ПРАВИТЕЛЬСТВО ПЕНЗЕНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

2 апреля 2021 г. № 164-пП

г.Пенза

**О внесении изменений
в постановление Правительства
Пензенской области от 20.04.2017 № 192-пП
(с последующими изменениями)**

Руководствуясь Законом Пензенской области от 22.12.2005 № 906-ЗПО "О Правительстве Пензенской области" (с последующими изменениями), Правительство Пензенской области **п о с т а н о в л я е т:**

1. Внести в постановление Правительства Пензенской области от 20.04.2017 № 192-пП "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Пензенской области" (с последующими изменениями) (далее - постановление) следующие изменения:

1.1. Дополнить приложение №1 "Перечень угроз безопасности персональных данных в информационных системах персональных данных" к приложению "Актуальные угрозы безопасности персональных данных при обработке в информационных системах персональных данных" к постановлению пунктами 7.34, 8.87, 8.88, 8.89, 8.90, 8.91, 8.92, 8.93, 8.94, 8.95, 8.96, 11.17, 17.14, 17.15, 19.21, 22.15 следующего содержания:

"7.34	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования "мастер-кодов" (инженерных паролей)	Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение;
8.87	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом; Внешний нарушитель со средним потенциалом; Внутренний нарушитель со средним потенциалом	Средство вычислительной техники, мобильное устройство

8.88	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом	Аппаратное устройство
8.89	Угроза перехвата управления информационной системой	Внутренний нарушитель со средним потенциалом	Инфраструктура информационных систем
8.90	Угроза обхода многофакторной аутентификации	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя
8.91	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Внешний нарушитель со средним потенциалом	Программное обеспечение (программы)
8.92	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Внешний нарушитель со средним потенциалом	Программное обеспечение (программы)
8.93	Угроза раскрытия информации о модели машинного обучения	Внешний нарушитель с высоким потенциалом; Внутренний нарушитель со средним потенциалом	Программное обеспечение (программы), использующее машинное обучение; модели машинного обучения
8.94	Угроза хищения обучающих данных	Внешний нарушитель со средним потенциалом; Внутренний нарушитель со средним потенциалом	Программное обеспечение (программы), использующее машинное обучение; обучающие данные машинного обучения
8.95	Угроза модификации модели машинного обучения путем искажения ("отравления") обучающих данных	Внешний нарушитель с высоким потенциалом; Внутренний нарушитель со средним потенциалом	Программное обеспечение (программы), использующее машинное обучение; модели машинного обучения; обучающие данные машинного обучения

8.96	Угроза подмены модели машинного обучения	Внутренний нарушитель с высоким потенциалом	Программное обеспечение (программы), использующее машинное обучение; модели машинного обучения;
11.17	Угроза нарушения функционирования ("обхода") средств, реализующих технологии искусственного интеллекта	Внешний нарушитель с высоким потенциалом; Внутренний нарушитель со средним потенциалом	Программное обеспечение (программы), реализующие технологии искусственного интеллекта;
17.14	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Внутренний нарушитель с высоким потенциалом	Аппаратное устройство, микропрограммное, системное и прикладное программное обеспечение
17.15	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внутренний нарушитель со средним потенциалом; Внешний нарушитель со средним потенциалом	Информационная система, файлы;
19.21	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение;
22.15	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Внутренний нарушитель со средним потенциалом	Программное обеспечение, каналы связи (передачи) данных.

2. Исполнительным органам государственной власти Пензенской области и подведомственным им организациям :

2.1. дополнить (при необходимости) Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых исполнительными органами государственной власти Пензенской области и подведомственных им организациях информационных системах персональных данных, в течение трех месяцев с момента официального опубликования настоящего постановления;

2.2. при дополнении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых исполнительными органами государственной власти Пензенской области и подведомственных им организациях информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Правительства Пензенской области, координирующего вопросы информатизации.

Временно исполняющий обязанности
Губернатора Пензенской области О.В. Мельниченко