ПРАВИТЕЛЬСТВО ОРЕНБУРГСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

12.08.2025 г. Оренбург № 855-пп

О внесении изменений в постановление Правительства Оренбургской области от 28 июня 2019 года № 418-пп

Правительство Оренбургской области п о с т а н о в л я е т:

1. Внести в постановление Правительства Оренбургской области от 28 июня 2019 года № 418-пп «Об утверждении положения об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области» следующие изменения:

1.1. В наименовании, преамбуле, пункте 1 постановления слова «органов исполнительной власти» заменить словами «исполнительных органов».

1.2. Пункт 2 постановления изложить в новой редакции:

«2. Исполнительным органам Оренбургской области при составлении частных моделей угроз руководствоваться нормативными правовыми актами Российской Федерации в сфере информационной безопасности и положением.».

1.3. Пункт 3 постановления после слова «руководствоваться» дополнить словами «нормативными правовыми актами Российской Федерации в сфере информационной безопасности и».

1.4. Пункт 4 постановления изложить в новой редакции:

«4. Контроль за исполнением настоящего постановления оставляю за собой.».

1.5. Приложение к постановлению изложить в новой редакции согласно приложению к настоящему постановлению.

2. Постановление вступает в силу после дня его официального опубликования.

Временно исполняющий обязанности Губернатора

АППАРАТ ГУБЕРНАТОРА И ПРАВИТЕЛЬСТВА ОРЕНБУРГСКОЙ ОБЛАСТИ * УПРАВЛЕНИЕ ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ

Е.А.Солнцев

Приложение
к постановлению Правительства
Оренбургской области
от 12.08.2025 № 855-пп

Положение
об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов Оренбургской области

I. Общие положения

1. Настоящее Положение определяет угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, владельцами и операторами которых являются исполнительные органы Оренбургской области, государственные учреждения и предприятия Оренбургской области (далее – исполнительные органы и организации).

2. При определении угроз безопасности персональных данных, актуальных для конкретной информационной системы персональных данных, следует проводить анализ угроз безопасности информации и уязвимостей программного обеспечения с учетом угроз и уязвимостей, содержащихся в банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю bdu.fstec.ru в информационно-телекоммуникационной сети «Интернет».

3. С целью реализации полномочий и осуществления функций исполнительными органами и организациями обрабатываются все категории персональных данных. Состав персональных данных, подлежащих обработке в конкретной информационной системе персональных данных, цели такой обработки, действия (операции), совершаемые с персональными данными в информационных системах персональных данных, определяются оператором информационных систем персональных данных.

II. Участники взаимодействия и сети передачи данных

4. Контролируемой зоной информационных систем персональных данных являются здания и отдельные помещения, принадлежащие исполнительным органам и организациям или арендуемые ими (далее – контролируемая зона). Все средства вычислительной техники, участвующие в обработке персональных данных, находятся в пределах контролируемой зоны. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование оператора связи (провайдера), используемые для информационного обмена по сетям связи общего пользования (сетям международного информационного обмена).

5. Локальные вычислительные сети передачи данных в исполнительных органах и организациях имеют подключения к следующим сетям:

1) внешние сети (сети провайдера). Подключение к внешним сетям (сетям провайдера) организовано посредством следующих типов каналов связи:

оптоволоконные каналы связи операторов связи (провайдеров);

проводные каналы связи операторов связи (провайдеров);

2) сети исполнительных органов и организаций, организаций (предприятий, учреждений), расположенных на территории Российской Федерации. Подключение к таким сетям осуществляется в соответствии с разработанными регламентами взаимодействия. Исполнительные органы и организации подключены к единой информационно-телекоммуникационной сети посредством защищенных каналов связи;

3) иные сети, взаимодействие с которыми организовано исполнительными органами и организациями с целью реализации своих полномочий.

6. Подключение к сетям связи общего пользования осуществляется исполнительными органами и организациями с применением средств криптографической защиты информации.

III. Объекты защиты и технологии обработки персональных данных в информационных системах персональных данных

7. При определении исполнительными органами и организациями угроз безопасности персональных данных в конкретной информационной системе персональных данных защите подлежат следующие объекты, входящие в информационные системы персональных данных:

персональные данные, обрабатываемые в информационных системах персональных данных;

информационные ресурсы информационных систем персональных данных (файлы, базы данных и другое);

средства вычислительной техники, участвующие в обработке персональных данных посредством информационных систем персональных данных;

средства криптографической защиты информации и средства защиты информации;

среда функционирования средств криптографической защиты информации;

информация, относящаяся к криптографической защите персональных данных, в том числе ключевая, парольная и аутентифицирующая информация средств криптографической защиты информации;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие и другие материалы, отражающие защищаемую информацию, относящуюся к информационным системам

персональных данных и их криптографической защите, включая документацию на средства криптографической защиты информации, технические и программные компоненты среды функционирования средств криптографической защиты информации;

носители защищаемой информации, используемые в информационных системах персональных данных, в том числе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации средств криптографической защиты информации и порядок доступа к ним;

каналы (линии) связи, включая кабельные системы, используемые информационными системами персональных данных;

сети передачи данных, не выходящие за пределы контролируемой зоны информационной системы персональных данных;

помещения, в которых обрабатываются персональные данные посредством информационных систем персональных данных и располагаются компоненты информационной системы персональных данных;

помещения, в которых расположены ресурсы информационных систем персональных данных, имеющие отношение к криптографической защите персональных данных.

8. К средствам вычислительной техники, участвующей в обработке персональных данных посредством информационных систем персональных данных, относятся:

автоматизированные рабочие места пользователей с различными уровнями доступа (правами) – программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к информационной системе персональных данных и предназначенный для локальной обработки информации;

терминальная станция – программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к информационной системе персональных данных, но не предназначенный для локальной обработки информации;

серверное оборудование – программно-аппаратный комплекс, предназначенный для обработки и консолидированного хранения данных информационных систем персональных данных. Серверное оборудование может быть представлено автоматизированными рабочими местами пользователей, выполняющими функции сервера;

сетевое и телекоммуникационное оборудование, используемое для информационного обмена между серверным оборудованием, автоматизированным рабочим местом пользователя, терминальными станциями (коммутаторы, маршрутизаторы и другое);

общесистемное программное обеспечение (операционные системы физических серверов, виртуальных серверов, автоматизированных рабочих мест).

9. Ввод персональных данных в информационные системы персональных данных в исполнительных органах и организациях

осуществляется как с бумажных, так и с электронных носителей информации. Персональные данные хранятся и (или) передаются третьим лицам как в электронном, так и в бумажном виде.

IV. Информационные системы персональных данных

10. Обработка персональных данных в информационной системе персональных данных осуществляется с соблюдением положений, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», и принятых в соответствии с ним нормативных правовых актов. Перечень обрабатываемых персональных данных в информационной системе персональных данных соответствует целям их обработки и не является избыточным.

11. Информационные системы персональных данных подразделяются на:

информационные системы персональных данных, операторами которых являются исполнительные органы и организации;

информационные системы персональных данных, эксплуатируемые исполнительными органами и организациями, но не в качестве их операторов.

12. В зависимости от принадлежности и количества субъектов персональных данных информационные системы персональных данных подразделяются на:

персональные данные сотрудников оператора численностью более 100 тыс. человек;

персональные данные сотрудников оператора численностью менее 100 тыс. человек;

персональные данные лиц, не являющихся сотрудниками оператора, численностью более 100 тыс. человек;

персональные данные лиц, не являющихся сотрудниками оператора, численностью менее 100 тыс. человек.

13. Для всех категорий персональных данных информационных систем персональных данных, указанных в пунктах 12, 13 настоящего Положения, необходимо обеспечивать следующие характеристики безопасности:

конфиденциальность;

целостность;

доступность.

При этом должна сохраняться возможность модификации и передачи персональных данных.

V. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

14. Видами актуальных угроз безопасности для информационных систем персональных данных, указанных в разделе IV настоящего Положения, являются:

угроза утечки информации;

угроза несанкционированного доступа;

угроза несанкционированной модификации (искажения);

угроза несанкционированной подмены;

угроза удаления информационных ресурсов;

угроза отказа в обслуживании;

угроза ненадлежащего (нецелевого) использования;

угроза нарушения функционирования (работоспособности);

угроза получения информационных ресурсов из недоверенного или скомпрометированного источника;

угроза распространения противоправной информации;

угроза несанкционированного массового сбора информации.