Фасхеев Кирилл Владимирович,

студент 5 курса института энергетики и автоматизированных систем,

ФГБОУ ВО «МГТУ им. Г.И. Носова»,

г. Магнитогорск

Научный руководитель ***Коновалов Максим Владимирович,***

старший преподаватель кафедры информационной безопасности

ФГБОУ ВО «МГТУ им. Г.И. Носова»,

г. Магнитогорск

АНАЛИЗ И ПРОВЕДЕНИЕ БАЗОВЫХ МЕРОПРИЯТИЙ В ОРГАНИЗАЦИИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ANALYSIS AND IMPLEMENTATION OF BASIC ACTIVITIES IN THE ORGANIZATION IN THE PROCESSING OF PERSONAL DATA IN INFORMATION SYSTEMS

Аннотация. В статье будут рассмотрены основные проблемы, с которыми сталкиваются коммерческие и государственные организации при работе с персональными данными работников и граждан, обратившихся к ним за предоставлением каких-либо услуг, а также при их обработке в информационных системах. На примере типовой организации будут выявлены цели и виды обработки данных, перечень обрабатываемых персональных данных, проведено определение уровня защищённости.

Ключевые слова: информационная безопасность, информационная система персональных данных, защита персональных данных, установка уровня защищённости, реестр операторов РКН.

In this paper, we will analyze the main problems faced by commercial and government organizations when working with personal data of employees and citizens who applied to them for the provision of any services, as well as during their processing in information systems. Using the example of a typical

organization, the goals and types of data processing, the list of personal data being processed will be identified, the level of security will be determined and the model of the probable offender will be built.

Keywords: information security, personal data information system, personal data protection, offender model, setting the level of security, register of operators of RKN.

В нынешнюю развитую цифровую эру современные организации обрабатывают и пропускают через себя поразительные по объёму потоки данных, в том числе личную информацию своих работников и что немало важно клиентов. Заполучив доступ к данным средней по численности организации можно причинить непоправимый финансовый вред компании-владельцу, а также репутации. Персональные данные заняли первое место по важности и ценности в современной стратегии ведения бизнеса, а также самой желанной наживой злоумышленников и конкурентов во всех областях.

Защита персональных данных [1] в Российской Федерации регламентируется законодательно со стороны следующих государственных структур: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) – является своеобразным куратором в сфере обработки, хранения и передачи (распространения) персональных данных, Федеральная служба по техническому и экспортному контролю (ФСТЭК) – орган исполнительной власти регламентирующий подоход к обеспечению защиты информации и информационных ресурсов, Федеральная служба безопасности Российской Федерации (ФСБ РФ) – орган исполнительной власти регламентирующий использование средств криптографической защиты информации при передаче персональных данных по каналам

связи, также в формирование правовой базы участвует Правительство Российской Федерации издавая акты управления общенормативного содержания и Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России).

Для обеспечения безопасности [2] организации коммерческие и государственные зачастую привлекают сторонние коммерческие компании-лицензиаты, которые являются обладателями лицензий вышеперечисленных государственных органов, но привлечение данных частных фирм не является необходимостью.

Целью данной статьи является разбор необходимых правовых решений и технических мероприятий проводимых при построении системы защиты информации информационной системы персональных данных.

Построение защиты для информационной системы не возможно без определения защищаемой информации, уровня обеспечения защиты и подбора средств защиты информации.

Из этого можно выявить основные задачи:

– выявление обрабатываемых персональных данных из процессов обработки и объединение их в одну информационную систему;

– определение уровня защищённости персональных данных;

– выбор средств защиты информации для выделенной системы.

Защищаемой информацией в рамках данной статьи будут являться персональные данные граждан, получающих услуги в организации, чья конфиденциальная информация обрабатывается в рамках осуществления деятельности предприятия. Приведённая в статье организация является удалённым сегментом юридического лица, предоставляющего развлекательные услуги (кино, игровые автоматы,

бильярдные зоны и пр.). Данные о гражданах, обратившихся в организацию, используются исключительно для одной цели - предоставления физическим лицам бонусной программы в виде специальных накопительных пластиковых карт (далее – VIP-карта). Персональные данные (далее – ПДн) передаются владельцем в бумажном виде на анкете заявителя и в дальнейшем вносятся в ИСПДн путём оцифровывания. Основываясь на этой информации, мы выделяем информационную систему персональных данных (далее - ИСПДн) «Граждане» и определяем способ обработки как смешанный т.е. включающий в себя как автоматизированный процессы (при помощи средств вычислительной техники), так и без использования средств автоматизации [3].

Перечень сведений, составляющих персональные данные и их способ обработки, приведен в Таблице 1.

Таблица 1.

Перечень сведений и способ обработки персональных данных граждан

№ п/п	Наименование персональных данных	Способ обработки
1.	Фамилия, имя, отчество	Смешанный
2.	Дата рождения	
3.	Номер телефона	
4.	Адрес электронной почты	
5.	Сведения о детях	
6.	Даты рождения детей	

Для установления уровня защищённости (далее - УЗ) [4] необходимо определить следующее: тип актуальных угроз, категорию персональных данных, количество субъектов ПДн. Для данной ИСПДн актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении,

используемом в информационной системе. Основываясь на Таблице 1 в защищаемой ИСПДн обрабатываются иные категории ПДн. Количество единовременно обрабатываемых данных о субъектах ПДн менее 100 000. Исходя из вышеизложенного ИСПДн «Граждане» присваивается 4 уровень защищённости персональных данных, для наглядности приведён Таблица 2.

Таблица 2.

Определение уровня защищённости

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		Более 100 тыс.	Менее 100 тыс.			Более 100 тыс.	Менее 100 тыс.		Более 100 тыс.	Менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

После определения уровня защищённости персональных данных при их обработке в информационных системах необходимо создать документ (приказ), в котором нужно определить комиссию в составе нескольких человек, а также закрепить обоснования и сам УЗ.

Чтобы определить характеристики необходимых средств защиты информации для нашей ИСПДн необходимо обратиться к Приказу ФСТЭК России № 21 [5], а точнее к таблице «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Основываясь на данной информации защищаемой ИСПДн необходимы следующие средства защиты: средство защиты информации от несанкционированного доступа (далее - СЗИ от НСД), антивирусное средство защиты (далее – АВ), средство межсетевого экранирования (далее – МЭ) и средство криптографиче-

ской защиты информации (далее – СКЗИ) при передаче данных по сети «Интернет» в соответствии с приказом ФСБ России от 10 июля 2014 г. № 378 [6]. Соотнеся полученные данные с государственным реестром сертифицированных средств мы можем выбрать необходимые средства и получить ценовую информацию от поставщиков. Сейчас на рынке преобладают следующие сертифицированные средства защиты: Secret Net Studio – в зависимости от комплектации может выполнять роль: СЗИ от НСД, АВ и МЭ. Dallas Lock 8.0-K/C – может служить как: СЗИ от НСД и МЭ. В качестве СКЗИ на рынке в основном преобладают решения компании Код Безопасности и InfoTeCS, которые в свою очередь могут выступать ещё и в качестве МЭ.

Далее требуется заполнить информационное письмо о внесение в реестр операторов обрабатывающих персональные данные, либо заполнить форму о внесении изменений если письмо уже было отправлено ранее. Обе формы можно найти на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по адресу: www.pd.rkn.gov.ru/operators-registry/notification/ (адрес актуален на момент написания статьи). После заполнения заявки и нажатия кнопки: «Отправить электронное уведомление и подготовить форму к распечатке» - рекомендуется печатный экземпляр отнести самостоятельно в Управление Роскомнадзора по вашему региону, а не пользуясь услугами почты. После принятия уведомления по прошествии нескольких рабочих дней вы сможете найти свою организацию в «Реестре операторов, осуществляющих обработку персональных данных» на сайте Управления, также при изменении количества и данных о ИСПДн необходимо вносить изменения.

Также для обеспечения безопасности не малую роль играет

разработка приказов, инструкций и прочей организационной распорядительной документации по защите информации и персональных данных, но ввиду большого объёма в данной статье она рассмотрена не будет.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных».

3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Приказ ФСТЭК России от 18.02.2013 № «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. Михайлова У.В., Хусаинов А.А. Особенности и проблемы, возникающие при разработке моделей угроз информационной безопасности //Безопасность информационного пространства: сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. – Курган: КГУ, 2016. – С. 72-75.

PREFERENCES

1. Federal Law of July 27, 2006 No. 149 «On Information, Information Technologies and on Protection of Information».

2. Federal Law of the Russian Federation of July 27, 2006 No. 152-ФЗ "On Personal Data".

3. Decree of the Government of the Russian Federation of September 15, 2008 No. 687 Moscow "On Approval of the Regulation on Peculiarities of Processing Personal Data Performed Without the Use of Automation Means".

4. Decree of the Government of the Russian Federation of November 1, 2012 No. 1119 Moscow "On approval of requirements for the protection of personal data when it is processed in personal data information systems".

5. Order of the FSTEC of Russia of February 18, 2013, No. "On Approving the Composition and

Content of Organizational and Technical Measures for Ensuring the Security of Personal Data During Their Processing in Personal Data Information Systems".

6. *Mihajlova U.V., Husainov A.A. Osobennosti i problemy, voznikajushhie pri razrabotke modelej ugroz informacionnoj bezopasnosti //Bezopasnost' informacionnogo prostranstva: sbornik materialov XV Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchenyh. Kurgan: KGU. – 2016. S. 72-75. State Register of Certified Information Security Means No. ROSS RU.0001.01BI00.*