Прим. №__

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська , 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

31.03.2020 № 05/01-295 На № _____ від _____

Міністерства, інші державні органи
(згідно зі списком на розсилку)

Щодо підсилення заходів з кіберзахисту

В зв'язку із пандемією вірусу COVID-19 та запровадженням карантину в Україні, на виконання вимог п.6 постанови Кабінету Міністрів України від 11 березня 2020 р. № 211 "Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-26», центральні і місцеві органи виконавчої влади, інші державні органи, органи місцевого самоврядування, підприємства, установи, організації забезпечили організацію роботи для своїх працівників в режимі реального часу через Інтернет.

Однак така форма роботи наражає інформаційно-телекомунікаційні системи та державні інформаційні ресурси, які в них обробляються, на підвищену небезпеку, підвищує ризики кібербезпеки, щонайменше:

виводу цих систем з ладу або неможливості їх штатного функціонування;

несанкціонованого витоку, модифікації та знищення державних інформаційних ресурсів;

несанкціонованого проникнення сторонніх осіб та встановлення виконавчих модулів шкідливого програмного забезпечення, тощо.

Вважаємо за необхідне проінформувати про необхідність вжиття додаткових заходів з кіберзахисту з метою запобігання реалізації зазначених ризиків кібербезпеки по відношенню до державних інформаційних ресурсів та систем в яких вони обробляються при організації віддаленої роботи співробітників. Рекомендуємо ввести додаткові заходи із забезпечення кіберзахисту інформаційно-телекомунікаційних систем міністерства, іншого державного органу, підприємства, установи та організації, які входять до сфери їх управління (далі – установа) наказом, звернувши в ньому увагу, принаймні на необхідність:

визначити всі інформаційно-телекомунікаційні системи (автоматизовані, інформаційні, телекомунікаційні, системи, автоматизовані системи управління технологічними процесами тощо) з якими віддалено мають право працювати

Додаток

Загальні рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи

1. Запровадити управління доступом користувачів та адміністраторів до інформаційних ресурсів, які обробляються в інформаційно-телекомунікаційних системах установи.

1.1 Механізми розподілу прав доступу до інформаційних ресурсів повинен:

охоплювати всі інформаційні ресурси інформаційно-телекомунікаційних систем установи (інформацію, яка зберігається та обробляється в інформаційно-телекомунікаційних системах, технологічну інформацію програмного та апаратного забезпечення інформаційно-телекомунікаційних систем, журнали реєстрації подій тощо);

визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами інформаційно-телекомунікаційних систем установи (читання, модифікація, створення, видалення тощо);

за необхідності також визначати права доступу користувачів та адміністраторів до служб (функцій) інформаційно-телекомунікаційних систем установи.

1.2 За можливості реалізації, в інформаційно-телекомунікаційних системах повинна надаватися перевага централізованому поширенню інформації щодо налаштувань прав та атрибутів доступу, параметрів реєстрації подій, інших параметрів безпеки та системних налаштувань компонентів систем.

2. Ідентифікація та автентифікація користувачів та адміністраторів інформаційно-телекомунікаційних систем установи.

2.1 Користувачі та адміністратори інформаційно-телекомунікаційних систем установи (за необхідності також активні процеси) повинні отримувати доступ до служб (функцій), інформації та компонентів систем в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо). Користувачі та адміністратори повинні використовувати складні паролі, які мають не менше чим 8 символів, цифри та букви в різних регістрах. Змінювати паролі не рідше одного разу на тиждень.

2.2 Засоби інформаційно-телекомунікаційних систем установи повинні надавати можливість ідентифікації операцій користувачів та адміністраторів інформаційно-телекомунікаційних систем та їх протоколювання в журналах реєстрації подій.

2.3 Для надання доступу до служб (функцій) та інформації інформаційно-телекомунікаційних систем установи повинна надаватися перевага використанню багатофакторної автентифікації користувачів та адміністраторів.

співробітники з метою невідкладного впровадження в таких системах заходів із кіберзахисту;

визначити коло працівників, яким надано право віддаленого доступу до інформаційно-телекомунікаційних систем установи, їх права та обов'язки;

заборони віддаленої роботи співробітників установи з системами, в яких обробляються державна таємниця, службова інформація, та автоматизованими системами управління технологічними процесами, а також заборони пересилання та обробки інформації з обмеженим доступом на робочі місця співробітників установи, які працюють віддалено;

невідкладного інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, а також Ситуаційного центру забезпечення кібербезпеки СБУ або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки на інформаційно-телекомунікаційні системи установи.

Віддалена робота співробітників установи з системами, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої визначена в законі, повинна відповідати політиці безпеки інформації, яка прийнята в установі, та вимогам законодавства у сфері захисту інформації.

Одночасно просимо організувати інформування підприємств, установ та організацій які знаходяться у сфері управління установи про необхідність запровадження додаткових заходів із кіберзахисту та надсилаємо у додатку загальні рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи.

Додаток: за текстом, на 9 арк.

Голова Служби Валентин ПЕТРОВ

Вик. Прохольський Р.О. 281-87-54

2.4 В інформаційно-телекомунікаційних системах установи повинні бути заблоковані або змінені облікові записи адміністраторів та їх паролів, встановлені за замовчуванням, в усіх компонентах систем. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні інформаційно-телекомунікаційних систем.

2.5 В інформаційно-телекомунікаційних системах установи повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів в усіх компонентах систем. Під час звільнення, переведення тощо співробітника його обліковий запис повинен бути негайно заблокований, видалений або змінені його права доступу відповідно до нової посади в усіх компонентах інформаційно-телекомунікаційних систем.

2.6 Обладнання (персональні комп'ютери, мобільні пристрої тощо) яке підключається до інформаційно-телекомунікаційних систем установи, повинно бути ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), а також повинні бути вжиті заходи, які унеможливлюють роботу обладнання в системах без відповідної ідентифікації. Повинен бути заборонений доступ до інформаційно-телекомунікаційних систем установи з незареєстрованого та невстановленого обладнання.

2.7 Повинна використовуватись повторна автентифікація користувачів та адміністраторів після певного проміжку часу відсутності активності в сеансі роботи.

3. Реєстрація подій компонентами інформаційно-телекомунікаційних систем установи та їх періодичний аудит.

3.1 Компоненти інформаційно-телекомунікаційних систем установи повинні забезпечити реєстрацію, збереження в електронних журналах та захист від модифікації інформації щонайменше про такі події:

доступ та дії з інформацією, яка зберігається та обробляється в інформаційно-телекомунікаційних системах установи, а також з налаштуваннями програмного та апаратного забезпечення систем, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

реєстрація подій, пов'язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів інформаційно-телекомунікаційних систем;

вхід/вихід користувачів та адміністраторів в/із компонентів інформаційно-телекомунікаційних систем;

невдалі спроби входу користувачів та адміністраторів в інформаційно-телекомунікаційні системи та перевищення граничної кількості спроб введення пароля;

реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах інформаційно-телекомунікаційних систем;

зміна пароля користувача в компонентах інформаційно-телекомунікаційних систем;

реєстрація подій, пов'язаних із зміною конфігураційних налаштувань компонентів інформаційно-телекомунікаційних систем;

спроби здійснення несанкціонованого доступу до ресурсів інформаційно-телекомунікаційних систем;

негативні результати перевірок цілісності даних та програмного і апаратного забезпечення інформаційно-телекомунікаційних систем;

всі дії адміністратора з журналами реєстрації подій (логами) компонентів інформаційно-телекомунікаційних систем та налаштування ним параметрів реєстрації.

Повний перелік подій, які реєструються компонентами інформаційно-телекомунікаційних систем, визначається виходячи із встановленої в інформаційно-телекомунікаційних системах установи політики інформаційної безпеки.

3.2 Журнали реєстрації подій (логи) компонентів інформаційно-телекомунікаційних систем повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнали реєстрації повинні містити інформацію, достатню для встановлення користувача, процесу і мережевого об'єкта, що мали відношення до кожної зареєстрованої події.

3.3 Адміністратори систем повинні проводити періодичний аудит журналів реєстрації подій (логів) компонентів інформаційно-телекомунікаційних систем установи з метою виявлення ймовірних атак чи сканувань та виявлення інших подій, які можуть стосуватися інформаційної безпеки.

3.4 Журнали реєстрації подій (логи) компонентів інформаційно-телекомунікаційних систем установи повинні архівуватися та зберігатися не менше року з моменту їх архівації.

4. Забезпечення мережевого захисту компонентів та інформаційних ресурсів інформаційно-телекомунікаційних систем установи.

4.1 В інформаційно-телекомунікаційних системах установи, у тому числі на віддалених робочих місцях користувачів та адміністраторів систем повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів з (антивірусне програмне забезпечення або інші засоби які включаються до свого складу такі функції з останніми оновленнями своїх антивірусних баз).

4.2 Доступ адміністраторам та користувачам зі своїх робочих місць до компонентів інформаційно-телекомунікаційних систем повинен надаватися виключно з визначених IP-адрес.

4.3 На межі (периметрі) інформаційно-телекомунікаційних систем установи між мережею Інтернет, зовнішніми мережами та системами установи повинні бути встановлені засоби мережевого захисту (IDS, IPS, Firewall тощо), що виконують щонайменше такі функції захисту:

захист від атак "нульового дня" (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

фільтрація трафіку та розмежування доступу між мережею Інтернет, зовнішніми мережами та системами установи за критеріями дозволених та

заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. Блокування трафіку та з'єднань, які не відповідають визначеним критеріям;

захист від атак типу "відмова в обслуговуванні" та інших відомих мережевих атак;

фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію інформаційно-телекомунікаційних систем установи;

захист від несанкціонованого доступу через Інтернет;

балансування навантаження;

маскування структури і мережевих адрес мережі;

завершення з'єднання з вузлом у разі атаки;

здійснення реєстрації подій, що мають відношення до безпеки;

інші функції, визначені політикою безпеки установи.

4.4 Для захисту інформаційно-телекомунікаційних систем установи повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення.

4.5 В інформаційно-телекомунікаційних системах установи необхідно здійснити розподіл систем установи на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.

4.6 Реалізована архітектура інформаційно-телекомунікаційних систем установи повинна надавати можливість розподілу мереж установи на такі частини / зони (віртуальні підмережі):

зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів інформаційно-телекомунікаційних систем;

зона прикладних застосувань інформаційно-телекомунікаційних систем (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

зона сховищ даних інформаційно-телекомунікаційних систем (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone);

зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;

тестова зона (Test-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення інформаційно-телекомунікаційних систем, перед тим як впровадити їх в промислову експлуатацію в інформаційно-телекомунікаційних системах.

Перелік частин / зон мережі, на які вони розподіляється, може відрізнятися від наведеного розподілу відповідно до функцій та структури мережі установи.

4.7 Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів / користувачів інформаційно-телекомунікаційних систем установи із зовнішніх мереж, повинні бути розміщені в зовнішній зоні інформаційно-телекомунікаційних систем установи. З'єднання серверів та обладнання, які розміщені в зовнішній зоні, із серверами та обладнанням внутрішньої мережі інформаційно-телекомунікаційних систем установи повинні захищатися міжмережевим екраном.

4.8 Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення інформаційно-телекомунікаційних систем установи, а також серверні частини засобів захисту інформації повинні бути розміщені в зоні прикладних застосувань системи безпеки (Security-zone) мережі, захищеної за допомогою міжмережевого екрана.

4.9 Сегмент інформаційної інфраструктури інформаційно-телекомунікаційних систем установи, в якому перебуває система керування технологічними процесами, повинен бути відокремленим від інших систем інформаційно-телекомунікаційних систем установи. У випадку логічного відокремлення на межі сегмента повинен бути встановлений міжмережевий екран.

4.10 Повинні бути визначені та відключені (заблоковані) програмні порти компонентів інформаційно-телекомунікаційних систем установи, які є небезпечними для забезпечення кібербезпеки.

4.11 Для захисту даних, які передаються через незахищене середовище, зокрема мережу Інтернет, між віддаленими користувачами, адміністраторами та інформаційно-телекомунікаційними системами установи необхідно використовувати захищені з'єднання із забезпеченням конфіденційності та цілісності цих даних та використанням засобів криптографічного захисту інформації (шифрування).

4.12 До глобальних мереж передачі даних, зокрема Інтернету, інформаційно-телекомунікаційні системи установи повинні підключатися через тих операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю.

5. Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів інформаційно-телекомунікаційних систем установи.

5.1 Для забезпечення відмовостійкості інформаційно-телекомунікаційних систем установи повинно здійснюватися, як мінімум, таке:

періодичне, але не рідше одного разу на тиждень, створення резервних копій інформаційних ресурсів інформаційно-телекомунікаційних систем

установи, включаючи інформацію, яка зберігається в інформаційно-телекомунікаційних системах установи, технологічну інформацію компонентів систем та образів віртуальних серверів інформаційно-телекомунікаційних систем, а також їх відновлення у випадку втрати або пошкодження. Носії даних, на яких зберігаються резервні копії, повинні зберігатися тільки у визначеного адміністратора, при цьому цей адміністратор повинен нести відповідальність за їх безпечне зберігання;

резервування критичних для функціонування інформаційно-телекомунікаційних систем установи програмних та апаратних компонентів для забезпечення їх сталого функціонування у випадку виходу з ладу одного з критичних компонентів. У разі використання в інформаційно-телекомунікаційних системах установи віртуальних серверів необхідно забезпечити їх резервування;

дублювання (кластеризація) критичних для функціонування інформаційно-телекомунікаційних систем установи програмних та апаратних компонентів інформаційно-телекомунікаційних систем для забезпечення їх сталого функціонування, зниження навантаження та збільшення продуктивності;

використання засобів балансування навантаження;

використання джерел безперебійного живлення для критичних компонентів інформаційно-телекомунікаційних систем установи;

зв'язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами), — для інформаційно-телекомунікаційних систем установи, які надають свої послуги через Інтернет.

5.2 Необхідно заборонити або щонайменше мінімізувати використання флеш та інших типів з'ємних носіїв даних на робочих станціях користувачів та адміністраторів інформаційно-телекомунікаційних систем установи.

5.3 Робочі станції користувачів та адміністраторів інформаційно-телекомунікаційних систем установи повинні бути недоступні для використання членами сім'ї співробітника установи.

6. Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації в інформаційно-телекомунікаційній системі установи.

6.1 В інформаційно-телекомунікаційних системах установи, включаючи віддалені робочі місця користувачів та адміністраторів систем, повинна проводитися перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів (антивірусне програмне забезпечення або інші засоби які включаються до свого складу такі функції з останніми оновленнями своїх антивірусних баз).

6.2 В інформаційно-телекомунікаційних системах установи, включаючи віддалені робочі місця користувачів та адміністраторів систем, повинно бути відключено автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації.

6.3 Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами цих систем.

7. Визначення умов використання програмного та апаратного забезпечення інформаційно-телекомунікаційних систем установи.

7.1 В інформаційно-телекомунікаційних системах установи повинна проводитися перевірка на цілісність та автентичність оновлень компонентів інформаційно-телекомунікаційних систем установи. У разі порушення цілісності або непідтвердження автентичності оновлення воно повинно бути відхилене і не повинно застосовуватися.

7.2 У складі інформаційно-телекомунікаційних систем установи, у тому числі віддалених робочих місць користувачів та адміністраторів, повинно використовуватися програмне та програмно-апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватися офіційні стабільні версії прикладного програмного забезпечення та драйверів. Все програмне забезпечення повинно регулярно оновлюватися до останніх версій та включати всі останні оновлення та патчі, включаючи останні критичні оновлення та оновлення безпеки, від виробників цих програмних та програмно-апаратних продуктів.

7.3 Програмні та апаратні засоби, які використовуються у складі інформаційно-телекомунікаційних систем установи, у тому числі віддалених робочих місць користувачів та адміністраторів, не повинні мати походження з іноземної держави, до якої застосовано санкції згідно із Законом України "Про санкції", чи бути розроблені/виготовлені юридичною особою — резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

8. Окремі практичні рекомендації щодо підвищення рівня захищеності інформаційно-телекомунікаційних систем установи.

8.1 Організувати процес контролю наявності вразливостей на активному мережевому, серверному обладнанні та робочих місцях користувачів інформаційно-телекомунікаційних систем установи.

8.2 Упровадити систему моніторингу працездатності мережевого, серверного обладнання інформаційно-телекомунікаційних систем установи, а також каналів зв'язку; як варіант використовувати можливості протоколу SNMP.

8.3 Для унеможливлення проведення атак типу Man-in-the-Middle з використанням техніки ARP-spoofing вжити заходів з налаштування статичних значень ARP-таблиць АРМ і серверного обладнання інформаційно-телекомунікаційних систем установи.

8.4 Вжити заходів з унеможливлення використання в інформаційно-телекомунікаційних системах установи стороннього програмного забезпечення.

8.5 Здійснити прив'язку MAC-адресів ПЕОМ співробітників до конкретного інтерфейсу комутатора, цим самим заборонивши підключення сторонніх ПЕОМ.

8.6 По можливості запровадити підключення користувачів до мережі з використанням стандарту IEEE 802.1x.

8.7 Забезпечити використання протоколів, які забезпечують стійке шифрування даних. Для протоколів HTTP, POP3, FTP та інших використовувати щонайменше SSL версії 3. Під час використання протоколу RDP вжити заходів з налаштування опції мережевої автентифікації (NLA), а також під час встановлення сесії між сервером і клієнтом дозволити використання лише стійких алгоритмів.

8.8 Не допускати простих та стандартних паролів для мережевого обладнання та інших компонентів інформаційно-телекомунікаційних систем установи з метою підвищення стійкості паролів облікових записів користувачів.

8.9 Обмежити можливість запуску виконуваних файлів (*.exe) на комп'ютерах користувачів установи з директорій %TEMP%, %APPDATA%.

8.10 Організувати процес безпечного доступу співробітників установи до ресурсів мережі Інтернет за допомогою PROXY-сервера. Налаштувати обмеження доступу до визначеного переліку веб-сайтів, балансування навантаження на канал зв'язку, журналювання сеансів користування Інтернетом та налаштувати заборону завантаження файлів певних типів *.exe, *.pdf, *.avi, які можуть містити шкідливе програмне забезпечення.

8.11 Закрити порти на серверному обладнанні інформаційно-телекомунікаційних систем установи, які не використовуються.

8.12 Постійно підтримувати рівень обізнаності персоналу установи у сфері інформаційної безпеки.

8.13 Використовувати тільки «LTS» версії фреймворків, бібліотек та останні версії CMS, плагінів та модулів на веб-сайтах установи.

8.14 Використовувати тільки захищені протоколи та з'єднання для адміністрування сайту чи серверу.

8.15 Розміщувати вебсервер на своєму, окремо виділеному, віртуальному або фізичному сервері.

8.15 Обмежити доступ до панелі адміністратора з мережі Інтернет та мереж загального користування.

8.16 Налаштувати кешування сторінок з метою збільшення швидкості роботи сайту та запобігання DOS, DDOS атак.

8.17 Перевірити ресурс на наявність шкідливого програмного забезпечення, використовуючи рекомендації із самостійного пошуку та ліквідації веб-шеллів (https://cert.gov.ua/files/pdf/CUA-14-06R.pdf).

8.18 Заборонити доступ до інформаційно-телекомунікаційних систем установи з незареєстрованого та невстановленого обладнання.

8.19 Заборонити або щонайменше мінімізувати використання флеш та інших типів з'ємних носіїв даних на робочих станціях користувачів та адміністраторів інформаційно-телекомунікаційних систем установи.

8.20 Робочі станції користувачів та адміністраторів інформаційно-телекомунікаційних систем установи повинні бути недоступні для використання членами сім'ї співробітника установи.

9. Рекомендації щодо дій по закінченню карантину.

9.1 Переглянути права доступу всіх користувачів та адміністраторів інформаційно-телекомунікаційних систем установи до інформаційних ресурсів та сервісів систем.

9.2 Змінити паролі та інші атрибути доступу користувачів та адміністраторів до інформаційно-телекомунікаційних систем установи.

9.3 Переглянути політику безпеки, прийняту в установі, відповідно до зміни порядку роботи користувачів в інформаційно-телекомунікаційних системах установи.

9.4 Провести контроль (аудит) рівня захищеності інформаційно-телекомунікаційних систем установи.

Т.в.о. директора Департаменту кіберзахисту
Адміністрації Держспецзв'язку Юрій ЦИПЛИНСЬКИЙ

«31» 03 2020 року