ПОЛТАВСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

РОЗПОРЯДЖЕННЯ

16.03.2023 м.Полтава № 163

Про проведення заходів щодо функціонування інформаційно-комунікаційних систем в облвійськадміністрації

Відповідно до законів України „Про захист інформації в інформаційно-комунікаційних системах", „Про основні засади забезпечення кібербезпеки України", наказа Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2021 № 601 „Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури" (зі змінами) з метою сталого функціонування інформаційно-комунікаційних систем (далі – ІКС) в облвійськадміністрації:

1. Керівникам структурних підрозділів облвійськадміністрації призначити відповідальну особу щодо забезпечення кіберзахисту у своїх підрозділах до 24.03.2023.

2. Відповідальним особам щодо забезпечення кіберзахисту провести роботу з ідентифікації та надати оцінку поточного стану кіберзахисту власних ІКС відповідно до Рекомендацій оцінювання та підвищення рівня кіберзахисту ІКС державних органів, зазначених у додатку, до 17.04.2023.

3. Відповідальним виконавцям пунктів 1 та 2 інформувати про стан виконання розпорядження Управління цифрової трансформації облвійськадміністрації (Коломоєць С.В.) у зазначені строки для подальшого узагальнення та інформування облвійськадміністрації до 27.03.2023 та 21.04.2023 відповідно.

4. Координацію роботи щодо виконання розпорядження покласти на Управління цифрової трансформації облвійськадміністрації (Коломоєць С.В.), контроль за виконанням розпорядження покласти на заступника начальника облвійськадміністрації з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) Панченка І.І.

Начальник обласної
військової адміністрації Дмитро ЛУНІН

Додаток
до розпорядження
начальника Полтавської обласної
військової адміністрації
16.03.2023 № 163

РЕКОМЕНДАЦІЇ
оцінювання та підвищення рівня кіберзахисту ІКС державних органів

Рекомендації оцінювання та підвищення рівня кіберзахисту інформаційно-комунікаційних систем (далі – ІКС) державних органів розроблено з метою надання роз'яснень щодо проведення заходів з ідентифікації та складання поточних профілів кіберзахисту та визначення суб'єктами, які складають такі профілі, поточного стану справ у забезпеченні своєї кібербезпеки та рівня впровадження цих заходів в ІКС державних органів.

Поточний профіль кіберзахисту створюється на основі Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2021 № 601 „Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури" (зі змінами) (далі – Методичні рекомендації) .

У Таблиці 2 наведено повний перелік заходів кіберзахисту, які мають бути враховані, впроваджені та описані в ІКС державних органів для забезпечення достатнього рівня кіберзахисту. Визначено 5 класів заходів кіберзахисту („Ідентифікація ризиків кібербезпеки (ID)", „Кіберзахист (PR)", „Виявлення кіберінцидентів (DE)", „Реагування на кіберінциденти (RS)", „Відновлення стану кібербезпеки (RC)"), кожний з яких містить категорії заходів кіберзахисту. У другій колонці Таблиці 2 вказано захід кіберзахисту відповідної категорії заходів відповідного класу заходів. У третій колонці необхідно заповнити поточний опис виконання заходів кіберзахисту в ІКС державних органів, як підтвердження, необхідно вказати назву документу (номер та дату реєстрації), в якому наявне підтвердження виконання заходу кіберзахисту. При цьому, якщо заходи безпеки застосовуються постійно, необхідно наводити підтвердження цьому. Нормативні та додаткові посилання, а також приклад опису поточної практики кіберзахисту для заповнення Таблиці наведено в Таблиці 1 до Методичних рекомендацій. У четвертій колонці необхідно заповнити цільовий опис виконання заходів кіберзахисту в ІКС державних органів, в п'ятій – описати заходи для досягнення цільового профілю кіберзахисту за роками, шляхом зіставлення поточного та цільового станів кіберзахисту.

У Таблиці 3 в другому стовбці вказано захід кіберзахисту відповідної категорії заходів відповідного класу заходів, в третьому – п'ятому стовбці необхідно визначити статус відповідності за шкалою, яка складається з чотирьох станів:

1. Реалізовано – якщо захід кіберзахисту виконано та постійно застосовується на системній основі. При визначенні статусу „Реалізовано" слід в Таблиці 2 навести документальне підтвердження такої реалізації, яке може виражатися у вигляді наказів, розпоряджень, сертифікатів, паспортів, формулярів тощо;

2. У процесі реалізації – якщо захід кіберзахисту виконано не в повному обсязі;

3. Розглядається – якщо захід кіберзахисту не реалізований, але розглядається до виконання в майбутньому;

4. Не потребується – якщо прийнято обґрунтоване рішення стосовно того, що захід кіберзахисту не буде реалізовуватися.

У стовбцях 3-5 визначається статус реалізації заходу кіберзахисту шляхом проставляння символу „☒" в одному з стовбців. Кожний захід кіберзахисту обов'язково повинен бути оцінений. Одночасне використання двох або більше символів „☒" для одного заходу кіберзахисту – не дозволяється.

У Таблиці 1 наведено форму для заповнення відомостей щодо узагальнення заходів кіберзахисту за статусом реалізації. За кожним класом заходів кіберзахисту підводиться підрахунок як за абсолютною шкалою, так й за відсотковою відносно загальної кількості заходів кіберзахисту. Сума символів „☒", проставлена в Таблиці 3, для кожного класу повинна співпадати з загальною кількістю заходів кіберзахисту. Відсоткові значення повинні бути округлені за правилами математики так, щоб їх загальна сума не перевищувала 100%.

Таблиця 1

№ з/п	Клас заходів кіберзахисту	Всього підкатегорій заходів кіберзахисту	Статус (кількість та % заходів за кожною категорією)			
			реалізовано	у процесі реалізації	розглядається	не потребується
1	Ідентифікація ризиків кібербезпеки (ID)	29	–	–	–	–
			– %	– %	– %	– %
2	Кіберзахист (PR)	39	–	–	–	–
			– %	– %	– %	– %
3	Виявлення кіберінцедентів (DE)	18	–	–	–	–
			– %	– %	– %	– %
4	Реагування на кіберінцеденти (RS)	16	–	–	–	–
			– %	– %	– %	– %
5	Відновлення стану кібебезпеки (RC)	6	–	–	–	–
			– %	– %	– %	– %
6	ВСЬОГО:	108	–	–	–	–
			– %	– %	– %	– %

Висновки:

1. Заходи кіберзахисту, що реалізовані – (– %)

2. Періодичність перегляду / переоцінки поточного профілю кіберзахисту.

3. Зіставлення поточного та цільового профілів кіберзахисту ІКС державних органів (заходи для досягнення цільового профіля за роками)

Таблиця 2

ОПИС
поточного та цільового станів кіберзахисту, порівняння станів кіберзахисту

№ з/п	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту	Заходи для досягнення цільового профіля за роками
1	2	3	4	5
Ідентифікація ризиків кібербезпеки (ID)				
ID.AM Управління активами				
1.	ID.AM-1. Фізичне обладнання та системи на власних ІКС ідентифіковано та задокументовано.	Проведена інвентаризація усього обладнання, в документі [від __.__.202_ № __] зафіксовані всі складові, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. На кожен екземпляр обладнання Системи заведено формуляр.		
2.	ID.AM-2. Програмне забезпечення, що використовуються власними ІКС для надання життєво важливих послуг та функцій, ідентифіковано та задокументовано.	Проведена інвентаризація програмного забезпечення та в документі (паспорт, опис тощо) [від _._.202_ № ___] задокументовано призначення та склад спеціалізованого програмного забезпечення його життєве важливі послуги та функції які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації		

1	2	3	4	5
3.	ID.AM-3. Електронні комунікації та потоки даних власних ІКС ідентифіковано та задокументовано.	Електронні комунікації та потоки даних в ідентифіковано та задокументовано в документі [від _._.202_ № ___] Визначено номери VLAN та IP-адресація внутрішніх підмереж для різних потоків даних: інформаційно-аналітичних, моніторингу та віддаленого управління.		
4.	ID.AM-4. Зовнішні інформаційні та інформаційно-комунікаційні системи, промислові системи, які взаємодіють з інформаційно-комунікаційними та іншими системами власних ІКС обліковано.	Взаємодіє з мережею Інтернет. Схема організації такої взаємодії задокументована [від _._.202_ № ___] та передбачає використання з'єднань через: 1. 2. 3.		
5.	ID.AM-5. Критичність активів (обладнання, устаткування, даних, програмного забезпечення) власних ІКС визначено відповідно до оцінки їх впливу на надання життєво важливих послуг та функцій власних ІКС.			
6.	ID.AM-6. Обов'язки штатного персоналу власних ІКС та персоналу партнерів організації (наприклад – постачальників, клієнтів, тощо) щодо забезпечення кібербезпеки визначено та закріплено у відповідних документах.			
ID.BE Середовище надання життєво важливих послуг та функцій				
7.	ID.BE-1. Роль власних ІКС в ланцюгу постачання товарів і послуг визначено та повідомлено всім постачальникам організації.			
8.	ID.BE-2. Місце та роль власних ІКС в системі надання життєво важливих послуг та функцій сектору (підсектору) критичної інфраструктури визначено і повідомлено всім постачальникам організації.			

1	2	3	4	5
9.	ID.BE-3. Пріоритетність цілей, завдань і заходів щодо забезпечення кібербезпеки, надання життєво важливих послуг та функцій встановлено та повідомлено.			
10.	ID.BE-4. Залежності та найважливіші процеси для забезпечення надання життєво важливих послуг та функцій встановлено.			
11.	ID.BE-5. Вимоги до стійкості власних ІКС щодо забезпечення надання життєво важливих послуг та функцій встановлено.			
	ID.GV Управління безпекою			
12.	ID.GV-1. Правила (політики) кібербезпеки власних ІКС встановлено та задокументовано			
13.	ID.GV-2. Обов'язки щодо забезпечення кібербезпеки власних ІКС скоординовано та узгоджено з обов'язками персоналу власних ІКС та із зовнішніми партнерами			
14.	ID.GV-3. Правові та нормативні вимоги щодо забезпечення кібербезпеки власних ІКС, в тому числі зобов'язання щодо захисту недоторканості особистого життя (приватності), усвідомлено та управління ними здійснюється			
15.	ID.GV-4. Процеси управління безпекою та управління ризиками спрямовано на вирішення питання оброблення ризиків кібербезпеки			
	ID.RA Оцінка ризиків			
16.	ID.RA-1. Вразливості активів власних ІКС проаналізовано, ідентифіковано та задокументовано			
17.	ID.RA-2. Інформацію про загрози безпеки та вразливості отримано з форумів обміну інформацією та офіційних джерел			
18.	ID.RA-3. Загрози кібербезпеки (модель загроз) як внутрішні, так і зовнішні визначено й задокументовано			

1	2	3	4	5
19.	ID.RA-4. Потенційні наслідки (рівень шкоди),які можуть завдати загрози в наслідок їх реалізації на безперервне надання життєво важливих послуг та функцій та ймовірності їх реалізації визначено			
20.	ID.RA-5. Для визначення ризику застосовуються данні щодо загроз, вразливостей, їх ймовірностей та рівня шкоди використано для визначення ризику кібербезпеки			
21.	ID.RA-6. Заходи реагування на ризик кібербезпеки визначено та їх пріоритетність встановлено			
ID.RM Стратегія управління ризиками організації				
22.	ID.RM-1. Процеси управління ризиками визначено, узгоджено із партнерами організації та управляються			
23.	ID.RM-2. Допустимий рівень ризику кібербезпеки визначено та чітко виражено			
24.	ID.RM-3. Визначення допустимого рівня ризику ґрунтується на ролі власних ІКС як складової частини сектору критичної інфраструктури та аналізі ризиків, притаманних відповідному сектору критичної інфраструктури			
ID.SC Управління ризиками системи постачання				
25.	ID.SC-1. Процеси управління ризиками кібербезпеки системи постачання визначено, узгоджено з партнерами організації та управляються			
26.	ID.SC-2. Постачальники (розпорядники) інформаційних систем, товарів і послуг для власних ІКС ідентифіковано, рівень їх критичності оцінено у відповідності до політики управління ризиками кібербезпеки з урахуванням ризиків, притаманних системі постачання			

1	2	3	4	5
27.	ID.SC-3. Постачальники товарів і послуг та партнери, у відповідності до договору, можуть впроваджувати заходи, спрямовані на досягнення мети політики інформаційної безпеки/кібербезпеки власних ІКС та плану управління ризиками постачання.			
28.	ID.SC-4. Постачальники товарів і послуг та партнери регулярно оцінюються за допомогою аудитів, результатів тестів або інших форм оцінки, щоб підтвердити, що вони виконують свої договірні зобов'язання.			
29.	ID.SC-5. З Постачальниками здійснюється планування та тестування реагування за відповідними політиками реагування на кіберінциденти та відновлення стану кібербезпеки			

№ з/п	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту	Заходи для досягнення цільового профіля за роками
1	2	3	4	5
Кіберзахист (PR)				
PR.AC Управління ідентифікацією, автентифікацією та контроль доступу				
30.	PR.AC-1. Ідентифікатори та дані автентифікації для авторизованих користувачів, адміністраторів та процесів призначаються, верифікуються, адмініструються, відкликаються (скасовуються) та перевіряються			
31.	PR.AC-2. Фізичний доступ до власних ІКС захищений та управляється			
32.	PR.AC-3. Здійснюється контроль та управління віддаленого доступу			
33.	PR.AC-4. Права доступу встановлено із застосуванням принципів мінімальних привілеїв та розподілу обов'язків			

1	2	3	4	5
34.	PR.AC-5. Цілісність електронної комунікаційної мережі захищено (наприклад, сегментація мережі)			
35.	PR.AC-6. Ідентичність особи підтверджується і прив'язується до облікових даних та затверджується під час взаємодії			
36.	PR.AC-7. Автентифікація користувачів, адміністраторів, пристроїв та інших активів здійснюється (наприклад методами однофакторної, багатофакторної автентифікації) відповідно до встановленого ризику порушення безпеки			
	PR.AT Обізнаність та навчання			
37.	PR.AT-1. Усі співробітники власних ІКС обізнані та пройшли підготовку з питань кібербезпеки			
38.	PR.AT-2. Користувачі (адміністратори) з перевагами доступу розуміють свої обов'язки з питань кібербезпеки			
39.	PR.AT-3. Партнери організації розуміють свої обов'язки з питань кібербезпеки			
40.	PR.AT-4. Керівництво власних ІКС розуміє свої обов'язки з питань кібербезпеки			
41.	PR.AT-5. Персонал із забезпечення фізичної та інформаційної безпеки розуміє свої обов'язки			
	PR.DS Безпека даних			
42.	PR.DS-1. Дані, що зберігаються, захищено			
43.	PR.DS-2. Дані, що передаються, захищено			
44.	PR.DS-3. Управління активами здійснюється з дотриманням правил видалення, передачі та розміщення			
45.	PR.DS-4. Необхідні спроможності для забезпечення доступності активів створено та підтримуються			
46.	PR.DS-5. Захист від витоку даних впроваджено			

1	2	3	4	5
47.	PR.DS-6. Механізми перевірки цілісності використовуються для верифікації програмного забезпечення, програмно-апаратних засобів та цілісності інформації			
48.	PR.DS-7. Середовища розробки та тестування відокремлені від виробничого середовища			
49.	PR.DS-8. Механізми перевірки цілісності використовуються для перевірки цілісності обладнання			
PR.IP Процеси та процедури кіберзахисту				
50.	PR.IP-1. Базова конфігурація інформаційно-телекомунікаційних систем/систем управління виробничими процесами створена й підтримується			
51.	PR.IP-2. Життєвий цикл розробки, експлуатації та управління системами (SDLC) впроваджено			
52.	PR.IP-3. Процеси (заходи) управління змінами конфігурації впроваджено			
53.	PR.IP-4. Резервне копіювання інформації проводиться, підтримується та періодично тестується			
54.	PR.IP-5. Правила (політика) та норми фізичної безпеки операційного середовища та обладнання організації (власних ІКС) виконуються			
55.	PR.IP-6. Дані знищуються відповідно до політики безпеки			
56.	PR.IP-7. Процеси кіберзахисту постійно вдосконалюються			
57.	PR.IP-8. Інформація про ефективність технологій захисту розподіляється			
58.	PR.IP-9. Плани реагування (реагування на кіберінциденти та забезпечення безперервності бізнесу) і плани відновлення (відновлення після кіберінциденту та відновлення після аварії) наявні та управляються			
59.	PR.IP-10. Плани реагування та відновлення тестуються			
60.	PR.IP-11. Кібербезпека, внесена до практики роботи з персоналом (наприклад, деініціалізація, перевірка персоналу)			
61.	PR.IP-12. План управління вразливостями розроблено й впроваджено			

1	2	3	4	5
	PR.MA Технічне обслуговування			
62.	PR.MA-1. Технічне обслуговування та ремонт активів власних ІКС виконуються та своєчасно документуються з використанням визначених та контрольованих засобів			
63.	PR.MA-2. Дистанційне обслуговування активів власних ІКС схвалено, задокументовано та виконується в спосіб, що унеможливлює несанкціонований доступ			
	PR.PT Технології кіберзахисту			
64.	PR.PT-1. Записи аудиту (журналів подій) визначено, задокументовано, впроваджено й перевірено відповідно до політик, правил, процедур з безпеки			
65.	PR.PT-2. Змінні носії захищено, а їх використання обмежено відповідно до правил, процедур з безпеки			
66.	PR.PT-3. Контроль доступу до систем і активів здійснюється із застосуванням принципу мінімальних привілеїв			
67.	PR.PT-4. Телекомунікаційні мережі та мережі управління захищено			
68.	PR.PT-5. Упровадження механізмів на власних ІКС для досягнення вимог до стійкості у разі надзвичайних ситуацій та інцидентів у кіберпросторі			

№ з/п	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту	Заходи для досягнення цільового профіля за роками
1	2	3	4	5
	Виявлення кіберінцидентів (DE)			
	DE.AE Аномалії та кіберінциденти			
69.	DE.AE-1. Еталони мережевих операцій та очікуваних потоків даних для користувачів і систем встановлені та управляються			

1	2	3	4	5
70.	DE.AE-2. Існує практика аналізу виявлених подій			
71.	DE.AE-3. Дані про кіберінциденти агрегуються та корелюються з декількох джерел і датчиків			
72.	DE.AE-4. Існує процес визначення можливих впливів кіберінцидентів			
73.	DE.AE-5. Пороги оповіщення про кіберінциденти встановлено			
	DE.CM Безперервний моніторинг кібербезпеки			
74.	DE.CM-1. Телекомунікаційна мережа (власних ІКС) відстежується для виявлення потенційних кіберінцидентів			
75.	DE.CM-2. Фізичне середовище відстежується для виявлення потенційних кіберінцидентів			
76.	DE.CM-3. Активність персоналу відстежується для виявлення потенційних кіберінцидентів			
77.	DE.CM-4. Шкідливий код виявляється			
78.	DE.CM-5. Несанкціонований програмний продукт виявлено			
79.	DE.CM-6. Активність зовнішнього постачальника товарів і послуг відстежується з метою виявлення потенційних кіберінцидентів			
80.	DE.CM-7. Моніторинг Неавторизованого персоналу, з'єднань, пристроїв і програмного забезпечення здійснюється на постійній основі			
81.	DE.CM-8. Сканування вразливостей виконується			
	DE.DP Процеси виявлення кіберінцидентів			
82.	DE.DP-1. Обов'язки щодо виявлення кіберінцидентів чітко визначено задля забезпечення звітності			
83.	DE.DP-2. Заходи виявлення кіберінцидентів відповідають всім застосованим вимогам.			
84.	DE.DP-3. Процеси виявлення кіберінцидентів протестовані			
85.	DE.DP-4. Інформацію про виявлені кіберінциденти повідомлено партнерів організації			
86.	DE.DP-5. Процеси виявлення кіберінцидентів постійно вдосконалюються			

№ з/п	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту	Заходи для досягнення цільового профіля за роками
1	2	3	4	5
Реагування на кіберінциденти (RS)				
RS.RP Планування реагування				
87.	RS.RP-1. План реагування виконується під час або після події			
RS.CO Комунікації				
88.	RS.CO-1. Персонал знає свої обов'язки та порядок дій у ситуаціях, коли необхідне реагування на кіберінциденти			
89.	RS.CO-2. Факти про кіберінциденти задокументовано та повідомляються відповідно до встановлених критерій			
90.	RS.CO-3. Здійснюється обмін інформацією про кіберінциденти відповідно до планів реагування			
91.	RS.CO-4. Координація з партнерами організації проводиться відповідно до планів реагування			
92.	RS.CO-5. З метою досягнення ширшої ситуативної обізнаності щодо стану кібербезпеки здійснюється обмін інформацією із основними суб'єктами національної системи кібербезпеки та зовнішніми партнерами організації			
RS.AN Аналіз				
93.	RS.AN-1. Повідомлення від систем виявлення кіберінцидентів досліджуються			
94.	RS.AN-2. Вплив кіберінциденту усвідомлено			
95.	RS.AN-3. Експертиза проводиться			
96.	RS.AN-4. Кіберінциденти класифіковано відповідно до планів реагування. Електронні докази збираються та фіксуються належним чином			

1	2	3	4	5
97.	RS.AN-5. Процеси для отримання, аналізу та реагування на вразливості, що розкриваються для організації з внутрішніх та зовнішніх джерел (наприклад, внутрішні тести, бюлетені з безпеки або дослідники проблем безпеки)			
RS.MI Мінімізація наслідків				
98.	RS.MI-1. Кіберінциденти стримано			
99.	RS.MI-2. Наслідки кіберінцидентів мінімізовано			
100.	RS.MI-3. Вперше виявлені вразливості усунене або задокументовано як прийняті ризики			
RS.IM Удосконалення				
101.	RS.IM-1. У планах реагування враховано отриманий досвід			
102.	RS.IM-2. Плани реагування оновлено			

№ з/п	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту	Заходи для досягнення цільового профіля за роками
1	2	3	4	5
Відновлення стану кібербезпеки (RC)				
RC.RP Планування відновлення				
103.	RC.RP-1. План відновлення виконується під час або після кіберінцидентів			
RC.IM Удосконалення				
104.	RC.IM-1. Плани відновлення враховують отриманий досвід			
105.	RC.IM-2. Плани відновлення оновлено			
RC.CO Комунікації				
106.	RC.CO-1. Процес зв’язків з громадськістю організовано та є керованим			

1	2	3	4	5
107.	RC.CO-2. Репутацію після кіберінцидентів відновлюється			
108.	RC.CO-3. Заходи з відновлення повідомлено внутрішнім та зовнішнім партнерам організації, а також керівництву			

Таблиця 3

ОЦІНЮВАННЯ
заходів кіберзахисту за статусом реалізації

№ з/п	Заходи кіберзахисту	Статус			
		реалізовано	у процесі реалізації	розглядається	не потребується
1	2	3	4	5	6
Ідентифікація ризиків кібербезпеки (ID)					
ID.AM Управління активами					
1.	ID.AM-1. Фізичне обладнання та системи на власних ІКС ідентифіковано та задокументовано.	☐	☐	☐	☐
2.	ID.AM-2. Програмне забезпечення, що використовуються власними ІКС для надання життєво важливих послуг та функцій, ідентифіковано та задокументовано.	☐	☐	☐	☐
3.	ID.AM-3. Електронні комунікації та потоки даних власних ІКС ідентифіковано та задокументовано.	☐	☐	☐	☐
4.	ID.AM-4. Зовнішні інформаційні та інформаційно-комунікаційні системи, промислові системи, які взаємодіють з інформаційно-комунікаційними та іншими системами власних ІКС обліковано.	☐	☐	☐	☐
5.	ID.AM-5. Критичність активів (обладнання, устаткування, даних, програмного забезпечення) власних ІКС визначено відповідно до оцінки їх впливу на надання життєво важливих послуг та функцій власних ІКС.	☐	☐	☐	☐

1	2	3	4	5	6
6.	ID.AM-6. Обов'язки штатного персоналу власних ІКС та персоналу партнерів організації (наприклад – постачальників, клієнтів, тощо) щодо забезпечення кібербезпеки визначено та закріплено у відповідних документах.	☐	☐	☐	☐
	ID.BE Середовище надання життєво важливих послуг та функцій				
7.	ID.BE-1. Роль власних ІКС в ланцюгу постачання товарів і послуг визначено та повідомлено всім постачальникам організації.	☐	☐	☐	☐
8.	ID.BE-2. Місце та роль власних ІКС в системі надання життєво важливих послуг та функцій сектору (підсектору) критичної інфраструктури визначено і повідомлено всім постачальникам організації.	☐	☐	☐	☐
9.	ID.BE-3. Пріоритетність цілей, завдань і заходів щодо забезпечення кібербезпеки, надання життєво важливих послуг та функцій встановлено та повідомлено.	☐	☐	☐	☐
10.	ID.BE-4. Залежності та найважливіші процеси для забезпечення надання життєво важливих послуг та функцій встановлено.	☐	☐	☐	☐
11.	ID.BE-5. Вимоги до стійкості власних ІКС щодо забезпечення надання життєво важливих послуг та функцій встановлено.	☐	☐	☐	☐
	ID.GV Управління безпекою				
12.	ID.GV-1. Правила (політики) кібербезпеки власних ІКС встановлено та задокументовано	☐	☐	☐	☐
13.	ID.GV-2. Обов'язки щодо забезпечення кібербезпеки власних ІКС скоординовано та узгоджено з обов'язками персоналу власних ІКС та із зовнішніми партнерами	☐	☐	☐	☐
14.	ID.GV-3. Правові та нормативні вимоги щодо забезпечення кібербезпеки власних ІКС, в тому числі зобов'язання щодо захисту недоторканості особистого життя (приватності), усвідомлено та управління ними здійснюється	☐	☐	☐	☐
15.	ID.GV-4. Процеси управління безпекою та управління ризиками спрямовано на вирішення питання оброблення ризиків кібербезпеки	☐	☐	☐	☐
	ID.RA Оцінка ризиків				
16.	ID.RA-1. Вразливості активів власних ІКС проаналізовано, ідентифіковано та задокументовано	☐	☐	☐	☐

1	2	3	4	5	6
17.	ID.RA-2. Інформацію про загрози безпеки та вразливості отримано з форумів обміну інформацією та офіційних джерел	☐	☐	☐	☐
18.	ID.RA-3. Загрози кібербезпеки (модель загроз) як внутрішні, так і зовнішні визначено й задокументовано	☐	☐	☐	☐
19.	ID.RA-4. Потенційні наслідки (рівень шкоди),які можуть завдати загрози в наслідок їх реалізації на безперервне надання життєво важливих послуг та функцій та ймовірності їх реалізації визначено	☐	☐	☐	☐
20.	ID.RA-5. Для визначення ризику застосовуються данні щодо загроз, вразливостей, їх ймовірностей та рівня шкоди використано для визначення ризику кібербезпеки	☐	☐	☐	☐
21.	ID.RA-6. Заходи реагування на ризик кібербезпеки визначено та їх пріоритетність встановлено	☐	☐	☐	☐
	ID.RM Стратегія управління ризиками організації				
22.	ID.RM-1. Процеси управління ризиками визначено, узгоджено із партнерами організації та управляються	☐	☐	☐	☐
23.	ID.RM-2. Допустимий рівень ризику кібербезпеки визначено та чітко виражено	☐	☐	☐	☐
24.	ID.RM-3. Визначення допустимого рівня ризику грунтується на ролі власних ІКС як складової частини сектору критичної інфраструктури та аналізі ризиків, притаманних відповідному сектору критичної інфраструктури	☐	☐	☐	☐
	ID.SC Управління ризиками системи постачання				
25.	ID.SC-1. Процеси управління ризиками кібербезпеки системи постачання визначено, узгоджено з партнерами організації та управляються	☐	☐	☐	☐
26.	ID.SC-2. Постачальники (розпорядники) інформаційних систем, товарів і послуг для власних ІКС ідентифіковано, рівень їх критичності оцінено у відповідності до політики управління ризиками кібербезпеки з урахуванням ризиків, притаманних системі постачання	☐	☐	☐	☐
27.	ID.SC-3. Постачальники товарів і послуг та партнери, у відповідності до договору, можуть впроваджувати заходи, спрямовані на досягнення мети політики інформаційної безпеки/кібербезпеки власних ІКС та плану управління ризиками постачання	☐	☐	☐	☐

1	2	3	4	5	6
28.	ID.SC-4. Постачальники товарів і послуг та партнери регулярно оцінюються за допомогою аудитів, результатів тестів або інших форм оцінки, щоб підтвердити, що вони виконують свої договірні зобов'язання.	☐	☐	☐	☐
29.	ID.SC-5. З Постачальниками здійснюється планування та тестування реагування за відповідними політиками реагування на кіберінциденти та відновлення стану кібербезпеки	☐	☐	☐	☐

№ з/п	Заходи кіберзахисту	Статус			
		реалізо-вано	у процесі реалізації	розгляда-ється	не потребує-ться
1	2	3	4	5	6
	Кіберзахист (PR)				
	PR.AC Управління ідентифікацією, автентифікацією та контроль доступу				
30.	PR.AC-1. Ідентифікатори та дані автентифікації для авторизованих користувачів, адміністраторів та процесів призначаються, верифікуються, адмініструються, відкликаються (скасовуються) та перевіряються	☐	☐	☐	☐
31.	PR.AC-2. Фізичний доступ до власних ІКС захищений та управляється	☐	☐	☐	☐
32.	PR.AC-3. Здійснюється контроль та управління віддаленого доступу	☐	☐	☐	☐
33.	PR.AC-4. Права доступу встановлено із застосуванням принципів мінімальних привілеїв та розподілу обов'язків	☐	☐	☐	☐
34.	PR.AC-5. Цілісність електронної комунікаційної мережі захищено (наприклад, сегментація мережі)	☐	☐	☐	☐
35.	PR.AC-6. Ідентичність особи підтверджується і прив'язується до облікових даних та затверджується під час взаємодії				
36.	PR.AC-7. Автентифікація користувачів, адміністраторів, пристроїв та інших активів здійснюється (наприклад методами однофакторної, багатофакторної автентифікації) відповідно до встановленого ризику порушення безпеки	☐	☐	☐	☐

1	2	3	4	5	6
PR.AT Обізнаність та навчання					
37.	PR.AT-1. Усі співробітники власних ІКС обізнані та пройшли підготовку з питань кібербезпеки	☐	☐	☐	☐
38.	PR.AT-2. Користувачі (адміністратори) з превагами доступу розуміють свої обов`язки з питань кібербезпеки	☐	☐	☐	☐
39.	PR.AT-3. Партнери організації розуміють свої обов'язки з питань кібербезпеки	☐	☐	☐	☐
40.	PR.AT-4. Керівництво власних ІКС розуміє свої обов'язки з питань кібербезпеки	☐	☐	☐	☐
41.	PR.AT-5. Персонал із забезпечення фізичної та інформаційної безпеки розуміє свої обов'язки	☐	☐	☐	☐
PR.DS Безпека даних					
42.	PR.DS-1. Дані, що зберігаються, захищено	☐	☐	☐	☐
43.	PR.DS-2. Дані, що передаються, захищено	☐	☐	☐	☐
44.	PR.DS-3. Управління активами здійснюється з дотриманням правил видалення, передачі та розміщення	☐	☐	☐	☐
45.	PR.DS-4. Необхідні спроможності для забезпечення доступності активів створено та підтримуються	☐	☐	☐	☐
46.	PR.DS-5. Захист від витоку даних впроваджено	☐	☐	☐	☐
47.	PR.DS-6. Механізми перевірки цілісності використовуються для верифікації програмного забезпечення, програмно-апаратних засобів та цілісності інформації	☐	☐	☐	☐
48.	PR.DS-7. Середовища розробки та тестування відокремлені від виробничого середовища	☐	☐	☐	☐
49.	PR.DS-8. Механізми перевірки цілісності використовуються для перевірки цілісності обладнання				
PR.IP Процеси та процедури кіберзахисту					
50.	PR.IP-1. Базова конфігурація інформаційно-телекомунікаційних систем/систем управління виробничими процесами створена й підтримується	☐	☐	☐	☐

1	2	3	4	5	6
51.	PR.IP-2. Життєвий цикл розробки, експлуатації та управління системами (SDLC) впроваджено	☐	☐	☐	☐
52.	PR.IP-3. Процеси (заходи) управління змінами конфігурації впроваджено	☐	☐	☐	☐
53.	PR.IP-4. Резервне копіювання інформації проводиться, підтримується та періодично тестується	☐	☐	☐	☐
54.	PR.IP-5. Правила (політика) та норми фізичної безпеки операційного середовища та обладнання організації (власних ІКС) виконуються	☐	☐	☐	☐
55.	PR.IP-6. Дані знищуються відповідно до політики безпеки	☐	☐	☐	☐
56.	PR.IP-7. Процеси кіберзахисту постійно вдосконалюються	☐	☐	☐	☐
57.	PR.IP-8. Інформація про ефективність технологій захисту розподіляється				
58.	PR.IP-9. Плани реагування (реагування на кіберінциденти та забезпечення безперервності бізнесу) і плани відновлення (відновлення після кіберінциденту та відновлення після аварії) наявні та управляються	☐	☐	☐	☐
59.	PR.IP-10. Плани реагування та відновлення тестуються	☐	☐	☐	☐
60.	PR.IP-11. Кібербезпека, внесена до практики роботи з персоналом (наприклад, деініціалізація, перевірка персоналу)				
61.	PR.IP-12. План управління вразливостями розроблено і впроваджено	☐	☐	☐	☐
	PR.MA Технічне обслуговування				
62.	PR.MA-1. Технічне обслуговування та ремонт активів ОКІ виконуються та своєчасно документуються з використанням визначених та контрольованих засобів	☐	☐	☐	☐
63.	PR.MA-2. Дистанційне обслуговування активів власних ІКС схвалено, задокументовано та виконується в спосіб, що унеможливлює несанкціонований доступ	☐	☐	☐	☐
	PR.PT Технології кіберзахисту				
64.	PR.PT-1. Записи аудиту (журналів подій) визначено, задокументовано, впроваджено й перевірено відповідно до політик, правил, процедур з безпеки	☐	☐	☐	☐
65.	PR.PT-2. Змінні носії захищено, а їх використання обмежено відповідно до правил, процедур з безпеки	☐	☐	☐	☐

1	2	3	4	5	6
66.	PR.PT-3. Контроль доступу до систем і активів здійснюється із застосуванням принципу мінімальних привілеїв	☐	☐	☐	☐
67.	PR.PT-4. Електронні комунікаційні мережі та мережі управління захищено	☐	☐	☐	☐
68.	PR.PT-5. Упровадження механізмів на власних ІКС для досягнення вимог до стійкості у разі надзвичайних ситуацій та інцидентів у кіберпросторі	☐	☐	☐	☐

№ з/п	Заходи кіберзахисту	Статус			
		реалізовано	у процесі реалізації	розглядається	не потребується
1	**2**	**3**	**4**	**5**	**6**
Виявлення кіберінцидентів (DE)					
Виявлення кіберінцидентів (DE)					
69.	DE.AE-1. Еталони мережевих операцій та очікуваних потоків даних для користувачів і систем встановлені та управляються	☐	☐	☐	☐
70.	DE.AE-2. Існує практика аналізу виявлених подій	☐	☐	☐	☐
71.	DE.AE-3. Дані про кіберінциденти агрегуються та корелюються з декількох джерел і датчиків	☐	☐	☐	☐
72.	DE.AE-4. Існує процес визначення можливих впливів кіберінцидентів	☐	☐	☐	☐
73.	DE.AE-5. Пороги оповіщення про кіберінциденти встановлено	☐	☐	☐	☐
DE.CM Безперервний моніторинг кібербезпеки					
74.	DE.CM-1. Телекомунікаційна мережа (власних ІКС) відстежується для виявлення потенційних кіберінцидентів	☐	☐	☐	☐
75.	DE.CM-2. Фізичне середовище відстежується для виявлення потенційних кіберінцидентів	☐	☐	☐	☐
76.	DE.CM-3. Активність персоналу відстежується для виявлення потенційних кіберінцидентів	☐	☐	☐	☐

1	2	3	4	5	6
77.	DE.CM-4. Шкідливий код виявляється	☐	☐	☐	☐
78.	DE.CM-5. Несанкціонований програмний продукт виявлено	☐	☐	☐	☐
79.	DE.CM-6. Активність зовнішнього постачальника товарів і послуг відстежується з метою виявлення потенційних кіберінцидентів	☐	☐	☐	☐
80.	DE.CM-7. Моніторинг Неавторизованого персоналу, з'єднань, пристроїв і програмного забезпечення здійснюється на постійній основі	☐	☐	☐	☐
81.	DE.CM-8. Сканування вразливостей виконується	☐	☐	☐	☐
DE.DP Процеси виявлення кіберінцидентів					
82.	DE.DP-1. Обов'язки щодо виявлення кіберінцидентів чітко визначено задля забезпечення звітності	☐	☐	☐	☐
83.	DE.DP-2. Заходи виявлення кіберінцидентів відповідають всім застосованим вимогам.	☐	☐	☐	☐
84.	DE.DP-3. Процеси виявлення кіберінцидентів протестовані	☐	☐	☐	☐
85.	DE.DP-4. Інформацію про виявлені кіберінциденти повідомлено партнерів організації	☐	☐	☐	☐
86.	DE.DP-5. Процеси виявлення кіберінцидентів постійно вдосконалюються	☐	☐	☐	☐

№ з/п	Заходи кіберзахисту	Статус			
		реалізовано	у процесі реалізації	розглядається	не потребується
1	2	3	4	5	6
Реагування на кіберінциденти (RS)					
RS.RP Планування реагування					
87.	RS.RP-1. План реагування виконується під час або після події	☐	☐	☐	☐
RS.CO Комунікації					

1	2	3	4	5	6
88.	RS.CO-1. Персонал знає свої обов'язки та порядок дій у ситуаціях, коли необхідне реагування на кіберінциденти	☐	☐	☐	☐
89.	RS.CO-2. Факти про кіберінциденти задокументовано та повідомляються відповідно до встановлених критерій	☐	☐	☐	☐
90.	RS.CO-3. Здійснюється обмін інформацією про кіберінциденти відповідно до планів реагування	☐	☐	☐	☐
91.	RS.CO-4. Координація з партнерами організації проводиться відповідно до планів реагування	☐	☐	☐	☐
92.	RS.CO-5. З метою досягнення ширшої ситуативної обізнаності щодо стану кібербезпеки здійснюється обмін інформацією із основними суб'єктами національної системи кібербезпеки та зовнішніми партнерами організації	☐	☐	☐	☐
RS.AN Аналіз					
93.	RS.AN-1. Повідомлення від систем виявлення кіберінцидентів досліджуються	☐	☐	☐	☐
94.	RS.AN-2. Вплив кіберінциденту усвідомлено	☐	☐	☐	☐
95.	RS.AN-3. Експертиза проводиться	☐	☐	☐	☐
96.	RS.AN-4. Кіберінциденти класифіковано відповідно до планів реагування. Електронні докази збираються та фіксуються належним чином	☐	☐	☐	☐
97.	RS.AN-5. Процеси для отримання, аналізу та реагування на вразливості, що розкриваються для організації з внутрішніх та зовнішніх джерел (наприклад, внутрішні тести, бюлетені з безпеки або дослідники проблем безпеки)	☐	☐	☐	☐
RS.MI Мінімізація наслідків					
98.	RS.MI-1. Кіберінциденти стримано	☐	☐	☐	☐
99.	RS.MI-2. Наслідки кіберінцидентів мінімізовано	☐	☐	☐	☐
100	RS.MI-3. Вперше виявлені вразливості усунене або задокументовано як прийняті ризики	☐	☐	☐	☐
RS.IM Удосконалення					
101	RS.IM-1. У планах реагування враховано отриманий досвід	☐	☐	☐	☐

1	2	3	4	5	6
102	RS.IM-2. Плани реагування оновлено	☐	☐	☐	☐

№ з/п	Заходи кіберзахисту	Статус			
		реалізовано	у процесі реалізації	розглядається	не потребується
1	2	3	4	5	6
Відновлення стану кібербезпеки (RC)					
RC.RP Планування відновлення					
103.	RC.RP-1. План відновлення виконується під час або після кіберінцидентів	☐	☐	☐	☐
RC.IM Удосконалення					
104.	RC.IM-1. Плани відновлення враховують отриманий досвід	☐	☐	☐	☐
105.	RC.IM-2. Плани відновлення оновлено	☐	☐	☐	☐
RC.CO Комунікації					
106.	RC.CO-1. Процес зв'язків з громадськістю організовано та є керованим	☐	☐	☐	☐
107.	RC.CO-2. Репутацію після кіберінцидентів відновлюється	☐	☐	☐	☐
108.	RC.CO-3. Заходи з відновлення повідомлено внутрішнім та зовнішнім партнерам організації, а також керівництву	☐	☐	☐	☐

Приклад заповнення Таблиці 1:

№ з/п	Клас заходів кіберзахисту	Всього підкатегорій заходів кіберзахисту	Статус (кількість та % заходів за кожною категорією)			
			реалізовано	у процесі реалізації	розглядається	не потребується
1	Ідентифікація ризиків кібербезпеки (ID)	29	6	7	16	0
			20,7%	24,1%	55,2%	0%
2	Кіберзахист (PR)	39	20	3	10	2
			57,1%	8,6%	28,6%	5,7%
3	Виявлення кіберінцедентів (DE)	18	7	0	11	0
			38,9%	0%	61,1%	0%
4	Реагування на кіберінцеденти (RS)	16	2	0	13	0
			13,3%	0%	86,7%	0%
5	Відновлення стану кібебезпеки (RC)	6	3	0	3	0
			50%	0%	50%	0%
6	ВСЬОГО:	108	38	10	53	2
			36,9%	9,7%	51,5%	1,9%

Керівник апарату
обласної військової адміністрації  Катерина БОЙКО