ПРАВИТЕЛЬСТВО ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 14.09.2016 г. № 498-П

Челябинск

О Перечне угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Челябинской области, Аппарате Губернатора и Правительства Челябинской области, аппарате Уполномоченных по правам человека, правам ребенка, защите прав предпринимателей в Челябинской области, при осуществлении ими соответствующих видов деятельности

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» и частью 2 статьи 1 Закона Челябинской области «О нормативных правовых актах Челябинской области, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных»

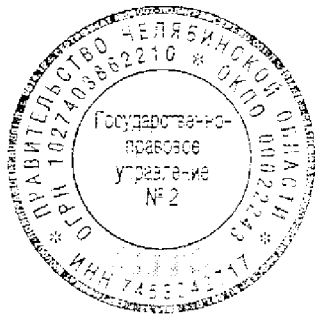
Правительство Челябинской области ПОСТАНОВЛЯЕТ:

1. Определить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Челябинской области, Аппарате Губернатора и Правительства Челябинской области, аппарате Уполномоченных по правам человека, правам ребенка, защите прав предпринимателей в Челябинской области, при осуществлении ими соответствующих видов деятельности (прилагается).

2. Руководителям органов исполнительной власти Челябинской области обеспечить принятие нормативных правовых актов, определяющих угрозы безопасности персональных данных при их обработке в информационных

системах персональных данных, эксплуатируемых в подведомственных учреждениях, при осуществлении ими соответствующих видов деятельности.

3. Настоящее постановление подлежит официальному опубликованию.

Председатель
Правительства Челябинской области  Б.А. Дубровский

ПРИЛОЖЕНИЕ
к постановлению Правительства
Челябинской области
от 14.09. 2016 г. № 498-П

Перечень
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Челябинской области, Аппарате Губернатора и Правительства Челябинской области, аппарате Уполномоченных по правам человека, правам ребенка, защите прав предпринимателей в Челябинской области, при осуществлении ими соответствующих видов деятельности

№ п/п	Наименование угрозы
I. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Челябинской области, Аппарате Губернатора и Правительства Челябинской области, аппарате Уполномоченных по правам человека, правам ребенка, защите прав предпринимателей в Челябинской области, при осуществлении ими соответствующих видов деятельности (далее именуются – угрозы безопасности персональных данных), определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю для информационных систем персональных данных обеспечения типовой деятельности	
1.	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой
2.	Угрозы разглашения пользовательских имен и паролей
3.	Угрозы, связанные с расширением привилегий пользователей
4.	Угрозы, связанные с возможностью внедрения операторов SQL
5.	Угрозы использования информации идентификации/аутентификации, заданной по умолчанию
6.	Угрозы несанкционированного копирования защищаемой информации
7.	Угрозы внедрения вредоносных программ
8.	Угрозы наличия механизмов разработчика
9.	Угрозы «Анализ сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации
10.	Угрозы сканирования, направленные на выявление типа операционной системы, сетевых адресов рабочих станций, открытых

	портов и служб, открытых соединений и другого
11.	Угрозы выявления паролей
12.	Угрозы получения несанкционированного доступа путем подмены доверенного объекта
13.	Угрозы типа «Отказ в обслуживании»
14.	Угрозы удаленного запуска приложений
15.	Угрозы несанкционированного отключения средств защиты информации
16.	Угрозы, связанные с недостаточной квалификацией обслуживающего информационные системы персональных данных (далее именуются – ИСПДн) персонала
17.	Угрозы непреднамеренного или преднамеренного вывода из строя технических средств
18.	Угрозы надежности технических средств и коммуникационного оборудования
19.	Угрозы утраты носителей информации
20.	Угрозы легитимности использования программного обеспечения
21.	Угрозы достаточности и качества применяемых средств защиты информации и средств антивирусной защиты
II. Угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю для информационных систем персональных данных обеспечения специальной деятельности	
22.	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой
23.	Угрозы использования информации идентификации/аутентификации, заданной по умолчанию
24.	Угрозы несанкционированного копирования защищаемой информации
25.	Угрозы внедрения вредоносных программ
26.	Угрозы наличия механизмов разработчика
27.	Угрозы утраты носителей информации
28.	Угрозы, связанные с расширением привилегий пользователей
29.	Угрозы, связанные с возможностью внедрения операторов SQL
30.	Угрозы «Анализ сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации
31.	Угрозы, связанные с анализом сетевого трафика между компонентами информационной системы с целью получения аутентификационной информации
32.	Угрозы сканирования, направленные на выявление типа операционной системы, сетевых адресов рабочих станций, открытых портов и служб, топологии сети, открытых соединений и другого

33.	Угрозы выявления паролей
34.	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
35.	Угрозы подмены доверенного объекта
36.	Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях
37.	Угрозы заражения DNS-кеша
38.	Угрозы неправомерных действий в каналах связи
39.	Угрозы типа «Отказ в обслуживании»
40.	Угрозы удаленного запуска приложений
41.	Угрозы непреднамеренного или преднамеренного вывода из строя технических средств и средств защиты информации
42.	Угрозы несанкционированного отключения средств защиты информации
43.	Угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала
44.	Угрозы надежности технических средств и коммуникационного оборудования
45.	Угрозы легитимности использования общесистемного программного обеспечения
46.	Угрозы достаточности и качества применяемых средств защиты информации и средств антивирусной защиты
47.	Угрозы совершения атак на монитор виртуальных машин из физической сети
48.	Угрозы совершения атаки с виртуальной машины на другую виртуальную машину
49.	Угрозы совершения атаки на систему управления виртуальной инфраструктурой
50.	Угрозы выхода процесса за пределы виртуальной машины
51.	Угрозы нарушения изоляции пользовательских данных внутри виртуальной машины
52.	Угрозы неконтролируемого копирования данных внутри хранилища больших данных
53.	Угрозы неконтролируемого уничтожения информации хранилищем больших данных
III. Угрозы безопасности персональных данных для информационных систем персональных данных обеспечения типовой и специальной деятельности, установленные дополнительно согласно требованиям Федеральной службы безопасности Российской Федерации	
54.	Угрозы внесения несанкционированных изменений в средства криптографической защиты информации (далее именуются – СКЗИ) и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, в совокупности

	представляющие среду функционирования СКЗИ (далее именуется – СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований
55.	Угрозы внесения несанкционированных изменений в документацию на СКЗИ и компоненты СФ
56.	Угрозы атаки на персональные и все возможные данные, передаваемые в открытом виде по каналам связи
57.	Угрозы получения из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть Интернет) информации об информационной системе, в которой используются СКЗИ
58.	Угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны автоматизированных систем (далее именуются – АС) и программного обеспечения (далее именуется – ПО), включая аппаратные и программные компоненты АС и ПО, а также специально разработанных АС и ПО
59.	Угрозы использования на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами; каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ
60.	Угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети
61.	Угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ