ДЕПАРТАМЕНТ ИНФОРМАТИЗАЦИИ И СВЯЗИ КРАСНОДАРСКОГО КРАЯ
Красная ул., д. 35, г. Краснодар, 350014
Тел. (861) 214-22-00, факс (861) 267-94-56
E-mail: dis@krasnodar.ru

07.12.2020 № 86-07.2-04-5749/20

На № _____ от _____

Руководителям органов исполнительной власти Краснодарского края и структурных подразделений администрации Краснодарского края (по списку)

Главам городских округов и муниципальных районов Краснодарского края

Администрация города Сочи
104220 571101
07.02-12/23422 от 08/12/2020

О противодействии угрозам информационной безопасности

Департамент информатизации и связи Краснодарского края (далее – департамент) сообщает о росте количества компьютерных атак, связанных с попытками получения злоумышленниками несанкционированного доступа к объектам информационной инфраструктуры Российской Федерации, государственным информационным системам и ресурсам.

С целью минимизации возможности реализации угроз информационной безопасности, направленных на информационные ресурсы исполнительных органов государственной власти и органов местного самоуправления муниципальных образований Краснодарского края, а также подведомственных учреждений, департамент просит обеспечить реализацию мер по защите информации согласно приложению.

Также департамент просит довести вышеуказанные рекомендации до подведомственных учреждений с целью их реализации.

Приложение: на 2 л. в 1 экз.

Временно исполняющий обязанности руководителя департамента

Подлинник электронного документа, подписанного электронной подписью, хранится в системе электронного документооборота администрации Краснодарского края
Сертификат 576324DBB0B19D229AEC56D59B0BDADA3FF64CB3
Владелец **Бережной Денис Сергеевич**
Действителен с 06.11.2019 по 06.02.2021

Д.С. Бережной

Клименко Ксения Викторовна
+7 (861) 214-22-07

Приложение
к письму департамента
информатизации
и связи Краснодарского края
от _____ № _____

Рекомендации по защите информационных ресурсов и систем органов власти и управлений Краснодарского края, подведомственных им учреждений

В интересах недопущения реализации угроз безопасности РФ в информационной сфере необходимо:

обеспечить использование и регулярное обновление штатных средств антивирусной защиты;

обеспечить регулярное обновление используемого программного обеспечения;

для предотвращения возможных компьютерных атак, направленных на эксплуатацию уязвимостей, определить и заблокировать порты, протоколы и сервисы, не используемые для функционирования процессов;

использовать двухфакторную авторизацию при удаленном доступе в сеть;

запретить доступ с помощью сторонних сервисов, которые подключаются через промежуточные серверы и самостоятельно проводят авторизацию и аутентификацию;

включить политики безопасности, которые ограничивают доступ к ресурсам из черных списков;

заблокировать доступ на потенциально вредоносные домены, добавить возможность фильтрации веб-содержимого;

обеспечить ведение журналирования действий пользователей с максимально возможным периодом хранения журналов;

настроить период неактивных удаленных подключений пользователей с требованием повторной аутентификации;

удалить неиспользуемые учетные записи и группы пользователей на средствах вычислительной техники;

организовать и осуществить в постоянном режиме антивирусную проверку сообщений электронной почты;

ограничить или прекратить использование небезопасных протоколов "ftp", "telnet", и других, передающих авторизованные и аутентификационные данные пользователей в открытом виде;

организовать контроль за подключением внешних устройств, в том числе машинных носителей информации;

обновить пароли всех пользователей в соответствии с парольной политикой;

настроить и осуществить автоматическое резервное копирование информационных систем;

осуществить хранение входящего и исходящего сетевого трафика на всех сетевых сегментах с максимально возможным периодом хранения, но не менее, чем за последние 24 часа;

привести в актуальное состояние имеющиеся планы, инструкции и руководства по реагированию на компьютерные инциденты;

запретить использование платформы видеоконференции "Zoom" и её аналогов при осуществлении служебной деятельности.