\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Мемлекеттік және жергілікті атқарушы органдарға**

(***тізім бойынша***)

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті (*бұдан әрі -Комитет*) қашықтан жұмыс режиміне көшуге байланысты, Қазақстан Республикасының Премьер-Министрі А. У. Маминнің 2020 жылғы 16 наурыздағы №1 хаттамалық тапсырмасына сәйкес **COVID-19 пандемиясы кезеңінде ақпараттық қауіпсіздіктің мынадай өзекті қатерлері болуы мүмкін екендігін хабарлайды**:

* коммерциялық алаяқтық тегін қызметтер санын арттыру: бейнеконференция, онлайн-оқыту, онлайн-кинотеатрларға жазылу, тамақ жеткізу үшін жалған мобильді қосымшалар және т. б.;
* **коммерциялық шпионаж** мақсатында шабуылдар жүргізу қаупін арттыру;
* қаржы саласы қызметкерлеріне мақсатты шабуылдар **санының өсуі**;
* **егде жастағы адамдарға қатысты** алаяқтық белсенділікті арттыру: тауарларды үйге жеткізу, COVID - 19 және т. б. дәрі- дәрмектер мен тестерді ұсыну;
* қашықтан жұмыс режиміне көшкен кезде еңбекақысын төмендететін қызметкерлер санатын пайдалана отырып, **инсайдерлік шабуылдар** санының өсуі;
* **туристік индустрияда** алаяқтық белсенділікті күшейту (*әуе желілерінің, қонақ үйлердің ақшалай қаражатын қайтару орталықтары және т. б.*).

Осыған байланысты, Комитет Group-IB-мен бірлесе отырып, **қауіпсіз қашықтағы жұмысты ұйымдастыру бойынша келесі ұсынымдарды әзірледі:**

* **екі факторлы аутентификациясы бар ұйым желісіне** қашықтағы қатынауды пайдалану.
* корпоративтік желіге кіру үшін аралық серверлер арқылы қосылатын және авторландыру мен аутентификацияны дербес жүргізетін **бөгде сервистерді пайдаланбаңыз.**
* **желіні сегменттеу және кіру құқықтарын бөлу**. Пайдаланушылардың қашықтағы белсенділігі де ұйымның периметрлік қорғаныс құралдарымен жабылуы қажет.
* үй компьютерлерінен жұмыс істеу кезінде корпоративтік ақпараттық жүйелерге **терминалдық қолжетімділікті** немесе ақпаратты қорғаудың барлық орнатылған құралдарымен виртуалды жұмыс орындарын пайдалану ұсынылады.
* **электрондық пошта екі факторлы аутентификациямен** **қорғалғанын** тексеріңіз. Бұдан басқа, зиянды кодты детонациялау үшін оқшауланған ортаға «күмәнді» хаттарды жіберу үшін электрондық поштамен жұмыс істеу жөніндегі шешімді енгізу қажет (*песочница*).
* қашықтан кіру үшін пайдаланылатын барлық сервистер мен жабдықтарды жаңартылған **микробағдарламалардың және қауіпсіздік патчаларының болуына тексеру**. Басқа нұсқа осы сервистерге тек екі факторлы аутентификациямен қорғалған VPN арқылы қол жеткізу болып табылады.
* пайдаланушылардың қашықтағы **іс-әрекеттері журналдарының бар-жоғын және жүргізу мерзімін**, сондай-ақ қайта аутентификациялау талабымен белсенді емес қашықтағы қосылу таймаутының бар-жоғын тексеру.

Сонымен қатар, бұл ақпаратты барлық ведомстволық бағынысты құрылымдар мен ұйымдардың назарына жеткізу қажет.

**Төраға орынбасары Р. Абдикаликов**

*🖍 Мусаибов М.М.*

*🕾 8-(7172)-74-22-22*

*🖅 m.musaibov@mdai.gov.kz*

**Государственным и местным исполнительным органам**

**(*по списку*)**

Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (*далее-Комитет*) сообщает что, в связи с переходом, в соответствии с протокольным поручением Премьер-Министра Республики Казахстан Мамина А.У. от 16 марта 2020 года №1, на удаленный режим работы возможны следующие **актуальные угрозы информационной безопасности в период пандемии COVID-19:**

* увеличение числа мошеннических бесплатных сервисов: платформ для проведения видеоконференций, онлайн-обучения, подписок на онлайн-кинотеатры, фейковых мобильных приложений для доставки еды и т.д.
* повышение риска проведения атак с целью **коммерческого** **шпионажа**.
* рост количества **целевых атак** на сотрудников из финансовой отрасли.
* увеличение мошеннической активности по отношению **к людям пожилого возраста**: доставка товаров на дом, предложения лекарств и тестов на COVID-19 и другое.
* рост числа **инсайдерских атак** с использованием тех категорий сотрудников, которым понижают оклад при переходе на удаленный режим работы.
* усиление мошеннической активности в **туристической индустрии** (*центры возврата денежных средств авиалиний, отелей и т.д*).

В этой связи, Комитетом совместно с Group-IB разработаны следующие **рекомендации по организации безопасной удаленной работы:**

* использовать удаленный доступ в сеть организации **строго с двухфакторной аутентификацией;**
* **не использовать** для доступа в корпоративную сеть **сторонние сервисы**, которые подключаются через промежуточные сервера и самостоятельно проводят авторизацию и аутентификацию;
* **сегментировать сети и разделить права доступа**. Желательно, чтобы даже удаленная активность пользователей покрывалась периметровыми средствами защиты организации;
* при работе с домашних компьютеров рекомендуется использовать **терминальный доступ** к корпоративным информационным системам или виртуальные рабочие места со всеми установленными средствами защиты информации;
* проверить, что **электронная почта защищена двухфакторной аутентификацией**. Кроме того, необходимо внедрить решение по работе с электронной почтой для отправки «сомнительных» писем в изолированнаю среду для детонации вредоносного кода (*песочница*);
* проверить все сервисы и оборудование, которые используются для удаленного доступа, **на наличие обновленных микропрограмм и патчей безопасности**. Другим вариантом является доступ к данным сервисам только через VPN, защищенный двухфакторной аутентификацией;
* проверить наличие и срок ведения **журналов удаленных действий** пользователей, а также наличие таймаута неактивного удаленного подключения с требованием повторной аутентификации.

Кроме того, данную информацию необходимо **довести до сведения** **всех подведомственных структур и организаций.**

**Заместитель Председателя Р. Абдикаликов**

*🖍 Мусаибов М.М.*

*🕾 8-(7172)-74-22-22*

*🖅 m.musaibov@mdai.gov.kz*