ЗАКОНОДАТЕЛЬНОЕ СОБРАНИЕ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

18.08.2016 499

от _____ № _____

Челябинск

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Законодательного Собрания Челябинской области

Законодательное Собрание Челябинской области ПОСТАНОВЛЯЕТ:

1. В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Законодательного Собрания Челябинской области (приложение).

2. Установить, что указанные угрозы безопасности персональных данных учитываются при разработке частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных Законодательного Собрания Челябинской области.

Председатель
Законодательного Собрания ОБЩИЙ ОТДЕЛ В.В. Мякуш

Приложение
к постановлению
Законодательного Собрания
Челябинской области
от 18.08.2016 № 499

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Законодательного Собрания Челябинской области

№ п/п	Наименование угрозы
1	2
I. Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю для информационных систем персональных данных Законодательного Собрания Челябинской области (далее – информационные системы персональных данных)	
1	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа, выявление паролей
2	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода (вывода), перехват управления загрузкой
3	Угрозы восстановления аутентификационной информации
4	Угрозы удаления аутентификационной информации
5	Угрозы использования информации идентификации и (или) аутентификации, заданной по умолчанию
6	Угрозы неправомерных действий в каналах связи
7	Угрозы обнаружения открытых портов и идентификации привязанных к ним сетевых служб, обнаружения хостов, топологии вычислительной сети
8	Угрозы перехвата данных, передаваемых по вычислительной сети
9	Угрозы использования слабостей протоколов сетевого или локального обмена данными
10	Угрозы перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
11	Угрозы получения предварительной информации об объекте защиты
12	Угрозы определения типов объектов защиты
13	Угрозы преодоления физической защиты, связанные с ошибками персонала
14	Угрозы несанкционированного восстановления удаленной защищаемой информации

1	2
15	Угрозы отказа внешних источников энергоснабжения
16	Угрозы надежности технических средств и коммуникационного оборудования
17	Угрозы информации, реализуемые с применением вредоносных программ
18	Угрозы достаточности применения средств антивирусной защиты
19	Угрозы информации, связанные с ошибками кода программного обеспечения, допущенными при его проектировании и разработке
20	Угрозы, связанные с недостаточной квалификацией обслуживающего персонала
21	Угроза невозможности восстановления сессии работы компьютера при выводе его из промежуточных состояний питания
22	Угрозы, связанные с расширением привилегий пользователей
23	Угрозы несанкционированного копирования защищаемой информации
24	Угрозы утраты, подлога носителей информации
25	Угрозы несогласованности политик безопасности
II. Актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных согласно требованиям Федеральной службы безопасности Российской Федерации	
26	Угрозы создания способов, подготовки и проведения атак за пределами контролируемой зоны в процессе эксплуатации средств криптографической защиты информации
27	Угрозы создания способов, подготовки и проведения атак на различных этапах жизненного цикла средств криптографической защиты информации, в том числе внесения изменений в документацию на средства криптографической защиты информации и компоненты среды их функционирования на этапах разработки (модернизации), производства, хранения, транспортировки средств криптографической защиты информации
28	Угрозы создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа средств криптографической защиты информации
29	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 информационных системах персональных данных, в которых используются средства криптографической защиты информации
30	Угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы персональных данных, в которых используются средства криптографической защиты информации, имеют выход в эти сети
31	Угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны аппаратных средств и программного обеспечения из состава

1	2
	средств информационных систем персональных данных, применяемых на местах эксплуатации средств криптографической защиты информации
32	Угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны аппаратных средств и программного обеспечения, включая аппаратные и программные компоненты средств криптографической защиты информации и среды их функционирования
33	Угрозы проведения атак при нахождении в пределах контролируемой зоны