**ГЛАВА ЧЕЧЕНСКОЙ РЕСПУБЛИКИ**

# ПЕРЕЧЕНЬ ПОРУЧЕНИЙ

от 14.11.2018 года № 01-27 пп

1. Руководителю Администрации Главы и Правительства Чеченской Республики А.М. Израйилову провести структурные изменения в Администрации Главы и Правительства Чеченской Республики, переименовав Управление защиты государственной тайны Администрации Главы и Правительства Чеченской Республики, в Управление технической защиты информации, противодействия иностранным техническим разведкам и государственной тайны Администрации Главы и Правительства Чеченской Республики, а также добавить штатные единицы в вышеназванное Управление.

Срок исполнения: до 14 декабря 2018 года.

2. Рекомендовать руководителям органов государственной власти Чеченской Республики, органов местного самоуправления и организаций Чеченской Республики:

2.1. Обеспечить при проведении работ по технической защите информации, содержащей сведения, составляющие государственную тайну, в органах государственной власти Чеченской Республики, органах местного самоуправления и организациях Чеченской Республики выполнение требований режима секретности в соответствии с требованиями «Инструкции по обеспечению режима секретности в Российской Федерации», утвержденной постановлением Правительства Российской Федерации от 5 января 2004 года № 3-1, Требований по технической защите информации, содержащей сведения, составляющие государственную тайну, утвержденных приказом ФСТЭК России от 20 октября 2016 года № 025.

Срок исполнения: до 31 января 2019 года.

2.2. Обеспечить принятие дополнительных мер по защите информации, не содержащей сведений, составляющих государственную тайну, в информационных системах, в том числе предназначенных для взаимодействия с сетью «Интернет», органов государственной власти Чеченской Республики, органов местного самоуправления и организаций Чеченской Республики в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17, обратив особое внимание на:

- необходимость оперативного обновления применяемого в информационных системах программного обеспечения, включая средства защиты периметра информационных систем, с целью устранения их уязвимостей;

- своевременность выявления инцидентов безопасности информации в информационных системах и реагирования на них.

Срок исполнения: до 1 января 2019 года.

2.3. В целях реализации положений Федерального закона от 26 июля 2017 года № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" субъектам критической информационной инфраструктуры разработать и утвердить планы мероприятий по реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов, предусмотрев в них в качестве первоочередных следующие мероприятия:

2.3.1. Создание комиссий по категорированию объектов критической информационной инфраструктуры.

Срок исполнения: до 1 января 2019 года.

2.3.2. Разработку перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направление их в ФСТЭК России.

Срок исполнения: до 1 января 2019 года.

2.3.3. Создание (совершенствование созданных) субъектами критической информационной инфраструктуры систем безопасности, включающих, в том числе назначение руководящего должностного лица, ответственного за организацию и контроль обеспечения безопасности значимых объектов критической информационной инфраструктуры, создание (назначение) структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры, а также разработку организационно-распорядительных документов по вопросам обеспечения безопасности критической информационной инфраструктуры.

Срок исполнения: до 1 января 2019 года.

2.3.4. Анализ и при необходимости приведение отраслевых (ведомственных) или локальных актов, регламентирующих вопросы обеспечения информационной безопасности и защиты информации, в соответствие с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ.

Срок исполнения: до 1 января 2019 года.

2.3.5. Проведение категорирования объектов критической информационной инфраструктуры в соответствии с утвержденным перечнем и направление результатов категорирования в ФСТЭК России.

Срок исполнения: до 1 января 2019 года.

2.3.6. Реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, с учетом установленной категорий значимости и особенности их функционирования.

Срок исполнения: до 1 февраля 2019 года.

2.4. Спланировать и провести с работниками, выполняющими функции с использованием значимых объектов критической информационной инфраструктуры, учебные занятия, в ходе которых проинформировать их о действующих требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры и наиболее актуальных угрозах безопасности информации.

Срок исполнения: до 1 февраля 2019 года.

2.5. Обеспечить реализацию первоочередных мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры в соответствии с пунктом 22 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденных приказом ФСТЭК России от 25 декабря 2017 года № 239.

Срок исполнения: постоянно.

2.6. Включать в технические задания на создание (модернизацию) значимых объектов критической информационной инфраструктуры требования по обеспечению их безопасности, установленные пунктом 10 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденных приказом ФСТЭК России от 25 декабря 2017 года № 239.

Срок исполнения: постоянно.

2.7. Проводить на регулярной основе анализ угроз безопасности информации и уязвимостей программного обеспечения, в том числе с учетом угроз и уязвимостей, содержащихся в банке данных угроз безопасности информации (bdu.fstec.ru), и, при необходимости, принимать дополнительные меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Срок исполнения: постоянно.

2.8. Представлять на рассмотрение и согласование в Управление ФСТЭК России по Южному и Северо-Кавказскому федеральным округам проекты нормативных правовых актов органов государственной власти Чеченской Республики устанавливающих актуальные угрозы безопасности персональных данных, подлежащих изданию во исполнение части 5 и 7 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Срок исполнения: до 1 марта 2019 года.

2.9. Организовать разработку и согласование моделей угроз безопасности информации и технических заданий, в части касающейся защиты информации, на создание региональных государственных и муниципальных информационных систем с Управлением ФСТЭК России по Южному и Северо-Кавказскому федеральным округам в соответствии с Требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлениями Правительства Российской Федерации от 6 июля 2015 года № 676, от 1 ноября 2012 года № 1119, приказами ФСТЭК России 11 февраля 2013 года № 17 и от 18 февраля 2013 года № 21.

Срок исполнения: до 1 февраля 2019 года.

2.10. В целях исполнения Указа Президента Российской Федерации от 22 мая 2015 года № 260 «О некоторых вопросах информационной безопасности» продолжить работу по подключению органов государственной власти Чеченской Республики, органов местного самоуправления и находящихся в их ведении государственных информационных систем и информационно-телекоммуникационных сетей к российскому государственному сегменту сети «Интернет», развитию инфраструктуры связи государственных органов Чеченской Республики.

Срок исполнения: до 1 февраля 2019 года.

2.11. Администрации Главы и Правительства Чеченской Республики совместно с ФСТЭК России и ЦССИ ФСО России в Чеченской Республике проработать вопрос создания центра управления и защиты информации при подключении и работе в российском государственном сегменте сети «Интернет».

Срок исполнения: до 1 февраля 2019 года.

2.12. Органам государственной власти Чеченской Республики, органам местного самоуправления и организациям Чеченской Республики осуществлять согласование заявок по закупкам, связанным с защитой информации, с Управлением технической защиты информации, противодействия иностранным техническим разведкам и государственной тайны Администрации Главы и Правительства Чеченской Республики.

Срок исполнения: постоянно.

2.13. Проверочные мероприятия по защите информации уполномочены проводить сотрудники Управления технической защиты информации, противодействия иностранным техническим разведкам и государственной тайны Администрации Главы и Правительства Чеченской Республики в соответствии со своими функциональными и должностными обязанностями.

Срок исполнения: постоянно.

2.14. Руководителям органов государственной власти Чеченской Республики, органов местного самоуправления и организаций Чеченской Республики разработать и утвердить Инструкцию по обеспечению информационной

безопасности компьютеров, подключенных к информационным ресурсам сети Интернет с учетом положений распоряжения Руководителя Администрации Главы и Правительства Чеченской Республики от 03 августа 2018 года № 67-ра.

Срок исполнения: до 25 декабря 2018 года.

3. Утвердить план работы Совета по технической защите информации при Главе Чеченской Республики на 2019 год согласно приложению.

Итоговую информацию о результатах проделанной работы по исполнению настоящего протокола представить в адрес Главы Чеченской Республики в срок до 1 апреля 2019 года.

Контроль за исполнением настоящего перечня поручений возложить на Управление защиты государственной тайны Администрации Главы и Правительства Чеченской Республики.

Р.А.Кадыров

Начальник отдела контроля
А.Т. Хачукаева
(8712) 22-36-35