ПРАВИТЕЛЬСТВО ПЕНЗЕНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от 22 июня 2018 г. № 337-пП

г.Пенза

О внесении изменений в постановление Правительства Пензенской области от 20.04.2017 № 192-пП

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" (далее - постановление) следующие изменения:

1.1. Дополнить приложение № 1 "Актуальные угрозы безопасности персональных данных при обработке в информационных системах персональных данных" к постановлению пунктами 2.6, 3.18, 5.4, 5.5, 5.6, 6.7, 6.8, 6.9, 6.10, 6.11, 7.30, 7.31, 7.32, 7.33, 8.81, 8.82, 8.83, 8.84, 8.85, 8.86, 10.21, 10.22, 10.23, 10.24, 17.13, 19.16, 19.17, 19.18, 19.19, 19.20, 20.35, 20.36, 21.5 следующего содержания:

"2.6	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Внешний нарушитель с высоким потенциалом	Мобильное устройство (аппаратное устройство)";
"3.18	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Внешний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение";
"5.4	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство
5.5	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение,

			системное программное обеспечение
5.6	Угроза несанкционированного использования привилегированных функций мобильного устройства	Внешний нарушитель с высоким потенциалом	Мобильное устройство";
"6.7	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Внешний нарушитель с низким потенциалом	Средство защиты информации
6.8	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель с низким потенциалом	Аппаратное средство
6.9	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Внешний нарушитель с высоким потенциалом	Аппаратное устройство
6.10	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования "мастер-кодов" (инженерных паролей)	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение
6.11	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внутренний нарушитель с низким потенциалом Внутренний нарушитель со средним потенциалом Внешний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	Средство вычислительной техники, мобильное устройство";
"7.30	Угроза перехвата одноразовых паролей в режиме реального времени	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение
7.31	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Внешний нарушитель со средним потенциалом	Мобильное устройство и запущенные на нем приложения (программное обеспечение, аппаратное устройство)
7.32	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Внешний нарушитель со средним потенциалом	Данные пользователя мобильного устройства (аппаратное устройство)
7.33	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Внешний нарушитель со средним потенциалом	Аппаратное устройство";
"8.81	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Внутренний нарушитель со средним потенциалом Внешний нарушитель с высоким потенциалом	Программное обеспечение автоматизи-рованной системы управления

			технологи-ческими процессами
8.82	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Средство защиты информации
8.83	Угроза несанкционированного воздействия на средство защиты информации	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	Средство защиты информации
8.84	Угроза подмены программного обеспечения	Внутренний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение
8.85	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение
8.86	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Внешний нарушитель со средним потенциалом	Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)";
"10.21	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение
10.22	Угроза несанкционированного использования системных и сетевых утилит	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Системное программное обеспечение
10.23	Угроза несанкционированной модификации защищаемой информации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Объекты файловой системы

10.24	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение";
"17.13	Угроза маскирования действий вредоносного кода	Внешний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение";
"19.16	Угроза использования уязвимых версий программного обеспечения	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение
19.17	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Внешний нарушитель с высоким потенциалом	Стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство)
19.18	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)
19.19	Угроза несанкционированной установки приложений на мобильные устройства	Внешний нарушитель со средним потенциалом	Мобильные устройства (аппаратное устройство, программное обеспечение)
19.20	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	Программное обеспечение";
"20.35	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Внешний нарушитель со средним потенциалом	Информационные ресурсы, объекты файловой системы
20.36	Угроза хищения аутентификационной информации из временных файлов cookie	Внешний нарушитель со средним потенциалом	Информация, хранящаяся на компьютере во временных файлах (программное обеспечение)";

"21.5	Угроза отказа подсистемы обеспечения температурного режима	Внутренний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлажденного воздуха в ЦОД, программируемые логические контроллеры, распределенные системы контроля, управленческие системы и другие программные средства контроля".

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

2.1. Дополнить (при необходимости) угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных системах персональных данных, в течение трех месяцев с момента официального опубликования настоящего постановления.

2.2. При дополнении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Настоящее постановление опубликовать в газете "Пензенские губернские ведомости" и разместить (опубликовать) на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru) и на официальном сайте Правительства Пензенской области в информационно-телекоммуникационной сети "Интернет".

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

Губернатор
Пензенской области И.А. Белозерцев