Додаток 2
до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (пункт 4 розділу VII)

Методичні рекомендації щодо розробки поточного профілю кіберзахисту

Поточний профіль кіберзахисту розробляється з використанням класифікації заходів кіберзахисту. Розробку поточного профілю кіберзахисту ОКІІ може здійснювати особа, відповідальна за впровадження заходів захисту інформації на ОКІ. Профіль кіберзахисту рекомендується розробляти для кожного ОКІІ окремо.

Розробка поточного профілю кіберзахисту має на меті зіставлення вимог Рекомендацій з практикою захисту інформації, що впроваджена на ОКІ. В цьому випадку можна розглядати три типи організації.

Організація першого типу (далі – Організація 1) реалізує підхід із захисту інформації, що базується на власній практиці із захисту інформації.

Організація другого типу (далі – Організація 2) організація, яка будувала систему захисту інформації на основі вимог міжнародних, національних або галузевих стандартів.

Організація третього типу (далі – Організація 3) – заходи захисту взагалі не реалізовані.

Поточна практика захисту інформації, що наведена у таблиці, є узагальнюючою та призначена для ілюстрації концепції зіставлення. Рівень специфічності та деталізації необхідний для того, щоб профіль був корисним та унікальним для кожної організації.

Таблиця – Приклади поточного профілю кіберзахисту ОКІІ

Функція кібербезпеки	Категорія заходів кіберзахисту	Заходи кіберзахисту	Профіль кіберзахисту
			Поточна практика захисту інформації
1	2	3	4
Організація 1 Підхід на основі власних заходів захисту			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Комутований доступ для здійснення технічного обслуговування персоналом постачальника надається у разі потреби та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється.

Продовження додатка 2

1	2	3	4
			Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Рівень упровадження – другий рівень – ризик-орієнтований.
Організація 2 Підхід, що базується на використанні вимог стандарту			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу здійснюється відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.1; A.6.2.2; A.11.2.6; A.13.1.1; A.13.2.1. Рівень упровадження – другий рівень – ризик-орієнтований.
			У разі побудованої КСЗІ. Контроль віддаленого доступу реалізовано відповідно до вимог НД ТЗІ 2.5-004-99: ДР-2, ДС-1, НР-2, НИ-2, НО-2, НЦ-1, НТ-2, НВ-1. Рівень гарантій – Г2. Рівень упровадження – третій рівень – повторюваний.
			У разі побудованої системи захисту інформації на основі галузевих стандартів. Система захисту інформації побудована відповідно до вимог міжнародного стандарту IEC 62443: IEC 62443-2-1:2015: 4.3.3.6.6. IEC 62443-3-3:2016: SR 1.13; SR 2.6. Рівень упровадження – другий рівень – ризик-орієнтований.

Продовження додатка 2

1	2	3	4
Організація 3 Підхід до опису відсутності заходів захисту			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Не застосовується – віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації. Заходи кіберзахисту не впроваджувалися.