Додаток

Рекомендації щодо мінімізації ризиків деструктивного кібервпливу

– неухильно дотримуватись норм Закону України «Про основні засади забезпечення кібербезпеки України» та положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29.12.2021 № 1426;

– утворити підрозділ із кіберзахисту або призначити осіб, на яких покладається забезпечення захисту інформації та контролю за ним відповідно до абзацу 2 статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

– розробити профілі кіберзахисту та періодично їх переглядати відповідно до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (зі змінами);

– виконувати Базові заходи з кіберзахисту, затверджені наказом Адміністрації Держспецзв'язку від 30.01.2025 № 54;

– розробити і затвердити план кіберзахисту та план реагування на кіберінциденти/кібератаки відповідно до абзацу 2 пункту 5 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29.12.2021 № 1426;

– встановити антивірусне програмне забезпечення;

– використовувати перевірене на вразливості та недокументовані функції програмне забезпечення;

– надавати перевагу вітчизняним програмним продуктам, зокрема, програмному забезпеченню з відкритим кодом і ліцензійному програмному забезпеченню, до якого не застосовуються спеціальні економічні та інші обмежувальні заходи (санкції);

– налаштувати політики управління доступом користувачів та адміністраторів, встановити стійкі паролі;

– налаштувати реєстрацію подій;

– регулярно проводити оновлення програмного забезпечення на обладнанні;

– перевірити обладнання на відсутність встановлених програм віддаленого керування;

– проводити резервне копіювання інформаційних ресурсів на обладнанні;

– встановити комплекти обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (далі – ІКС) кіберзахисту державних інформаційних ресурсів, який забезпечує проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, і відбулися або відбуваються;

– налагодити взаємодію з платформами обміну інформацією щодо шкідливого програмного забезпечення (MISP CERT-UA, MISP-UA або іншими), з національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA та з оперативним центром реагування на кіберінциденти (SOC);

– здійснювати моніторинг публікацій на офіційному сайті команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA та вживати заходів щодо опрацювання відповідних рекомендацій;

– підключитись до сервісу доменних імен для кібербезпеки органів державної влади та операторів критичної інфраструктури, як частини системи реагування на кіберінциденти, кібератаки, кіберзагрози щодо об’єктів кіберзахисту (DNS);

– періодично проводити тестування систем у відповідності до Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16.05.2023 № 497.

Заступник директора Департаменту –
начальник відділу Департаменту кіберзахисту
Адміністрації Держспецзв’язку Денис ЗУБКОВ