ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ БУРЯТИЯ

БУРЯАД УЛАСАЙ ЗАСАГАЙ ГАЗАР

П О С Т А Н О В Л Е Н И Е

Т О Г Т О О Л

от 22 февраля 2017 г. № 73

г. Улан-Удэ

Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Республики Бурятия

В соответствии с пунктом 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также в целях совершенствования системы защиты персональных данных в исполнительных органах государственной власти Республики Бурятия Правительство Республики Бурятия **п о с т а н о в л я е т**:

1. Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Республики Бурятия (далее – Перечень).

2. Исполнительным органам государственной власти Республики Бурятия руководствоваться Перечнем при разработке частных моделей угроз безопасности персональных данных информационных систем персональных данных исполнительных органов государственной власти Республики Бурятия с учетом их назначения, условий и особенностей функционирования.

3. Настоящее постановление вступает в силу со дня его подписания.

Исполняющий обязанности Председателя Правительства Республики Бурятия **А. Чепик**

Проект представлен Администрацией Главы и Правительства
тел. 21-20-47

лн1

УТВЕРЖДЕН
постановлением Правительства
Республики Бурятия
от 22.02.2017 № 73

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Республики Бурятия

1. Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Республики Бурятия (далее – актуальные угрозы безопасности ИСПДн ИОГВ РБ), разработан в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

2. К основным видам актуальных угроз безопасности ИСПДн ИОГВ РБ относятся:

2.1. Угрозы утечки по техническим каналам.

2.1.1. Угрозы утечки видовой информации.

2.2. Угрозы несанкционированного доступа к информации (далее - НСД).

2.2.1. Угрозы НСД в ИСПДн путем физического доступа.

2.2.2. Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств.

2.2.3. Угрозы НСД в виртуальной среде.

2.2.4. Угрозы НСД в ИСПДн, реализуемые по локальной сети:

- угроза «Сканирование сети»;
- угроза «Анализ сетевого трафика» с перехватом передаваемой по локальной сети информации;
- угрозы выявления паролей внутри сети;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

2.2.5. Угрозы НСД в ИСПДн, реализуемые с использованием протоколов межсетевого взаимодействия:

- угрозы «Анализа сетевого трафика» при межсетевом взаимодействии;
- угроза «Сканирование сети»;
- угрозы подмены доверенного объекта при межсетевом взаимодействии;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных во внешних сетях;
- угрозы выявления паролей при межсетевом взаимодействии;
- угрозы удаленного запуска приложений при межсетевом взаимодействии;

- угрозы внедрения вредоносных программ при межсетевом взаимодействии.

2.3. Угрозы, возникающие при передаче данных по каналам связи:

- угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых средствами криптографической защиты информации (далее - СКЗИ) персональных данных или создания условий для этого (далее - атака) при нахождении в пределах контролируемой зоны;

- угрозы проведения атаки на этапе эксплуатации средств криптографической информации на следующие объекты:

- документацию на СКЗИ и компоненты среды функционирования (далее - СФ) СКЗИ;

- помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

- угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

- угрозы использования штатных средств ИСПДн, ограниченного мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

- угрозы физического доступа к СВТ, на которых реализованы СКЗИ и СФ;

- угрозы возможностей воздействия на аппаратные компоненты СКЗИ и СФ, ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

3. Угрозы безопасности, актуальные для разноплановых систем, которые могут быть нейтрализованы только с помощью СКЗИ, необходимо дополнительно учитывать при разработке частных моделей угроз в соответствии с разделами Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных ФСБ России 31 марта 2015 года № 149/7/2/6-432.