УТВЕРЖДЕНО
приказом государственного автономного
учреждения Республики Коми
«Центр информационных технологий»
от 19.08.2020 № 94
(ПРИЛОЖЕНИЕ № 1)

ПОЛОЖЕНИЕ
об обеспечении информационной безопасности инфраструктуры электронного правительства в Республике Коми

1. Настоящее положение об обеспечении информационной безопасности инфраструктуры электронного правительства в Республике Коми (далее – Положение) разработано во исполнение пункта 2 постановления Правительства Республики Коми от 31 декабря 2010 г. № 506 «О региональном операторе безопасности инфраструктуры электронного правительства в Республике Коми» и определяет цели, задачи и основные направления обеспечения информационной безопасности инфраструктуры электронного правительства в Республике Коми (далее - электронное правительство).

2. Действие настоящего Положения распространяется на органы исполнительной власти Республики Коми, государственные учреждения Республики Коми, а также иные организации, подключенные к государственной информационно-телекоммуникационной сети Республики Коми (далее – ГИТС).

3. Правила и процедуры, направленные на защиту инфраструктуры электронного правительства, определяются оператором безопасности инфраструктуры электронного правительства в политиках информационной безопасности и доводятся до органов государственной власти Республики Коми, государственных учреждений Республики Коми и иных организаций в части их касающейся.

4. Целью обеспечения информационной безопасности инфраструктуры электронного правительства является защита компонентов инфраструктуры электронного правительства от внутренних и внешних угроз информационной безопасности.

5. Задачами обеспечения информационной безопасности инфраструктуры электронного правительства являются:

– Предотвращение неправомерного доступа к информации, обрабатываемой в компонентах инфраструктуры электронного правительства, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

– Недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование компонентов инфраструктуры электронного правительства;

– Обеспечение функционирования компонентов инфраструктуры электронного правительства в условиях воздействия угроз безопасности информации;

– Обеспечение возможности восстановления функционирования компонентов инфраструктуры электронного правительства.

6. Основные направления обеспечения информационной безопасности инфраструктуры электронного правительства:

– Разработка и внедрение политик информационной безопасности и иных организационно-распорядительных документов по обеспечению информационной безопасности инфраструктуры электронного правительства;

– Реализация требований к обеспечению безопасности государственных информационных систем Республики Коми (далее – ГИС), значимых объектов критической информационной инфраструктуры (далее – ЗОКИИ) и инфраструктуры электронного правительства, а также требований к обеспечению их функционирования в соответствии с законодательством Российской Федерации;

– Проектирование систем защиты информации, обрабатываемой в ГИС и на ЗОКИИ;

– Проведение аттестационных испытаний объектов информатизации, входящих в электронное правительство, по требованиям безопасности информации, определенных законодательством Российской Федерации;

– Организация обработки и хранения государственных информационных ресурсов органов государственной власти Республики Коми в контролируемых центрах обработки данных с соблюдением установленных требований законодательством Российской Федерации к информационной безопасности;

– Разработка, внедрение, исследование эффективности, сопровождение средств и комплексов технической защиты информации, содержащейся в ГИС, ЗОКИИ и иных информационных системах органов государственной власти Республики Коми и государственных учреждений Республики Коми от несанкционированного доступа;

– Внедрение в органах государственной власти Республики Коми и государственных учреждениях Республики Коми средств защиты информации, прошедших оценку соответствия (в том числе в установленных случаях сертификацию), в порядке, установленном законодательством Российской Федерации;

– Контроль принятых мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в органах государственной власти Республики Коми и государственных учреждениях Республики Коми и обеспечения безопасности ЗОКИИ;

– Выявление компьютерных атак и уязвимостей информационной безопасности ГИС, инфраструктуры электронного правительства, центров обработки данных ГИТС, локальных вычислительных сетей и ЗОКИИ в соответствии с требованиями законодательства Российской Федерации;

– Мониторинг и передача сведений об инцидентах в Национальный координационный центр по компьютерным инцидентам в соответствии с требованиями законодательства Российской Федерации;

– Консультационная и информационная поддержка организаций-участников электронного правительства в области выполнения обеспечения информационной безопасности электронного правительства, включая расследование инцидентов информационной безопасности, устранение уязвимостей информационной безопасности и повышение осведомленности пользователей ГИТС в области выявления и противодействия актуальным компьютерным атакам;

– Обучение и повышение квалификации специалистов, работающих в области информационной безопасности, защиты информации, обеспечения безопасности ЗОКИИ.