Додаток 3
до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (пункт 4 розділу VII)

Методичні рекомендації щодо розробки
цільового профілю кіберзахисту

Створюючи цільовий профіль кіберзахисту, організація враховує:
вимоги нормативно-правових актів та нормативних документів;
сучасні практики захисту інформації;
сучасні практики управління ризиками;
поточне середовище ризику;
цілі діяльності та завдання;
організаційні обмеження.

У таблиці наведено приклад гіпотетичного цільового профілю кіберзахисту для конкретного результату заходів кіберзахисту підкатегорії (PR.AC-3) для трьох організацій, що використовують три різні підходи.

Організація 1 визначила, що чинна практика захисту, яку вона використовує для управління віддаленим доступом, є недостатньою для опрацювання ризиків кібербезпеки, тому потрібно впровадити додаткові заходи кіберзахисту. Організація 2 доходить до такого самого висновку та визначає додаткові вимоги стандартів безпеки, які хотіла б впровадити у себе. Організація 3 демонструє, що поточний профіль є ідентичним цільовому профілю кіберзахисту для визначених заходів кіберзахисту. Такі випадки відбудуться тоді, коли стандарти, інструменти, методи, що реалізуються організацією, достатньою мірою відповідають її вимогам кібербезпеки та управління ризиками.

Однак таке узгодження поточного профілю та цільового профілю кіберзахисту може тривати тільки протягом короткого періоду часу, оскільки вимоги організації до кібербезпеки та управління ризиками будуть розвиватися в міру її розвитку та виникнення нових ризиків. Наприклад, організація може визначити, що поточна практика більше не потрібна або недостатня, та виключити її з цільового профілю кіберзахисту.

При розробці цільового профілю кіберзахисту організації можуть використати ширший підхід – з урахуванням більш ефективних і дієвих підходів до управління ризиками у всій організації.

Окрім цільового профілю кіберзахисту, організація вибирає цільовий рівень упровадження заходів кіберзахисту, який застосовується до процесу управління ризиками в межах сфери своєї діяльності. Організація самостійно вибирає прийнятний для неї рівень («бажаний» стан) та визначає заходи кіберзахисту та заходи щодо управління ризиками, необхідні для досягнення цієї мети.

Використовуючи стандарти, інструменти, методи щодо управління кібербезпекою, організація відображає бажані результати у цільовому профілі кіберзахисту та цільовому рівні реалізації.

Таблиця – Приклади цільового профілю кіберзахисту ОКІІ

Функція кібербезпеки	Категорія заходів кіберзахисту	Заходи кіберзахисту	Профілі кіберзахисту	
			Поточний профіль кіберзахисту – поточна практика захисту інформації	Цільовий профіль кіберзахисту
1	2	3	4	5
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. 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.	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. 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. Огляд авторизованого списку облікових записів VPN

Продовження додатка 3

1	2	3	4	5
				рекомендується здійснювати двічі на рік.* Цільовий 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.; A.13.1.1; A.13.2.1. Рівень упровадження – другий рівень – ризик-орієнтований.	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу рекомендується здійснювати відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.; A.6.2.; A.11.2.6; A.13.1.1; A.13.2.1. A.13.2.2;* A.13.2.3;* A.13.2.4;* A.14.2.8;* A.15*. Рівень впровадження – третій рівень – повторюваний.
			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 КСЗІ. Контроль віддаленого доступу рекомендується реалізовувати відповідно до вимог НД ТЗІ 2.5-004-99: ДР-3,* ДС-1, ДЗ-1;* НР-2, НИ-2, НК-1;* НО-2, НЦ-2, НТ-2,* НВ-1. Рівень гарантій – Г3. Цільовий рівень упровадження – третій

Продовження додатка 3

1	2	3	4	5
				рівень – повторюваний.
			У разі побудованої системи захисту інформації на основі галузевих стандартів. Контроль віддаленого доступу реалізовано відповідно до вимог міжнародного стандарту: 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.	У разі побудованої системи захисту інформації на основі галузевих стандартів. Контроль віддаленого доступу рекомендується реалізовувати відповідно до вимог міжнародного стандарту: IEC 62443-2-1:2015: 4.3.3.6.4* 4.3.3.6.6. 4.3.3.6.7* IEC 62443-3-3:2016: SR 1.13; SR 2.6; SR 1.13 (1).* Цільовий рівень упровадження – другий рівень – ризик-орієнтований.
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.	Не застосовується – віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації.

Примітка

* Організація визначила необхідність впровадження додаткових практик, які вона хоче впровадити для успішного досягнення результату на основі аналізу поточного середовища ризику, цілей і завдань діяльності у сфері надання основних послуг.