УДК 004.658

*А. А. Персичкин*

# ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИЩЕННОСТЬ ОБЪЕКТОВ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

*Проанализированы основные проблемы по организации сохранности персональных данных в различных организациях, рассмотрены подходы к построению систем их защиты и предложены конкретные рекомендации по обеспечению инженерно-технической защищенности объектов обработки персональных данных.*



*The paper analyzes the main problems of the organization of personal data security in various organizations, considers the approaches to building systems of their protection and offers specific recommendations to ensure the engineering and technical security of personal data processing facilities.*

**Ключевые слова:** персональные данные, информационная система, инженерно-техническая защищенность.

**Keywords:** personal data, information system, engineering and technical security.

## Введение

В настоящее время персональные данные (далее — ПД) перешли из предмета дискуссий в самостоятельное понятие, имеющее свои свойства, одно из которых — значимость. С точки зрения юридической значимости ПД относятся к информации, не подлежащей разглашению без ведома ее обладателя. *Персональные данные — это тайна.* Российским законодательством определено более 100 видов тайн, и только государственная тайна и ПД подлежат обязательной защите, то есть *без соответствующей системы защиты информации обработка персональных данных в РФ запрещена*.

## Организация защиты персональных данных

Само понятие «персональные данные» появилось в связи с обработкой информации о гражданах в информационных системах. Соответственно, построение системы защиты ПД в основном рассматривается с точки зрения информационной безопасности указанных систем, и в этой области наработана полноценная методическая и практическая база. Хотелось обратить внимание на то, что «размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц» [1].


*Вестник Балтийского федерального университета им. И. Канта.*
*Сер.: Физико-математические и технические науки. 2019. № 4. С. 64 – 66.*

Иными словами, перед созданием инфраструктуры обработки ПД в виде информационной системы и соответствующей системы защиты необходимо обеспечить физическую защищенность объекта обработки ПД в целом. Проблема в том, что в настоящее время отсутствуют конкретные методические рекомендаций, регламентирующие мероприятия по инженерно-технической защите указанных объектов. Это при очевидности того, что указанные мероприятия должны быть реализованы в первую очередь — до начала обработки персональных данных.

Из практики организации комплексной защиты объектов информатизации можно выделить следующие физические объекты, свойства которых являются критериями инженерно-технической защищенности: инженерные конструкции (стены строений, перекрытия и т.д.), дверные и оконные конструкции, запирающие устройства.



Выбор конкретного инженерного объекта (стены, замка и т.д.) обязательно должен проводиться в соответствии с положениями нормативно-правового акта, который подтверждал бы факт соответствия инженерного объекта требуемым критериям защиты. Такими документами следует считать ГОСТы, соблюдение которых является обязательным при построении систем защиты.

Сейчас государственные стандарты охватывают все инженерные объекты, участвующие в создании систем инженерно-технической защиты. Для реализации конкретной системы требуется создание юридически значимых методических рекомендаций, в которых указываются соответствия технических параметров инженерного объекта требуемым критериям защищенности.

В этой связи для построения системы инженерно-технической защищенности объектов с обработкой ПД предлагается использовать [2], в котором подробно категорированы инженерные сооружения и даны конкретные рекомендации по выбору строительных, дверных и оконных конструкций, запирающих устройств. В частности, в документе объектам (помещениям) с обработкой сведений, составляющих персональные данные граждан, присвоена категория А2 — высокая степень защищенности (помещения с обработкой сведений, составляющих государственную тайну, имеют самую высокую категорию А1).

В качестве примера приведем рекомендации [2] для дверных конструкции объектов категории А2: «Дверные конструкции 3 класса защиты (высокая степень защиты объекта от проникновения): двери, соответствующие II классу защиты от взлома ГОСТ Р 51072-05; двери II класса защиты от взлома по ГОСТ Р 51072-05 с защитным остеклением класса Б1 и выше по ГОСТ Р 51136-08».

**Выводы**

Дадим основные рекомендации по обеспечению инженерно-технической защищенности объектов обработки ПД:

— помещения, в которых ведется обработка и хранение ПД, должны быть обеспечены охранно-пожарной сигнализацией и системой

контроля управления доступом (СКУД), выведенной на пульт охраны. С этой целью оператор должен заключить договор с организацией, имеющей лицензию на оказания охранных услуг;

— на все инженерно-технические средства охраны (технические средства охраны, двери, запирающие устройства, хранилища) должны быть сертификаты, подтверждающие соответствие требованиям безопасности;

— система инженерно-технической защиты должна состоять из нескольких рубежей, суммарное время преодоления которых должно быть больше промежутка с момента поступления сигнала тревоги до прибытия сотрудников охранной организации. В основном время преодоления рубежа охраны определяется классом защиты запорных устройств и хранилищ, а время реагирования сотрудников охранной организации прописывается при заключении договора на оказание охранных услуг;



— в организации, обрабатывающей ПД, должны быть разработаны и выполняться регламенты по обеспечению сохранности ПД: использование СКУД, сдача помещений под охрану, сдача опечатанного пенала с ключами от охраняемых помещений на пост охраны и т. д.

**Список литературы**

1. *Об утверждении* Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 17 ноября 2007 г. №781. Доступ из справ.-правовой системы «Гарант».

2. *Р 78.36.032-2013.* Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Ч. 1 : Методические рекомендации (утв. МВД России 11 декабря 2013 г.). Доступ из справ.-правовой системы «Гарант».

**Об авторе**

Андрей Андреевич Персичкин — директор ГАУ КО «Калининградский государственный научно-исследовательский центр информационной и технической безопасности», Россия.

E-mail: a.persichkin@kgnic.ru

**The author**

Andrey A. Persichkin, Head of the Kaliningrad State Research Center of Information and Technical Security, Russia.

E-mail: a.persichkin@kgnic.ru