Прим. № 1

Рекомендації
із першочергових заходів кіберзахисту
об’єктів, що виконують завдання в сфері оборони і безпеки

1. Обробка інформації, яка відноситься до державних інформаційних ресурсів та до інформації з обмеженим доступом (таємна, службова, конфіденційна інформація), вимога щодо захисту якої встановлена законом, має здійснюватись у відповідності до вимог законодавства.

2. Для забезпечення функціонування інформаційно-комунікаційних систем (далі – ІКС) мають використовуватись користувачі з унікальними персоніфікованими логінами (іменами).

3. Забороняється використовувати один і той самий пароль для кількох облікових записів.

4. Забороняється використовувати облікові записи та паролі «за замовчуванням». Неперсоналізовані і гостьові облікові записи користувачів (включаючи адміністраторів) мають бути відключені, паролі «за замовчуванням» – змінені.

5. Рекомендується використовувати керування доступом на основі ролей (Role-Based Access Control, RBAC).

6. Паролі користувачів ІКС повинні відповідати визначеним критеріям щодо складності та частоти зміни.

Рекомендується:

довжина пароля – не менше ніж 12 символів;

одночасне використання великих і малих літер, цифр, спеціальних символів;

частота зміни пароля – кожні 3 місяці.

7. Забороняється повідомляти логін та пароль облікового запису іншим особам.

8. Для доступу користувачів та адміністраторів до систем використовувати багатофакторну автентифікацію (де це можливо).

9. При визначенні прав доступу користувачам має застосовуватись принцип «мінімально достатніх повноважень» відповідно до їх функціональних обов’язків (права доступ мають надаватись лише у разі необхідності). Має проводитись регулярний перегляд прав доступу користувачів та адміністраторів.

Рекомендується: проводити перегляд прав доступу не рідше ніж один раз на півроку.

10. Під час звільнення з посади співробітника його облікові записи повинні бути негайно заблоковані або видалені в усіх компонентах систем. При переведенні співробітника на іншу ділянку (до іншого підрозділу) має проводитись перегляд прав доступу його облікових записів.

11. Адміністрування системи має здійснюватись з використанням окремих облікових засобів з підвищеними привілеями. Їх використання співробітниками,

які виконують функції адміністраторів, дозволяється лише у разі необхідності (під час виконання діяльності, що не вимагають функцій адміністрування, вони мають використовувати облікові записи без підвищених привілеїв).

12. Налаштування програмних та апаратних засобів «за замовченням» мають бути змінені.

13. На робочих станціях користувачів та компонентах ІКС може бути встановлене лише ліцензійне програмне забезпечення, що входить до переліку дозволеного.

14. Використання програмного забезпечення, внесеного до відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання (зокрема розробленого в Російській федерації), забороняється.

15. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор.

16. Має забезпечуватись регулярне оновлення програмного забезпечення, встановленого в ІКС.

17. На робочих станціях користувачів та серверах має бути встановлене антивірусне програмне забезпечення з регулярним оновленням антивірусних баз з проведенням періодичних сканувань систем.

18. На робочих станціях користувачів має бути налаштовано автоматичне блокування екрана, у разі відсутності активності користувача, з можливістю відновлення сесії шляхом введення паролю/PIN коду.

19. Мережа об’єкта повинна бути розділена на сегменти. Взаємодія між ними повинна здійснюватись із використанням міжмережевих екранів.

20. Архітектура мережі повинна забезпечувати виділення окремо:

зовнішньої зони (DMZ-zone): для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів;

зони прикладних застосувань (APP-zone): для розміщення серверів застосувань (з можливістю підключення до неї користувачів сервісів);

зони сховищ даних (DB-zone): для розміщення баз даних та доступу за запитами APP-zone;

зони прикладних застосувань системи безпеки (Security-zone): для розміщення сервісів та служб захисту інформації та робочих станцій адміністраторів;

тестової зони (Test-zone): для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення.

21. Сегмент, в якому перебуває автоматизована система керування технологічними процесами (АСК ТП, ICS), повинен бути відокремленим від інших систем та компонентів.

22. IP-камери систем відеореєстрації, повинні бути винесені в окремий сегмент мережі, доступ до нього має бути доступний лише з визначених робочих станцій організації, підключення до нього з мережі Інтернет заборонено.

Рекомендується використовувати власні сервери відеореєстрації замість хмарних, які надаються вендором (розробником).

23. Забороняється використання на об’єктах критичної інформаційної інфраструктури (далі – ОКІІ) об’єкта критичної інфраструктури технологій Wi-Fi та Bluetooth.

24. У разі необхідності використання в інших системах об’єкта (які не відносяться до ОКІІ) обладнання Wi-Fi, воно повинно бути винесено в окремий сегмент мережі з використанням протоколів безпеки безпровідного з’єднання *(рекомендується WPA3 (Enterprise)* та надійних логіну і паролю, функція WPS має бути відключена.

25. Для підключення гостьових користувачів до мережі Wi-Fi відповідне комутаційне обладнання слід розгорнути в окремому сегменті мережі, який не має доступу до сегментів критичних систем організації.

26. Підключення до ІКС віддалених користувачів, адміністраторів, взаємодія компонентів системи (поза контрольованою територією) та іншими (зовнішніми) ІКС має здійснюватись лише з використанням захищених з’єднань (зокрема VPN) з використанням засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

27. Для забезпечення відмовостійкості має забезпечуватись:

періодичне створення резервних копій інформаційних ресурсів критичних компонентів ІКС, включаючи технологічну інформацію компонентів системи та образів серверів системи для їх відновлення у випадку втрати або пошкодження;

використання джерел безперебійного живлення для критичних компонентів системи;

зв’язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами).

28. Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані. Сервіси компонентів системи, які не використовуються мають бути відключені.

29. Підключення компонентів ІКС до сервісів Telegram має бути заблоковано, а можливість встановлення та використання клієнтського програмного забезпечення Telegram заборонено.

30. Має забезпечуватись реєстрація подій компонентами ІКС у захищених журналах (логах) реєстрації подій та їх періодичний аудит, зокрема з використанням засобів автоматизації (наприклад SIEM).

31. Під час виконання службових обов’язків користувачі мають суворо дотримуватись правил кібергігієни (https://cert.gov.ua/recommendations).

32. Користувачі мають виконувати вимоги щодо забезпечення конфіденційності і приватності. Забороняється передавати таємну, службову, конфіденційну інформацію через незахищені і не призначені для цього канали

зв’язку і системи передачі даних (зокрема через месенджери Signal, WhatsApp тощо). Також забороняється повідомляти стороннім особам таємну, службову, конфіденційну інформацію, зокрема персональні дані.

33. Зі співробітниками мають проводитись регулярні заняття (тренінги) з питань забезпечення кібербезпеки та виконання правил кібергігієни з подальшою перевіркою отриманих знань і навичок.

34. Має бути розроблений на доведений до користувачів план реагування на кіберінциденти (хто, коли і що має робити). Ці плани повинні регулярно (принаймні щорічно) переглядатись.

35. З метою перевірки стану захищеності на регулярній основі слід проводити:

сканування мережі об’єкта на наявність вразливостей вебсервісів об’єкта та тести на проникнення (Penetration test);

кібернавчання, зокрема з імітацією появи кіберінцидентів (наприклад фішингових розсилок) та перевіркою дій співробітників у разі їх появи;

перевірка відновлення критичних компонентів системи з резервних копій.

36. З метою здійснення вказаних заходів пропонуємо використовувати послуги, що надаються Державним центром кіберзахисту Держспецзв’язку:

підключення до системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (d.liutin@cip.gov.ua);

підключення до системи захищеного доступу державних органів до мережі Інтернет (noc@cip.gov.ua);

проведення оцінки стану захищеності державних інформаційних ресурсів і сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті (pentest@cip.gov.ua);

проведення навчання співробітників з використанням системи «Кіберполігон (тренінгова кіберплатформа)» (training@cip.gov.ua);

використання сервісів Національного центру резервування державних інформаційних ресурсів (nccsa@cip.gov.ua);

використання оновлення антивірусного програмного забезпечення із застосуванням Центру антивірусного захисту інформації (cazi@cip.gov.ua).

37. У разі появи кіберінциденту (кібератаки) має забезпечуватись невідкладне інформування команди CERT-UA (cert@cert.gov.ua, incidents@cert.gov.ua) та ситуаційного центру забезпечення кібербезпеки СБУ (incident@dis.gov.ua).

Начальник 7 управління
ДЦКЗ Держспецзв’язку Олександр КОРНІЛЕНКО

Драний Олексій 281 80 57