НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru



# Об угрозах безопасности информации, связанных с пандемией коронавируса (COVID-19.).

ALRT-20200320.1 | 20 марта 2020 г.

TLP: WHITE

| | |
|---|---|
| Актуальность угрозы | Актуально в настоящее время и в ближайшей перспективе. |
| Описание | Поступающие в НКЦКИ сведения свидетельствуют об активном использовании злоумышленниками ситуации вокруг пандемии коронавируса для осуществления широкого спектра вредоносной деятельности.<br>Сведения связанные с этими угрозами можно разделить на два типа:<br>1. Мошенничество. Злоумышленники могут попытаться получить доступ к персональным данным пользователя или завладеть денежными средствами обманным путем.<br>2. Угрозы связанные с удаленным режимом работы. Недостаточная защищенность удаленных рабочих мест может являться причиной возникновения компьютерных инцидентов в корпоративных и ведомственных информационных системах. |
| Рекомендации по противодействию угрозам компьютерной безопасности в период пандемии COVID-19 для граждан: | 1. Проявляйте осторожность при обработке электронных сообщений с темой, вложением или гиперссылкой, связанных с COVID-19. Не раскрывайте личную или финансовую информацию в электронном письме и не отвечайте на запросы о предоставлении этой информации.<br>2. Используйте официальные источники для получения актуальной, основанной на фактах, информации о COVID-19.<br>3. Для предотвращения кражи персональных данных подключайтесь только к проверенным интернет-платформам для проведения видеоконференций, онлайн-обучения, подписок на онлайн-кинотеатры, мобильных приложений для доставки еды и т. д.<br>4. Прежде чем делать пожертвования, проверяйте подлинность благотворительных организаций во избежание кражи денежных средств. |

| | |
|---|---|
| Рекомендации по обеспечению информационной безопасности при удаленном режиме работы: | 1. Убедитесь, что средства антивирусной защиты и межсетевого экранирования надлежащим образом настроены и функционируют на всех узлах системы.<br>2. Проверьте обновление всех сервисов и оборудования, которые используются для удаленного доступа (VPN, устройства сетевой инфраструктуры).<br>3. Используйте удаленный доступ в сеть организации строго с двухфакторной авторизацией.<br>4. Запретите использовать доступ в корпоративную сеть с помощью сторонних сервисов, которые подключаются через промежуточные сервера и самостоятельно проводят авторизацию и аутентификацию.<br>5. Организуйте контроль за подключением внешних устройств, в том числе USB-носителей информации, к устройству, предназначенному для удаленного доступа.<br>6. Задайте ограничение скорости VPN соединений для приоритизации пользователей, которым потребуется более высокая пропускная способность.<br>7. Осуществите сегментирование сети и разделите права доступа.<br>8. Используйте не прямой, а терминальный удаленный доступ в сеть к виртуальному рабочему месту со всеми установленными средствами защиты информации.<br>9. Проверьте, что электронная почта защищена двухфакторной авторизацией. Необходимо обеспечить анализ электронной почты антивирусными средствами.<br>10. Используйте стойкий пароль к управляющей панели роутера и WPA2 шифрование при подключении к сети Интернет с применением Wi-Fi.<br>11. Проверьте наличие и срок ведения журналов удаленных действий пользователей, а также наличие тайм-аута неактивного удаленного подключения с требованием повторной аутентификации.<br>12. Обновите пароли всех пользователей в соответствии с парольной политикой.<br>13. Осуществляйте мониторинг безопасности систем с повышенной бдительностью.<br>14. Приведите в актуальное состояние имеющиеся в организации планы, инструкции и руководства по реагированию на компьютерные инциденты с учётом изменений в инфраструктуре.<br>15. Акцентируйте внимание сотрудников на фишинговых атаках, связанных с тематикой COVID-19. |

16. Проинформируйте сотрудников о необходимости ограничения доступа к удаленному рабочему месту детей, родственников и посторонних лиц, а в случае невозможности – ограничения прав их учетных записей.