получить доступ к другим абонентам этой сети, к электронной почте, к телетайпам и телефаксам, работающим с этой сетью. Оснащение средств оргтехники процессорами и памятью, подключение этих средств к персональным компьютерам или включение их в вычислительные сети в качестве отдельных терминалов является основополагающей тенденцией развития всех технических средств управления.

Одним из основных направлений совершенствования систем связи (как и многих других ТСУ) является переход на цифровые технологии. Важнейшей тенденцией является создание интегрированных систем, включающих различные средства и системы связи, что создает предпосылки для формирования в недалеком будущем глобальной коммуникационной системы.

Имеются и общие тенденции развития, присущие всем классам средств организационной техники, к которым относятся:

–совершенствование ранее существовавших и появление принципиально новых средств организационной техники;

–повышение производительности и качества работы технических средств управления;

–расширение функций и сервисных возможностей офисных аппаратов;

–высокие требования безопасности эксплуатации;

–возможность использования современных технических средств непосредственно в офисе, на рабочих местах сотрудников – т. е. превращение средств оргтехники, в полном смысле этого слова, в офисные;

–оснащение средств оргтехники процессорами и памятью; возможность их подключения к персональному компьютеру или включение в корпоративную вычислительную сеть в качестве отдельных терминалов;

– появление интегрированных систем, сочетающих различные технологии и обладающие широким набором возможностей.

–простота освоения и использования современных офисных аппаратов, которые не требуют специального обучения персонала и, как правило, эксплуатируются сотрудниками параллельно с выполнением своих основных обязанностей.

Все перечисленные факторы оказывают позитивное влияние на повышение эффективности деятельности офисных работников, а следовательно, на повышение эффективности управления.

Симоненко О. С., Барнаул (АлтГУ)

ОРГАНИЗАЦИОННАЯ ДОКУМЕНТАЦИЯ В СИТЕМЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Деятельность подавляющего большинства организаций неотъемлемо включает в себя работу по обработке персональных данных (далее ПД) различных категорий. Известно, что безопасность ПД при их обработке в информационных системах

персональных данных (далее ИСПДн) достигается путем построения системы защиты ПД, которая подразумевает под собой принятие организационных и технических мер[1].

В рамках рассматриваемой темы нас будет интересовать организационная часть мер во исполнение безопасности ПД в ИСПДн. Данные меры включают в себя подготовку и внедрение организационно-распорядительной документации и реализацию необходимых мероприятий по защите ПД.

Создание пакета документов направлено на исполнение обязанностей оператора, установленных ФЗ № 152 «О персональных данных»[2], осуществляется в соответствии с ним и множеством иных принятых нормативных актов. В свою очередь, контроль и надзор за созданием и предоставлением такого пакета документов осуществляет Уполномоченный орган – Роскомнадзор[3].

Согласно Постановлению Правительства № 211[4] установлен перечень таковых документов, но, следует заметить, что в сферу его действия входят лишь ИСПДн государственных и муниципальных органов. Кроме того, необходимо учитывать, что состав описываемых организационных мер может видоизменяться в зависимости от специфики конкретной системы, включая следующие аспекты: категория ПД (общедоступные, специальные, биометрические, ПД работников организации, иные ПД), объем обрабатываемых ПД, особенности структура ИСПДн и др., в связи с чем, не существует единого обязательного и всеобъемлющего перечня для всех возможных организаций и их ИСПДн. Обозначим, что речь идет об автоматизированных ИСПДн, т. к. требования к эксплуатации ИСПДн, осуществляющих обработку ПД без средств автоматизации, устанавливаются Постановлением Правительства № 687[5].

Примерный перечень основных документов может иметь в своем составе: положение об обеспечении защиты ПД в ИСПД, которое содержит установленные в организации требования по обеспечению безопасности ПД, включающие в себя принципы защиты ПД, описание процесса сбора и хранения ПД, информацию о том, в каких структурных подразделениях хранятся ПД, сведения о носителях ПД, фиксацию лиц, получающих право доступа и т. д.; положение об обработке ПД, представляющее собой правила по обработке ПД, которые должны содержать описание процесса обработки и использования ПД в организации, состав ПД, права и

---

[1] Требований к защите персональных данных при их обработке в информационных системах персональных данных: утв. Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 // Российская газета. 2012. 07 ноября.

[2] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Российская газета. 2006. 29 июня.

[3] Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: утв. Постановлением Правительства РФ от 16 марта 2009 г. N 228 // Российская газета. 2009. 24 марта.

[4] 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: Постановление Правительства РФ от 21 марта 2012 г. N 211 // Российская газета. 2012. 30 марта.

[5] Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: утв. Постановлением Правительства от 15 сентября 2008 г. N 687 // Российская газета. 2008. 24 сентября.

ответственность пользователя ИСПДн, сроки хранения, порядок уничтожения по достижению цели обработки и т. д.; приказ о назначении ответственного за обработку ПД; перечень должностных лиц, допущенных к обработке ПД, который фиксирует перечень должностных лиц, имеющих право на доступ к ИСПДн в рамках служебных обязанностей, а также широту полномочий каждого из них по отношению к конкретным действиям; перечень ПД; перечень ИСПДн; технический паспорт информационных систем, описывающий структурные особенности и принципы работы ИСПДн; перечень средств защиты; частная модель угроз безопасности ПД при их обработке в ИСПДн и модель нарушителя безопасности ПД при их обработке в ИСПДн, которые составляется на основе методических документов ФСТЭК[1]; регламент по учету, хранению и уничтожению носителей ПД; регламент по допуску лиц к ИСПДн; регламент по резервному копированию ПД; уведомление об обработке ПД; форма согласия на обработку ПД; форма обязательства о неразглашении ПД. Кроме описанных организационных актов следует предусмотреть различные индивидуальные инструкции по работе в системе в зависимости от прав пользователя, журналы регистраций, приказы о назначениях.

Таким образом, складывается достаточно трудоемкий процесс по реализации организационных мер по обеспечению защиты ПД в ИСПДн, в частности, оформление надлежащего пакета документов. Во многом, данная причина обуславливает рост популярности использования привлечения квалифицированных специалистов извне, что более рационально с расчетом затраченных средств и ресурсов.

Соколова А. О., Екатеринбург (УрФУ)

ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ КАК ВАЖНЫЙ ЭТАП РАЗРАБОТКИ И РЕАЛИЗАЦИИ ПРОЕКТА СОВЕРШЕНСТВОВАНИЯ ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ ОРГАНИЗАЦИЕЙ

В настоящее время совершенствование информационно-документационного обеспечения конкретной организацией целесообразно проводить в рамках разработки и реализации единого организационного проекта.

Практика разработки и реализации подобных оргпроектов охарактеризована и обобщена в публикациях специализированных журналов. В этих статьях, в частности, выделяются следующие основные этапы организационного проектирования: 1. Проведение предпроектного обследования, т. е. сбор исходных данных для проектирования; 2. Анализ существующей системы делопроизводства на основе

[1] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСТЭК России от 15.02.2008. URL: http://www.zakonprost.ru/content/base/268759; Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСТЭК России от 14.02.2008 (ред. 06.05.2015 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_77814/