АДМИНИСТРАЦИЯ КУРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 06.08.2020 № 801-па

г. Курск

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов государственной власти Курской области

В соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Администрация Курской области ПОСТАНОВЛЯЕТ:

Утвердить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов государственной власти Курской области.

И.о. Губернатора
Курской области А.Б. Смирнов

Комитет административного обеспечения Администрации Курской области
Отдел делопроизводства

311155 945109

УТВЕРЖДЕН
постановлением Администрации
Курской области
от 06.07.2020 № 801-па

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов государственной власти Курской области

1. Угроза деструктивного изменения конфигурации/среды окружения программ.
2. Угроза доступа к защищаемым файлам с использованием обходного пути.
3. Угроза загрузки нештатной операционной системы.
4. Угроза использования информации идентификации/ аутентификации, заданной по умолчанию.
5. Угроза использования механизмов авторизации для повышения привилегий.
6. Угроза использования слабостей протоколов сетевого/локального обмена данными.
7. Угроза некорректного использования функционала программного обеспечения.
8. Угроза неправомерного ознакомления с защищаемой информацией.
9. Угроза несанкционированного восстановления удалённой защищаемой информации.
10. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.
11. Угроза несанкционированного доступа к аутентификационной информации.
12. Угроза несанкционированного доступа к виртуальным каналам передачи.
13. Угроза несанкционированного изменения аутентификационной информации.
14. Угроза несанкционированного копирования защищаемой информации.
15. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
16. Угроза обнаружения хостов.
17. Угроза обхода некорректно настроенных механизмов аутентификации.

18. Угроза определения топологии вычислительной сети.

19. Угроза передачи данных по скрытым каналам.

20. Угроза перехвата вводимой и выводимой на периферийные устройства информации.

21. Угроза перехвата данных, передаваемых по вычислительной сети.

22. Угроза повышения привилегий.

23. Угроза подмены доверенного пользователя.

24. Угроза получения предварительной информации об объекте защиты.

25. Угроза заражения компьютера при посещении неблагонадёжных сайтов.

26. Угроза неправомерного шифрования информации.

27. Угроза распространения «почтовых червей».

28. Угроза «фишинга».

29. Угроза несанкционированной модификации защищаемой информации.

30. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.

31. Угроза маскирования действий вредоносного кода.

32. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет.

33. Угроза использования уязвимых версий программного обеспечения.

34. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика.

35. Угроза перехвата информации, передаваемой за пределами контролируемой зоны по защищенным каналам связи.

36. Обобщенные возможности источников атак, признанные актуальными:

– возможности у внешних пользователей самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

– возможности внутреннего нарушителя зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к информационной системе персональных данных и контролю за правильностью обработки информации.