РОССИЙСКАЯ ФЕДЕРАЦИЯ
ПРАВИТЕЛЬСТВО
РЕСПУБЛИКИ ХАКАСИЯ

РОССИЯ ФЕДЕРАЦИЯЗЫ
ХАКАС РЕСПУБЛИКАНЫҢ
ПРАВИТЕЛЬСТВОЗЫ

ПОСТАНОВЛЕНИЕ

от 11.08. 2017 г. № 410

г. Абакан

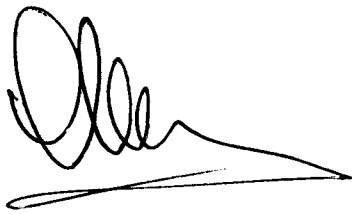
Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами государственной власти Республики Хакасия

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Республики Хакасия, подведомственных им учреждениях и предприятиях, Правительство Республики Хакасия ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами государственной власти Республики Хакасия (далее – Перечень).

2. Рекомендовать государственным органам Республики Хакасия и органам местного самоуправления в Республике Хакасия при разработке нормативных правовых актов, в которых определяются угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых ими при осуществлении соответствующих видов деятельности, руководствоваться указанным в пункте 1 настоящего постановления Перечнем.

Исполняющий обязанности Главы
Республики Хакасия – Председателя
Правительства Республики Хакасия



О. Нам

Приложение

УТВЕРЖДЕН
постановлением Правительства
Республики Хакасия
от «11» 08 2017 г. № 410

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами государственной власти Республики Хакасия

1. Угрозы утечки видовой информации.

2. Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой.

3. Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения несанкционированного доступа программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.).

4. Угрозы внедрения вредоносных программ (вирусов).

5. Угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации.

6. Угрозы сканирования, направленные на выявление типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений и другое.

7. Угрозы типа «Отказ в обслуживании».

8. Угрозы типа «Навязывание ложного маршрута сети».

9. Угрозы типа «Внедрение ложного объекта в сети, подмены доверенного объекта сети».

10. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств.

11. Угрозы доступа к информации, ее модификации и уничтожения лицами, не имеющими прав доступа.

12. Угрозы несанкционированного доступа к информации, находящейся на носителях переданных в ремонт или выведенных из эксплуатации.

13. Угрозы несанкционированного доступа к информации по каналам, выходящим за контролируемую зону.

14. Угрозы выявления паролей по сети.

15. Угрозы среды виртуализации.