

Особенности защиты  
персональных данных  
в Интернет-порталах



Защита персональных является важным направлением деятельности множества компаний. Эта деятельность ориентирована на защиту прав субъектов персональных данных, а так же на выполнение требований, установленных нормативными правовыми актами в данной области.

Достаточно остро проблема защиты персональных данных (ПДн) затрагивает деятельность Интернет-порталов, предлагающих физическим лицам различные услуги и интернет-сервисы, такие как:

- online продажа товаров и оказание услуг;
- сетевые игры;
- социальные сети и профессиональные сообщества.

Трудности при выполнении требований регуляторов<sup>1</sup> возникают уже на этапе классификации информационной истемы персональных данных (ИСПДн), формулирования целей и определения правового основания обработки ПДн. Другой организационной проблемой является получение согласия субъекта ПДн на обработку его персональных данных. Часто в подобных системах возникает вопрос с трансграничной передачей ПДн.

К основным особенностям, удорожающим и усложняющим технические аспекты создания системы защиты персональных данных Интернет-порталов, следует отнести:

- распределенную информационно-вычислительную архитектуру ИСПДн;
- значительный объем обрабатываемых ПДн;
- применение специализированных технологий и программно-технических средств, не обладающих сертификатами соответствия по требованиям безопасности информации;
- различные подходы к реализации ИТ-инфраструктуры портала (от аренды вычислительных мощностей центров обработки данных (ЦОД) до использования собственного серверного комплекса).

Таким образом, важно не только создать систему защиты персональных данных в соответствии с действующими требованиями регуляторов, но и сформировать надлежащее организационное обеспечение.

Для решения проблемы получения согласия субъекта ПДн на обработку его персональных данных могут применяться договоры публичной оферты, предусмотренные статьей 437 Гражданского кодекса РФ. Текст соответствующего соглашения размещается на сайте оператора, при этом указывается его статус и то обстоятельство, что соглашение заключается между оператором и пользователем (субъектом ПДн) в форме договора присоединения. Акцептом условий размещенного на сайте соглашения как правило является совокупное осуществление пользователем действий, необходимых для регистрации на Интернет-портале (так называемые конклюдентные действия). В тексте оферты следует указать, что ее акцепт означает полное и безоговорочное принятие пользователем всех условий соглашения без каких-либо изъятий и/или ограничений и равносителен заключению двухстороннего письменного соглашения о предоставлении доступа к сервисам Интернет-портала (п. 3 ст. 434 ГК РФ). Пользователь производит акцепт соглашения после ознакомления с его условиями (в соста-

в которых содержатся положения о согласии на обработку персональных данных). Как правило, устанавливается, что срок акцепта не ограничен, а соглашение может быть расторгнуто в установленном порядке. Такой подход позволяет говорить о получении согласия, поскольку в регистрационной системе портала фиксируется выполнение конклюдентных действий, свидетельствующих об акцепте соглашения. Следует отметить, что приведенный подход требует от оператора предусматривать процедуру верификации пользователя (субъекта ПДн) с использованием контактной информации, предоставленной при регистрации.

В качестве основания для обработки ПДн рекомендуется указывать Федеральный закон, постановление Правительства Российской Федерации, иной нормативный правовой акт, закрепляющий основание и порядок обработки персональных данных. Интернет-магазины используют в качестве такого НПА «Правила продажи товаров дистанционным способом», утвержденные постановлением Правительства РФ от 27 сентября 2007 г. N 612. Если деятельность организации, содержащей Интернет-портал, лицензируется, в качестве основания может быть указана соответствующая лицензия. Универсальным основанием является и устав организации, в котором закреплены цели ее деятельности, в т.ч. требующие обработки ПДн.

Обеспечение безопасности ПДн в соответствии с требованиями руководящих и методических документов ФСТЭК ФСБ России для ИСПДн, представляющих собой Интернет-порталы, зачастую сопряжено с большими трудностями ввиду повсеместного использования сторонних ЦОД при размещении технических средств, а также невозможностью использования дополнительных («наложенных») средств защиты информации, что в большинстве случаев обусловлено спецификой технологического процесса обработки информации.

Исходя из типовой распределенной архитектуры Интернет-портала, представленной на рисунке (Рисунок 1) необходимо отметить, что основные угрозы связаны прежде всего с сетевыми воздействиями, направленными на различные узлы портала, а так же с злонамеренными действиями обслуживающего персонала.

С технической точки зрения в 90 % случаев можно утверждать, что большинство подсистем безопасности, необходимых к реализации в СЗПДн в соответствии с требованиями

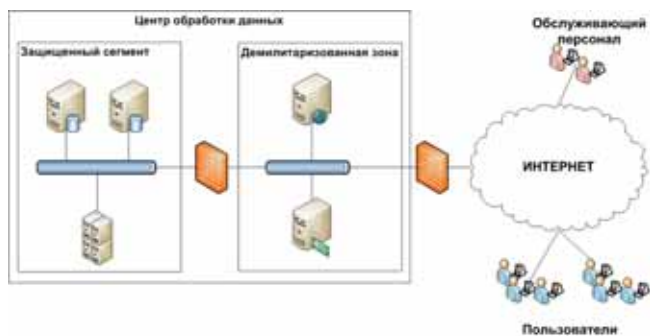


Рис. 1 Типовая схема интернет-портала

ми регуляторов, уже существуют в системном и прикладном программном обеспечении Интернет-портала (веб-сервер, система управления базами данных, сервер приложений). К подсистемам СЗПДн, функции которых уже реализованы, как правило относятся:

- подсистема управления доступом (частично – включая средства обеспечения безопасности межсетевое взаимодействия);
- подсистема регистрации и учета;
- подсистема обеспечения целостности;

При этом основной задачей оператора ПДн является «легализация» существующих механизмов безопасности (подтверждение их соответствия требованиям РД и МД регуляторов). Это подтверждение на практике реализуется с помощью сертификации встроенных механизмов защиты программного обеспечения информационной системы на соответствие требованиям безопасности информации. Наличие сертифицированного «программного ядра» портала совместно с использованием услуг аттестованных центров обработки данных позволит сэкономить на защите ИСПДн и отказаться от повсеместного использования наложенных средств защиты.

В целях выполнения требований законодательства и создания эффективной и отвечающей современным условиям системы защиты персональных данных компания «ИНФОРИОН» предлагает комплексный подход, позволяющий наиболее рационально преодолеть трудности, возникающие при создании СЗПДн Интернет-портала.

Основой подхода является комплекс услуг и технических решений включающих:

- консалтинговые услуги в области соблюдения законности обработки ПДн;
- подготовку необходимой организационно-распорядительной документации, определяющей правила, требования, порядок обработки и обеспечения безопасности ПДн;
- разработку требований к ИТ-инфраструктуре центра обработки данных;
- поиск оптимального ЦОД с точки зрения безопасности и производительности для реализации Интернет-портала (либо помощь в получении подтверждения соответствия требованиям безопасности информации);
- доработку механизмов безопасности портала до требований РД и МД регуляторов;
- сертификацию программного комплекса портала;
- аттестацию развернутого Интернет-портала по требованиям безопасности информации (по усмотрению оператора).

Результатом приведенного перечня работ является пакет организационно-распорядительных документов по организации обработки и защите ПДн и система защиты персональных данных, созданная в соответствии с требованиями, предусмотренными руководящими и методическими документами.

Подход, предлагаемый компанией «ИНФОРИОН», позволит создать оптимальную систему защиты персональных данных Интернет-портала с точки зрения стоимости и эффективности снижения рисков.