таганрог год 2011 Секретарь

Регистрационный номер 006/11

Рис. 2. Пример сертификатов, выдаваемых ЮФУ

Слушатели семинарских занятий получают базовые знания, необходимые для грамотного выполнения работ по созданию системы защиты персональных данных в организации. Полученные знания также позволяют контролировать и проверять работы по защите, если они были выполнены сторонними организациями. Достигнутые результаты семинарских занятий приведены в табл. 2.

Таблица 2

Виды организаций	Место проведения занятий	Число слушателей
Бюджетные организации г. Таганрога (Больницы, поликлиники, образовательные учреждения)	г. Таганрог	24
Организации здравоохранения Ростовской области	г. Ростов-на-Дону	50
Администрация Краснодарского края	г. Краснодар	40
Всего		114

Следует отметить, что повышение квалификации специалистов, а также обучение работников организаций-операторов персональных данных в области защиты информации является одной из приоритетных задач на ближайшее время в РФ – это отмечает и ФСТЭК России в методических документах.

Начиная с 1 июля 2011 г., закон № 152 «О персональных данных» в полной мере вступил в силу. В силу этого проблема создания системы защиты обрабатываемых данных приобрела особую актуальность. В рамках инновационной деятельности и для выполнения работ по защите конфиденциальной информации (в том числе персональных данных) ЮР РУНЦ ИБ были получены необходимые лицензии ФСТЭК и ФСБ.

В первую очередь интерес представляет методологический подход ЮР РУНЦ ИБ в поэтапном создании системы защиты ПДн согласно требованиям законодательства и методическим документам регуляторов.

Этап 1. Предпроектное обследование объекта информатизации

Шаг 1. Сбор технических показателей и анализ технологических процессов

Цели:

- определение технических характеристик системы;
- определение технологических характеристик системы.

Методы:

- сбор данных о технических характеристиках системы инструментальным методом (с использованием специализированных технических и программных средств);
- устный опрос сотрудников Заказчика, обладающих информацией по рассматриваемым вопросам в пределах их компетенции.

Результат:

- заполненные опросные листы в бумажном либо электронном виде;
- сгенерированные электронные отчеты по результатам применения инструментальных средств;
- согласованное с Заказчиком «Описание технологического процесса обработки информации».

Шаг 2. Оценка текущего уровня защиты информации

Цель:

- выявление уязвимостей системы.

Методы:

- инструментальный анализ (тестирование на проникновение), с применением средств анализа защищённости программных компонентов локальных вычислительных сетей;
- криптоанализ парольной информации (в целях проверки соответствия паролей пользователей требованиям безопасности). По согласованию с Заказчиком проводятся мероприятия по перехвату сетевого трафика, криптоанализу перехваченных хэшей паролей пользователей с применением радужных таблиц (rainbow table), мероприятия по анализу устойчивости ПЭВМ и серверов к активным методам перехвата информации (различные методы MITM атак, фишинг и др.), мероприятия по оценке устойчивости серверной инфраструктуры Заказчика к атакам хакеров (удалённое тестирование на проникновение на основе технологий Metasploit Framework, анализ веб-страниц, форумов, почтовых серверов и т.д.);
- анализ групповых политик безопасности.

Результат:

- сгенерированные электронные отчёты средств анализа защищенности, отражающие текущее состояние информационной безопасности ресурсов Заказчика;
- перечень рекомендаций по устранению выявленных недостатков.

Шаг 3. Подготовка документации по результатам обследования

Цель:

- документальное оформление результатов предварительного обследования.

Метод:

- экспертно-документальный.

Результат:

- согласованное с заказчиком «Аналитическое обоснование необходимости создания системы защиты информации»;

- согласованная с заказчиком «Модель нарушителя и модель актуальных угроз»;
- согласованное с заказчиком «Техническое задание на создание системы защиты информации»;
- оформленный «Акт классификации информационной системы персональных данных».

Этап 2. Организация деятельности по защите ПДн

Цель:

- создание нормативно-правового базиса, необходимого для функционирования подсистемы обеспечения информационной безопасности.

Метод:

- экспертный анализ существующей нормативно-правовой базы Заказчика (должностных инструкций, положений, организационной структуры) с оценкой соответствия представленных документов требованиям руководящих документов ФСТЭК, ФСБ, РКН.

Результат:

- распределение ответственности за информационную безопасность организации между должностными лицами;
- дополненные и исправленные внутренние документы Заказчика. При необходимости специалистами компании даётся разъяснение по каждому факту исправления документа;
- комплекс проектов вновь созданных внутренних документов Заказчика, отвечающий требованиям регуляторов;
- комплекс рекомендаций по организации взаимодействия с внешними организациями и физическими лицами;
- проект системы защиты информации.

Этап 3. Поставка технических средств защиты информации

Поставка сертифицированных средств защиты информации в соответствии со спецификацией.

Этап 4. Пусконаладочные работы

Цель:

- штатное, в соответствии с эксплуатационной документацией, функционирование компонентов системы защиты информации на объекте информатизации.

Метод:

- экспертные, программно-технические и инструментальные.

Результат:

- оформленный акт внедрения и правильности функционирования средств защиты информации.

Этап 5. Аттестация информационной системы персональных данных

Цель:

- документальное подтверждение соответствия информационной системы персональных данных требованиям регуляторов.

Метод:

- экспертно-документальные и инструментальные.

Результат:

- комплект аттестационной документации, утвержденный руководителем ЮР РУНЦ ИБ, включающий протоколы аттестационных испытаний и «Аттестат соответствия» информационной системы требованиям по защите информации.

Необходимо уточнить, что аттестация информационных систем персональных данных (ИСПДн) – это комплекс работ, включающих в себя различные проверки и выдачу Аттестата соответствия. Организация, выдавшая Аттестат соответствия, несёт полную ответственность за соответствие созданной системы защиты информации требованиям ФСТЭК и, в случае наличия обоснованных претензий со стороны Регуляторов, принимает меры по устранению выявленных недостатков совместно с Заказчиком (ст.783, ч.2 ст. 723 Гражданского кодекса Российской Федерации). В случае наличия серьёзных претензий со стороны Регуляторов к качеству работ, может быть принято решение о приостановлении действия соответствующих лицензий.

В соответствии с требованиями «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного приказом ФСТЭК от 05.02.2010 г. № 58, комплекс организационно-технических мероприятий по созданию системы защиты информации должен предусматривать внедрение следующих основных подсистем:

- подсистема управления доступом;
- подсистема регистрации и мониторинга событий;
- подсистема обеспечения целостности;
- подсистема защиты баз данных;
- подсистема анализа защищенности;
- подсистема антивирусной защиты;
- подсистема защиты от сетевых вторжений;
- подсистема межсетевого экранирования.

Одним из наиболее частых вопросов, которые задают организации-операторы ПДн, – это стоимость создания системы защиты информации согласно требованиям законодательства. Сложность ответа на этот вопрос состоит в том, что комплекс мероприятий, который нужно провести для создания системы защиты, определяется при детальном анкетировании конкретной организации. На стоимость влияют множество факторов. Вот, например, некоторые из них:

1. Наличие лицензионного программного обеспечения. Зачастую в организациях отсутствуют лицензии на операционные системы или другое важное программное обеспечение (ПО), которое необходимо для деятельности организации. При выполнении работ по защите перечень используемого ПО вносится в ряд важных организационных и аттестационных документов (техпаспорт объекта информатизации, протоколы аттестационного обследования и прочие). Поэтому прежде чем начинать работы, следует закупить лицензии на необходимое ПО, если они отсутствуют. Например, легализация ОС Windows на одной рабочей станции может обойтись до 5600 руб.
2. Необходимость передачи конфиденциальной информации по сетям общественного пользования за пределы контролируемой зоны. Обычно такая ситуация возникает, когда организация имеет филиалы или располагается в пределах нескольких далеко расположенных зданий, или существует необходимость передачи отчётности по Интернету (например, в фонды медицинского страхования или другие). В этом случае возникает актуальная угроза перехвата передаваемого трафика. В связи с удаленностью точек обмена информацией предотвратить угрозу организационным способом (например, визуальным наблюдением) не получится. Поэтому необходимо покупать криптографические средства защиты передаваемой информации. Кроме того, необходимо разрабатывать дополнительную документацию: модель угроз по ФСБ, инструкции, журналы и прочее. Всё это повышает стоимость работ.

3. Класс защищаемой информационной системы. Для ИСПДн определены 4 класса (К1, К2, К3, К4). Основная масса реально работающих систем может быть отнесена к классам К2 и К3. Для таких систем можно использовать штатные средства защиты от несанкционированного доступа (НСД) сертифицированных операционных систем. Это наиболее предпочтительный вариант, отличающийся дешевизной и простотой эксплуатации. Однако, если класс ИСПДн равен К1, то штатные средства защиты не подходят, и нужно закупать сертифицированные ФСТЭК по классу К1 средства защиты от НСД сторонних разработчиков. Это также требует дополнительных расходов.

Следует заметить, что таких факторов, влияющих на стоимость создания системы защиты, достаточно много, и определить стоимость работ для конкретной организации без анкетирования представляется маловероятным.

Для лучшего представления о стоимости закупки средств защиты информации можно привести табл. 3. В ней приведена спецификация на закупку средств защиты для одной рабочей станции, подключенной к сети Интернет, на которой функционирует ИСПДн класса К3. Конфиденциальная информация по сети не передается. Это типовой вариант бухгалтерского или кадрового рабочего места.

Таблица 2

% п/п	Наименование	Количество	Стоимость, руб.
Средства защиты от НСД			
1	Дистрибутив сертифицированной ОС Windows XP	1	1 300
2	Полный пакет для сертифицированной версии ОС Windows XP Professional	1	2 600
3	Пакет «Базовый контроль» для сертифицированной версии ОС Windows XP Professional для использования	1	1 200
4	Лицензия на использование программы контроля сертифицированной версии ОС Windows XP Professional (XP_ Check 3.0)	1	900
5	ПАК усиления функций безопасности ОС MS Windows XP Professional – сертифицированный USB-ключ eToken PRO	1	1 200
Средства защиты межсетевого взаимодействия			
6	Установочный комплект Security Studio Endpoint Protection (Personal Firewall, HIPS). Межсетевой экран и средство обнаружения вторжений	1	300
7	Право на использование Средств защиты информации Security Studio Endpoint Protection: Personal Firewall, HIPS	1	2 440
Средство защиты от вирусов и других вредоносных программ			
8	Антивирус Dr.Web Desktop Security Suite, на 12 месяцев, неисключительное право	1	990
9	Медиа-комплект для Windows сертифицированный. Антивирус Dr.Web	1	900
ИТОГО			1 1830

К представленной таблице можно добавить лишь, что существует достаточно много вариантов формирования спецификации на основе различных производителей программного обеспечения. В данном примере приведен наиболее оптимальный на наш взгляд набор средств защиты для заданной выше ИСПДн. Важно заметить, что все средства защиты по требованиям законодательства РФ должны быть сертифицированными ФСТЭК (для криптографии ФСБ).

На сегодняшний день ЮР РУНЦ ИБ успешно выполнил работы по защите систем персональных данных в больницах, поликлиниках, детских санаториях города Таганрога. Муниципалитет города во исполнение закона № 152-ФЗ «О персональных данных» в первую очередь выделяет бюджет для защиты таких организаций, где обрабатываются сведения о состоянии здоровья граждан.

Таким образом, Южно-Российский региональный учебно-научный центр по проблемам информационной безопасности в системе высшей школы ЮФУ (ЮР РУНЦ ИБ) в рамках инновационной деятельности ЮФУ активно участвует в деятельности по защите конфиденциальной информации и персональных данных организаций и предприятий, проводит внедрения систем защиты, а также регулярно организует курсы и семинары повышения квалификации в этой области.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.06 г. № 152-ФЗ «О персональных данных».
2. Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.08 г. № 55/86/20.
3. Указ Президента РФ от 06.03.97 г. № 188 "Об утверждении перечня сведений конфиденциального характера" (с изменениями на 23 сентября 2005 г.).
4. Приказ ФСТЭК России №58 "Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных" от 5 февраля 2010 г.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Макаревич Олег Борисович – Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге; e-mail: mak@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634312018; кафедра безопасности информационных технологий; зав. кафедрой.

Басан Александр Сергеевич – e-mail: tftrtu@mail.ru; тел.: 89885370968; кафедра безопасности информационных технологий; доцент.

Makarevich Oleg Borisovich – Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: mak@sfedu.ru; 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security in data processing technologies; chief of the department.

Basan Alexandr Sergeevich – e-mail: tftrtu@mail.ru; phone: +79885370968; the department of security in data processing technologies; associate professor.