

ЗАТВЕРДЖЕНО

Наказ Служби безпеки України і  
Адміністрації Державної служби  
спеціального зв'язку та захисту  
інформації України  
19 грудня 2024 року № 627 / 772

## РЕКОМЕНДАЦІЇ

### з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент»

#### I. Загальні положення

1. Ці Рекомендації призначені для операторів критичної інфраструктури, які розробляють план захисту об'єкта критичної інфраструктури (далі – ОКІ) за проектною загрозою національного рівня «кібератака/кіберінцидент» (далі – Рекомендації).

2. Рекомендації розроблено відповідно до Законів України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах», постанови Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», постанови Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», постанови Кабінету Міністрів України від 14.10.2022 № 1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури», постанови Кабінету Міністрів України від 04.08.2023 № 818 «Деякі питання паспортизації об'єктів критичної інфраструктури» та з урахуванням Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (зі змінами), Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570, Проектних загроз критичній інфраструктурі національного рівня, затверджених наказом Адміністрації Держспецзв'язку від 28.07.2023 № 219/ДСК.

3. Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і не є обов'язковими для використання.

4. У цих Рекомендаціях терміни вживаються в такому значенні:  
унікальний ідентифікатор об'єкта критичної інформаційної інфраструктури – унікальний буквено-цифровий номер, який присвоюється кожному індивідуально визначеному об'єкту критичної інформаційної інфраструктури (далі – ОКІІ) після внесення його до державного реєстру ОКІІ.

Інші терміни вживаються у значеннях, наведених в Законах України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», постанові Кабінету Міністрів України від 04.08.2023 № 818 «Деякі питання паспортизації об'єктів критичної інфраструктури» та Методичних рекомендаціях щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (зі змінами), Методичних рекомендаціях щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570.

5. План захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» (далі – План захисту) розробляється оператором критичної інфраструктури (далі – оператор) відповідно до форми, затвердженої наказом Служби безпеки України і Адміністрації Держспецзв'язку.

6. Інформація, яка вноситься до Плану захисту, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства у сфері захисту інформації.

7. План захисту подається оператором на погодження функціональним органам у сфері захисту критичної інфраструктури (далі – функціональні органи) разом із супровідним листом і копією загальної характеристики ОКІ.

Підписує супровідний лист і затверджує План захисту керівник оператора або особа, яка виконує його обов'язки.

Оператору необхідно надати дозвіл уповноваженому підрозділу (органу) Служби безпеки України на копіювання поданих документів, що містять інформацію з обмеженим доступом, в порядку, визначеному законодавством.

План захисту, поданий з порушенням встановлених вимог, повертається оператору для усунення недоліків.

8. План захисту погоджується та подається у такій послідовності:

1) до уповноваженого підрозділу (органу) Адміністрації Держспецзв'язку;

2) до уповноваженого підрозділу (органу) Служби безпеки України.

9. У випадку погодження Плану захисту уповноваженим підрозділом (органом) Адміністрації Держспецзв'язку та наявності зауважень (пропозицій) до Плану захисту від уповноваженого підрозділу (органу) Служби безпеки України, План захисту потребує повторного погодження кожним із вказаних уповноважених підрозділів (органів).

10. Порядок перегляду Плану захисту передбачений пунктом 12 Порядку розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 04.08.2023 № 818.

11. Оператор визначає об'єкти інформаційної інфраструктури (далі – ОІ), що експлуатуються на ОКІ та інформація про які вноситиметься до Плану захисту.

В обов'язковому порядку до Плану захисту вносяться відомості про всі ОКІІ, що експлуатуються на ОКІ.

Інформація про інші ОІ (автоматизовані, інформаційні, електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами) ОКІ, які не віднесено до ОКІІ, але є необхідними для забезпечення безперервного та стійкого функціонування ОКІ, також підлягає обов'язковому внесенню до Плану захисту.

До Плану захисту не вносяться відомості про окремі ПЕОМ, які не мають підключень до будь-яких інформаційно-комунікаційних систем або мереж (автоматизовані системи класу «1»).

## II. Порядок заповнення Плану захисту

1. На титульній сторінці Плану захисту зазначаються:  
гриф обмеження доступу;  
назва ОКІ та унікальний реєстровий номер ОКІ.

2. В пункті 1 Плану захисту зазначаються:

в Таблиці 1 Плану захисту – повна та скорочена назви ОІ. Унікальний ідентифікатор ОКІІ зазначається у випадку, якщо ОІ віднесено до ОКІІ I або II категорії критичності;

в Таблиці 2 Плану захисту – інформація стосовно подання та внесення відомостей про ОКІІ до державного реєстру ОКІІ. Заповнюється у випадку, якщо ОІ віднесено до ОКІІ I або II категорії критичності;

в Таблиці 3 Плану захисту – стан виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Необхідно вказати відповідальну особу за виконання вимог до кіберзахисту ОКІ з числа керівників

оператора, стан виконання цих вимог у відсотках на момент заповнення Плану захисту та зазначити запланований термін виконання вимог у повному обсязі;

в Таблиці 4 Плану захисту – відомості про підрозділ або призначених осіб, на яких покладається забезпечення захисту інформації та контроль за станом кіберзахисту ОКІ, а саме прізвище, власне ім'я, по батькові (у разі наявності), займана посада, назва підрозділу та контактні дані (номер телефону, e-mail адреса).

3. В Таблиці 5 пункту 2 Плану захисту зазначаються:

визначена життєво важлива функція та/або послуга ОКІ, надання якої забезпечується (підтримується) ОП. Зазначається відповідно до Переліку секторів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», у разі забезпечення (підтримки) ОП відповідної послуги;

вид інформації за порядком доступу, яка обробляється або планується для оброблення на ОП (вибрати з наданого переліку). У разі якщо, в переліку не зазначено вид інформації, яка обробляється або планується для оброблення на ОП, в графі «Інше» зазначити, яка саме;

використання незахищеного середовища для передачі інформації в межах ОП (відповідь «Так» обирається для автоматизованих систем класу «3», відповідь «Ні» обирається для автоматизованих систем класу «2»);

підключення до мережі Інтернет або до інших інформаційно-комунікаційних систем (далі – ІКС), які не входять до складу ОП. У разі підключення до мережі Інтернет вказати повне найменування постачальника електронних комунікаційних мереж та/або послуг і чи має постачальник електронних комунікаційних мереж та/або послуг захищені вузли доступу до глобальних мереж передачі даних зі створеними комплексними системами захисту інформації з підтвердженою відповідністю, перелік IP-адрес, що використовуються, та контактні дані постачальників електронних комунікаційних мереж та/або послуг (номер телефону, e-mail адреса). У разі підключення до інших ІКС, які не входять до складу ОП, але мають фізичне підключення до нього, вказати повне найменування таких ІКС;

використання бездротових технологій (Wi-Fi, Bluetooth тощо). У разі використання вказати, що саме. У випадку, якщо в переліку не зазначено необхідного варіанту, – вписати;

взаємодія ОП з іншими ОП, а саме отримання ОП життєво важливих послуг від інших ОП(ОКІІ), ненадання яких вплине на функціонування ОП. Надання ОП життєво важливих послуг іншим ОП(ОКІІ), неотримання яких вплине на їх функціонування. Описати цю взаємодію, вказати повне найменування іншого ОП, унікальний ідентифікатор ОКІІ (за наявності) та контактні дані (номер телефону, e-mail адреса);

атестат відповідності комплексної системи захисту інформації (далі – КСЗІ) ОП або результати незалежного аудиту ОКІ (за наявності). У разі наявності атестата відповідності КСЗІ ОКІІ або елемента ОКІІ, зазначити який саме (на що саме виданий атестат, номер, дата та ким виданий). Вказати номер

та дату сертифіката відповідності та/або звіту за результатами незалежного аудиту інформаційної безпеки на ОКІ, висновок за результатами аудиту. За наявності іншого документа, що засвідчує відповідність КСЗІ ОКІ, в графі «Інше» зазначити, який саме;

взаємодія з платформами обміну інформацією щодо шкідливого програмного забезпечення (MISP CERT-UA, MISP-UA або інші з переліку) (за наявності), і з якою (якими) саме. В разі, якщо в переліку не зазначено платформи обміну інформацією щодо шкідливого програмного забезпечення, з якою є взаємодія, в графі «Інша» зазначити, яка саме;

взаємодія з командами реагування на кіберінциденти (CERT, CSIRT тощо) (за наявності). У разі, якщо є, вказати найменування команди реагування на кіберінциденти, тип за формою власності (вибрати з переліку), тип за належністю (вибрати з переліку) та контактну інформацію (номер телефону, e-mail адреса) зазначеної команди реагування на кіберінциденти;

взаємодія з центрами управління безпекою (SOC). У разі, якщо є, вказати найменування центру управління безпекою, тип за належністю (вибрати з переліку) та контактну інформацію (номер телефону, e-mail адреса) зазначеного SOC;

використання програмних та/або апаратних засобів:

а) що мають походження або виготовлені державою-агресором;

б) виготовлених фізичними або юридичними особами, щодо яких застосовано персональні спеціальні економічні та інші обмежувальні заходи (санкції) згідно із Законом України «Про санкції»;

в) отриманих на безоплатній основі від фізичних або юридичних осіб.

У разі використання необхідно вказати назви програмних та/або апаратних засобів, компанії-розробника, компанії-постачальника, компанії, що здійснює підтримку такого(их) засобу(ів), наявність плану по заміщенню такого(их) засобу(ів) (для підпунктів «а» і «б»), орієнтовні терміни заміщення такого(их) засобу(ів) (для підпунктів «а» і «б»);

перевірка ефективності заходів щодо захисту ОП від зовнішнього проникнення шляхом виконання тестів на проникнення (Penetration test). У разі проведення такого тестування необхідно стисло описати проведені заходи та результати;

використання механізму здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (Bug Bounty). У разі використання такого механізму необхідно стисло описати вжиті заходи та результати, а також зазначити посилання на публічну пропозицію, де виставляється повна інформація (відповідно до пункту 6 Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16 травня 2023 року № 497).

Також в пункті 2 Плану захисту розміщується:

рисунок загальної функціональної схеми системи (мережі) ОКІ;

опис загальної функціональної схеми системи (мережі) ОКІ та технології обробки інформації, де надається стислий опис роботи системи (мережі) ОКІ (не має перевищувати двох сторінок). Мають бути описані основні функції, завдання, принципи функціонування, технології обробки інформації, вплив на надання життєво важливої(их) функції(й) та/або послуги(г) ОКІ. Опис має давати загальне уявлення про систему (мережу) ОКІ.

4. У таблиці 6 пункту 3 Плану захисту зазначаються властивості проектних загроз національного, секторального та об'єктового (у разі наявності) рівня.

5. Загальний порядок реагування на кібератаки/кіберінциденти, який передбачений пунктом 4 Плану захисту, розробляє підрозділ або призначені особи, на яких покладається забезпечення захисту інформації та контроль за станом кіберзахисту ОКІ.

Основною рекомендацією є вивчення та дослідження сучасних видів кібератак/кіберінцидентів, розроблення методів і механізмів запобігання та протидії можливим кібератакам/кіберінцидентам на постійній основі.

Після виявлення кібератаки/кіберінциденту доцільно:

визначити категорію (рівень) критичності кібератаки/кіберінциденту на поточний момент відповідно до трьох критеріїв критичності кібератаки/кіберінциденту відповідно до пункту 5 розділу III Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570 (далі – Методичні рекомендації № 570);

поінформувати про кібератаку/кіберінцидент урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузеву команду реагування на комп'ютерні надзвичайні події), а також Ситуаційний центр забезпечення кібербезпеки СБУ або відповідний підрозділ регіонального органу СБУ (відповідно до пункту 8 Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19.06.2019 № 518);

вжити невідкладних заходів з нейтралізації/зменшення потенційного негативного ефекту від реалізації кібератаки/кіберінциденту відповідно до розділу IV Методичних рекомендацій № 570;

вжити заходів для відновлення штатного режиму функціонування шляхом усунення інциденту і пом'якшення наслідків від реалізації кіберзагроз або інших умов, якими скористався зловмисник або групи таких осіб відповідно до розділу V Методичних рекомендацій № 570;

пом'якшити наслідки від реалізації кіберзагроз та інших умов, якими скористався зловмисник, відповідно до розділу VI Методичних рекомендацій № 570.

Відповідно до особливостей функціонування та затверджених інструкцій реагування на кіберінциденти на ОКІ рекомендовано описати стисле викладення дій, що виконуються на ОКІ.

6. План кіберзахисту ОКІ, передбачений пунктом 5 Плану захисту, містить мінімальний набір завдань, які в першу чергу (але не обмежуючись ними надалі в діяльності з підвищення рівня кіберзахисту критичної інформаційної інфраструктури) мають бути впроваджені або заплановані для впровадження на ОКІ. План кіберзахисту ОКІ передбачає 5 класів завдань 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.

Клас «Ідентифікація ризиків кібербезпеки» (ID) має на меті розвинути розуміння того, як краще керувати ризиками кібербезпеки для систем, ресурсів, даних та можливостей, тобто визначити, які процедури та інформаційні активи потребують захисту. Він передбачає заходи щодо інвентаризації апаратного та програмного забезпечення, створення політик кібербезпеки, ідентифікації загроз та вразливостей тощо.

Клас «Кіберзахист» (PR) рекомендує запобіжні заходи для захисту, тобто визначає діяльність із розробки та впровадження відповідних методів, засобів, процедур кіберзахисту для забезпечення стійкого, безперервного та безпечного надання життєво важливих функцій та/або послуг. Ці заходи дозволяють обмежити або стримати вплив кіберінцидентів. Основними заходами є керування доступом до інформаційних активів та інформації, захист інформації, регулярне створення резервних копій, захист апаратного забезпечення, керування вразливостями, навчання користувачів, збір і зберігання журналів (логів) реєстрації подій тощо.

Клас «Виявлення кіберінцидентів» (DE) містить заходи, що допомагають розробити та впровадити відповідні заходи для своєчасної ідентифікації кіберінциденту. Наприклад, тестування та оновлення процесів виявлення, ведення та моніторинг журналів (логів) реєстрації подій, розуміння впливу кіберінцидентів, відстеження потоків даних.

Клас «Реагування на кіберінциденти» (RS) містить заходи щодо розробки та впровадження заходів для реагування на кіберінциденти та кібератаки. Реалізація заходів спрямована на зниження потенційного негативного впливу кіберінциденту на надання життєво важливих послуг та функцій, наприклад, створення, тестування та оновлення планів реагування, координація внутрішніх та зовнішніх зацікавлених сторін тощо.

Клас «Відновлення стану кібербезпеки» (RC) допомагає розробити та впровадити відповідні заходи для підтримання стійкості, своєчасного відновлення штатної роботи після кіберінциденту та зменшення негативного впливу кіберінциденту. Такими заходами є розроблення, тестування, оновлення планів відновлення, керування зв'язками з громадськістю, відновлення репутації після кіберінциденту, а також спілкування з внутрішніми та зовнішніми зацікавленими сторонами.

У Плані кіберзахисту рекомендовано заповнити Таблиці 7-11 Плану захисту, де описується поточний стан виконання завдань кіберзахисту та наявні ресурси, а як підтвердження вказати назву документа, номер та дату реєстрації,

в якому підтверджується виконання завдання кіберзахисту. Для заповнення поля «Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси» доцільно використовувати Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601. У разі наявності секторальних вимог або стандартів, або рекомендацій, затверджених відповідною міжнародною організацією (наприклад, МАГАТЕ, ІКАО тощо), перед заповненням Таблиці 7 Плану кіберзахисту доцільно навести перелік відповідних секторальних документів та спосіб їх врахування щодо ОКІ, для яких вони передбачені. При цьому, якщо заходи безпеки застосовуються постійно, рекомендовано наводити підтвердження цього. Також варто зазначити заплановані заходи для виконання завдань кіберзахисту, визначити та вказати відповідальну особу за їх виконання, зазначити запланований термін та додаткові ресурси для реалізації запланованих завдань кіберзахисту.

У випадку, якщо в Плані захисту буде описано декілька ОП, обов'язково зазначати його назву.

Таблиця 7 пункту 5 Плану захисту заповнюється шляхом описання виконання наступних завдань із кіберзахисту:

Завдання 1. Провести ідентифікацію інформаційних, програмних та апаратних ресурсів (програмних та апаратних компонентів, змінних (зовнішніх) пристроїв та носіїв інформації тощо). Доцільно проводити інвентаризацію інформаційних та операційних активів, не рідше ніж раз на рік. Для виконання цього можуть бути заплановані такі заходи:

проведення інвентаризації усього інформаційного та операційного обладнання. Бажано зафіксувати у документі, визначеному керівництвом ОКІ, результати інвентаризації та всі складові, які беруть участь у технологічному процесі обробки та впливають на безпеку ОКІ: точно описує поточну мережу ОКІ, охоплює всі компоненти в межах акредитації ОКІ, визначає рівень деталізації, який вважається необхідним для відстеження та звітування;

бажано створити календарний план змін усього інформаційного та операційного обладнання ОКІ.

Завдання 2. Створити підрозділ (або призначити посадову особу) з інформаційної безпеки, що відповідає за політику інформаційної безпеки, прийняту на ОКІ, та контроль за її дотриманням. Підрозділ або посадова особа повинні бути підпорядковані безпосередньо керівнику ОКІ. Бажано визначити обов'язки персоналу ОКІ, відповідального за планування діяльності з кібербезпеки, та забезпечити його ресурсами для виконання такої діяльності. На виконання цього завдання можуть бути заплановані такі заходи:

на ОКІ затвердити положення про визначення керівної посадової особи, відповідальної за кібербезпеку на всьому ОКІ, в тому числі систем управління технологічними процесами, а також систем, що впливають на безпеку функціонування ОКІ;

затвердити функціональні обов'язки персоналу ОКІ щодо планування діяльності з кібербезпеки та ознайомити з ними;

визначити термін перегляду та оновлення документів з організації діяльності відповідальної особи за кібербезпеку на всьому ОКІ, в тому числі систем управління технологічними процесами, а також систем, що впливають на безпеку функціонування ОКІ;

визначити перелік персоналу ОКІ, відповідального за планування діяльності з кібербезпеки.

Завдання 3. Забезпечити належну взаємодію підрозділів ІТ та кіберзахисту шляхом розроблення Порядку взаємодії та обміну інформацією між підрозділами ІТ та кіберзахисту з урахуванням повноважень підрозділів під час реагування на кіберінциденти.

Завдання 4. Опрацювати вплив відомих вразливостей, тобто виправляти або іншим чином пом'якшувати протягом визначеного проміжку часу усі відомі використовувані вразливості у системах, що підключаються до мережі Інтернет, в першу чергу для важливіших інформаційних активів ОКІ. Для виконання зазначеного завдання можуть бути заплановані заходи:

сканування на наявність вразливостей в інформаційній системі та інстальованих застосунках щотижня та коли виявляються нові вразливості, які потенційно впливають на систему (мережу) ОКІ;

виявлення, виправлення та повідомлення про недоліки системи, що підключаються до мережі Інтернет, враховуючи ризики в першу чергу для важливіших інформаційних активів ОКІ;

виправлення помилок в організаційному процесі управління конфігурацією.

Завдання 5. Залучити сторонню організацію для проведення незалежного аудиту інформаційної безпеки. Для виконання зазначеного завдання можуть бути заплановані заходи:

розробити план оцінювання безпеки та приватності, який описує сферу й охоплює:

заходи захисту та посилені заходи, що підлягають оцінюванню;

процедури оцінювання, які використовуватимуться для визначення заходів;

середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання.

Завдання 6. Забезпечити реагування на інформування постачальниками про виявлені ними інциденти. Для виконання зазначеного завдання можуть бути заплановані заходи:

затвердження договору та процедури інформування між ОКІ та постачальниками про інциденти безпеки;

визначення та задокументування організаційного нагляду, повноваження та обов'язки користувачів щодо постачальників послуг та партнерів;

оцінка та перегляд ризиків ланцюга постачання, пов'язаних з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають.

Завдання 7. Забезпечити реагування на інформування постачальниками про виявлені ними вразливості. Для виконання зазначеного завдання можуть бути заплановані заходи:

за можливості укласти договір та процедури інформування постачальників послуг та партнерів про інциденти безпеки;

оцінка і перегляд ризиків ланцюга постачання, пов'язані з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають.

Завдання 8. Затвердити вимоги щодо кібербезпеки до постачальників послуг та партнерів. Для виконання зазначеного завдання можуть бути заплановані заходи:

розроблення, затвердження та використання стратегії придбання та методи закупівель, для захисту від загроз в ланцюзі постачання визначити та пом'якшити їх;

оцінка і перегляд загроз ланцюга постачання, пов'язаних з постачальниками або підрядниками, системою, системними компонентами або системною послугою, яку вони надають.

Таблиця 8 у пункті 5 Плану захисту заповнюється шляхом описання виконання таких завдань із кіберзахисту:

Завдання 1. Затвердити процедуру ідентифікації та багатофакторної автентифікації користувачів та адміністраторів (парольна політика). Рекомендується впровадити політику та/або процес для всього ОКІ щодо зміни паролів виробника за замовчуванням – для будь-якого/всіх апаратних засобів, програмного та інформаційного перед підключенням до внутрішньої чи зовнішньої мережі. Для виконання зазначеного завдання можуть бути заплановані заходи:

управління паролями шляхом: перевірки, як частини початкового розподілу паролів, особи, групи, ролі або пристрою, який отримує пароль; заборони повторного використання паролів; забезпечення використання механізмів перевірки надійності паролів для їх використання за призначенням;

створення та реалізація процедур для первинного розповсюдження паролів або втрачених/скомпрометованих або пошкоджених паролів, а також для відкликання паролів;

зміна під час першого використання паролів для програмного та апаратного забезпечення, запропонованих розробниками та постачальниками;

зміна/оновлення паролів у щомісячний термін або коли фіксуються кіберінциденти;

захист вмісту паролів від несанкціонованого розкриття та модифікацій;

змінювання паролів для облікових записів груп/ролей при зміні ролей в цих облікових записах;

ведення списку часто використовуваних або скомпрометованих паролів та оновлення його;

заборона використання користувачами часто використовуваних або скомпрометованих паролів;

зберігання паролів за допомогою затвердженого алгоритму гешування, переважно використовуючи ключову геш-функцію.

Завдання 2. Забезпечити використання надійних паролів. Рекомендовано впровадити системну політику використання парольних фраз менеджерів

паролів, щоб полегшити роботу користувачам зберігати достатньо довгі паролі, а при технічній неможливості застосувати та прописати компенсаційні елементи управління з реєстрацію всіх спроб входу до цих інформаційних активів. Для виконання зазначеного завдання можуть бути заплановані заходи:

- формування політики використання парольних фраз і менеджерів паролів;
- надання дозволу користувачеві вибирати довгі паролі та фрази.

Завдання 3. Забезпечувати унікальність облікових даних. Для виконання зазначеного завдання можуть бути заплановані заходи:

- формування політики використання парольних фраз і менеджерів паролів;
- ведення моніторингу використовуваних паролів для облікових записів, програм, служб тощо.

Завдання 4. Затвердити процедуру вчасного видалення облікових даних звільнених працівників. Рекомендовано ввести політику щодо процедури блокування користувачів та доступів до ресурсів після звільнення працівників. Додаткові заходи щодо безпеки персоналу наведені в НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» (пункти: PS-1 Політика та процедури кадрової безпеки; PS-2 Визначення посадового ризику; PS-3 Перевірка персоналу; PS-4 Звільнення персоналу; PS-5 Переведення персоналу; PS-6 Угоди про доступ; PS-7 Безпека зовнішнього персоналу; PS-8 Кадрові санкції).

Завдання 5. Унеможливити отримання зловмисником прав доступу до привілейованих облікових даних адміністраторів або користувачів. Для виконання зазначеного завдання можуть бути заплановані заходи:

- впровадження принципу мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених цілей (призначення, місії), завдань та функцій;

- рекомендувати користувачам системних облікових записів або ролей, які мають доступ до визначених функцій безпеки або інформації, що стосується безпеки, використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій;

- обмеження привілейованих облікових записів в системі.

Завдання 6. Здійснити розподіл мережі на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту. Для виконання цього завдання може бути заплановано проведення заходів щодо:

- заборони всіх підключень до системи (мережі) ОКІ за замовчуванням, якщо вони не дозволені явно (наприклад, через IP-адресу та порт) для певної системної функції;

- встановлення права доступу із застосуванням мінімальних привілеїв та розподілу обов'язків.

Завдання 7. Забезпечити виявлення невдалих спроб входу в систему та перевищення граничної кількості спроб введення пароля. Для виконання

зазначеного завдання можуть бути заплановані заходи, наприклад, шляхи зв'язку між електронними комунікаційними мережами налаштувати через налаштований брандмауер, бастіонний хост, «jump box» або демілітаризовану зону, яка ретельно контролюється, записує в мережеві журнали подій та дозволяє з'єднання авторизованим користувачам лише із визначеними відповідно до їх ролей інформаційними активами. Для виконання зазначеного завдання можуть бути заплановані заходи:

- здійснення маршрутизації до зовнішніх мереж через автентифіковані проксі-сервери на керованих інтерфейсах;

- дотримання форматів протоколів;

- запобігання входу систем у незахищені стани в разі аварійного завершення роботи пристрою захисту периметра;

- визначення типів подій, які система може реєструвати для підтримки функції аудиту;

- встановлення обмеження на визначену кількість послідовних неуспішних спроб входу користувача в систему (мережу) ОКІ впродовж визначеного часового періоду;

- автоматичне виконання блокування облікового запису/вузла, доки він не буде розблокований адміністратором;

- автоматичне надсилання особі та/або підрозділу, що відповідає за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту ОКІ повідомлення, коли користувачем перевищено максимальну кількість невдалих спроб входу в систему (мережу) ОКІ;

- реєстрація для отримання облікового запису для логічного доступу передбачає авторизацію привілейованого користувача;

- блокування на визначений час підозрілого облікового запису при спробі входу до нього.

Завдання 8. Впровадити багатофакторну автентифікацію. Для виконання зазначеного завдання можуть бути заплановані заходи:

- унікальна ідентифікація та автентифікація користувачів або процесів, що діють від імені користувачів;

- реалізація багатофакторної автентифікації для доступу до привілейованих облікових записів;

- реалізація багатофакторної автентифікації для віддаленого доступу до непривілейованих облікових записів такої, що один із факторів забезпечується пристроєм, окремим від системи, який отримує доступ.

Завдання 9. Впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності. Втілення цього завдання можливе шляхом планування проведення навчання з питань безпеки та приватності на основі ролей для співробітників, які обслуговують або захищають ОКІ:

- перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і щомісячно після цього;

- коли цього потребують системні зміни;

- оновленням навчального контенту на основі ролей щорічно;

включенням у рольове навчання інформації, отриманої з внутрішніх або зовнішніх інцидентів та порушень безпеки;

введенням до програми навчання практичних занять з безпеки та приватності, які мають підкріпити досягнення цілей навчання.

Завдання 10. Запровадити додаткове навчання з кібербезпеки для персоналу підрозділу кіберзахисту. Для виконання зазначеного завдання можуть бути заплановані заходи з додаткового навчання з кібербезпеки персоналу, який обслуговує або захищає ОКІ, принаймні раз на рік відповідно до їх обов'язків.

Завдання 11. Забезпечити шифрування при обміні інформацією про інформаційні активи між підрозділами ІТ та кіберзахисту. Для виконання зазначеного завдання можуть бути заплановані заходи:

забезпечення конфіденційності та цілісності визначеної інформації в стані спокою;

проведення щорічного виявлення використання будь-якого застарілого або слабкого шифрування;

реалізація механізмів криптографічного захисту для запобігання несанкціонованому розкриттю інформації під час передачі;

реалізація криптографічного механізму захисту зовнішніх повідомлень, якщо вони не захищені.

Завдання 12. Забезпечити захист інформації з обмеженим доступом (за наявності), створення (модернізація) комплексної системи захисту інформації. Для виконання зазначеного завдання можуть бути заплановані заходи:

навчання уповноважених осіб тому, щоб загальнодоступна інформація не містила інформацію з обмеженим доступом;

перегляд запропонованого змісту інформації до публікації в загальнодоступній системі, щоб гарантувати, що там не міститься інформація з обмеженим доступом;

забезпечення захисту від витоку інформації каналами побічних електромагнітних випромінювань та наведень випромінювання електромагнітних сигналів;

перевірка окремих осіб перед дозволом на доступ до інформаційної системи за необхідності.

Завдання 13. Забезпечити захищеність електронної пошти від спуфінгу, фішингу та перехоплення повідомлень. Для виконання зазначеного завдання можуть бути заплановані заходи:

підтримувати центральну вебсторінку ресурсу на головному загальнодоступному вебсайті ОКІ, яка слугує центральним джерелом інформації та яка використовує публічні адреси електронної пошти, щоб дати можливість громадськості надавати відгуки та/або направляти запитання щодо програми приватності;

розробити політику користування електронною поштою;

визначити та застосувати STARTTLS, інфраструктуру політики відправника, технологію DomainKeys Identified Mail, ідентифікацію повідомлень для всієї інфраструктури корпоративної електронної пошти;

під час передачі інформації між різними доменами безпеки варто змінювати інформацію, яка не підлягає оприлюдненню, реалізувавши апаратні засоби криптографічного захисту;

запобігати ексфільтрації інформації.

Завдання 14. Вимкнути встановлені за замовчуванням макроси та інший програмний код. Для виконання зазначеного завдання можуть бути заплановані заходи:

визначати прийнятні та неприйнятні мобільні коди та технології мобільних кодів;

встановити такі обмеження на використання програмного забезпечення з відкритим вихідним кодом: включити системну політику, яка за умовчанням вимикає макроси Microsoft Office.

Завдання 15. Описати конфігураційні файли критичних програмних та апаратних компонентів. Для виконання зазначеного завдання можуть бути заплановані заходи:

розробити, задокументувати та підтримувати за допомогою заходів конфігурації поточні базові налаштування системи;

переглядати та оновлювати базові налаштування системи щорічно або після кіберінциденту або при встановленні нових (оновленні) компонентів системи;

реалізувати конфігураційні установки.

Завдання 16. Забезпечити документування та актуалізацію схем (креслень) обладнання структурованої кабельної системи та кабельних каналів, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з'єднань. Для виконання зазначеного завдання можуть бути заплановані заходи:

побудувати й задокументувати карту топології мереж;

відстежувати та керувати змінами конфігураційних параметрів топології мереж відповідно до організаційної політики та процедур;

розробити та задокументувати процес інвентаризації компонентів мережі, який:

точно описує поточну мережу ОКІ;

охоплює всі компоненти в межах акредитації мережі;

не включає повторний облік компонентів або компонентів, будь-якої іншої мережі;

визначає рівень деталізації, який є необхідним для відстеження та звітування;

впровадити визначені односторонні інформаційні потоки за допомогою апаратних механізмів;

відокремлювати потоки інформації логічно або фізично, використовуючи визначені механізми та/або методи для досягнення необхідного поділу за типами інформації.

Завдання 17. Затвердити процедури інсталяції інформаційно-комунікаційних технологій. Затвердити політики встановлення засобів мережевого захисту, встановлення або видалення користувачами програмного

забезпечення. Для виконання зазначеного завдання можуть бути заплановані заходи:

- встановити визначені правила (політики), що регулюють встановлення обладнання або програмного забезпечення користувачами;

- застосовувати правила (політики) встановлення обладнання або програмного забезпечення за допомогою організаційних та автоматизованих методів;

- відстежувати відповідність правилам (політики) розгортанням обладнання або програмного забезпечення щорічно.

Завдання 18. Забезпечити регулярне створення та зберігання резервних копій інформаційних ресурсів. Для виконання зазначеного завдання можуть бути заплановані заходи:

- проводити резервне копіювання інформації користувачів, що містить системні компоненти;

  - проводити резервне копіювання інформації на системному рівні;

  - проводити резервне копіювання документації, включно з документацією, пов'язаною із забезпеченням безпеки та приватності;

  - забезпечити захист конфіденційності, цілісності та доступності резервних копій інформації в місцях їх зберігання;

  - зберігати резервні копії визначеного критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою в окремому сховищі або у вогнестійкому контейнері, які не пов'язані із системою;

  - розробити та узгодити план перевірок резервних копій;

  - оновлювати план перевірок резервних копій.

Завдання 19. Затвердити, регулярно тестувати та вносити зміни до планів реагування на кіберінциденти. Для виконання зазначеного завдання можуть бути заплановані заходи:

- розробити план реагування на кіберінциденти, який:

  - надає ОКІ дорожню карту для впровадження її можливостей реагування на кіберінциденти;

  - надає високорівневий підхід до того, як здатність реагування на кіберінциденти вписується в загальну практику;

  - відповідає унікальним вимогам ОКІ, які пов'язані із завданнями, розміром, структурою і функціями;

  - визначає підзвітні кіберінциденти;

  - надає показники для вимірювання можливостей реагування на кіберінциденти всередині ОКІ;

  - визначає ресурси та управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на кіберінциденти;

  - вирішує питання обміну інформацією про кіберінциденти;

  - оновлювати план реагування на інциденти в разі системних та організаційних змін або проблем, що виникають при реалізації, виконанні чи тестуванні плану;

  - впровадити можливості обробки кіберінцидентів безпеки та приватності,

включно з підготовкою, виявленням і аналізом, локалізацією, ліквідацією та відновленням;

координувати діяльність з обробки кіберінцидентів із заходами із забезпечення безперервності функціонування;

впроваджувати досвід, отриманий під час поточних дій з обробки кіберінцидентів, у процедури реагування на кіберінциденти, навчання й тестування та вносити відповідні зміни;

забезпечити, щоб строгість, інтенсивність, обсяг і результати діяльності з обробки кіберінцидентів можна було порівняти та передбачити на всьому ОКІ.

Завдання 20. Забезпечити збір журналів (логів) реєстрації подій. Для виконання зазначеного завдання можуть бути заплановані заходи:

переконатися, що записи результатів аналізу журналів подій містять інформацію, яка встановлює таке: який тип події стався; коли відбулася подія; де відбулася подія; джерело події; наслідки події; результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.

Завдання 21. Забезпечити безпечне зберігання журналів (логів) реєстрації подій. Для виконання зазначеного завдання можуть бути заплановані заходи:

побудувати та задокументувати структуру системи безпечного зберігання журналів подій;

організувати проходження результатів аналізу журналів подій, орієнтованих на доступ і кібербезпеку (наприклад, системи виявлення вторгнень/системи запобігання вторгненням, брандмауер, запобігання втраті даних, віртуальна приватна мережа);

визначити період зберігання (рекомендовано до трьох років) та порядок знищення записів результатів аналізу журналів подій, щоб забезпечити підтримку розслідувань (постфактум) кіберінцидентів та приватності.

Завдання 22. Забезпечити ідентифікацію обладнання та вжиття заходів, які унеможливають роботу обладнання в мережі без відповідної ідентифікації. Для виконання зазначеного завдання можуть бути заплановані заходи:

обмежити доступ до визначених типів цифрових та/або нецифрових носіїв інформації персоналом;

заборонити використання не зареєстрованих та не передбачених для застосування портативних пристроїв зберігання даних, якщо такі пристрої не мають визначеного власника.

Завдання 23. Забезпечити контрольоване використання Інтернет-послуг, виявлення аномальної взаємодії та створити необхідні обмеження. Для виконання зазначеного завдання можуть бути заплановані заходи:

встановити та задокументувати обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення кожного типу віддаленого доступу;

авторизувати віддалений доступ до Інтернет-служб, перш ніж будуть дозволені такі підключення;

підтримувати окремий домен виконання для кожного процесу, що виконується в системі.

Завдання 24. Забезпечити підключення ОП до мережі Інтернет через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, та тільки у випадку неможливості функціонування без підключення до Інтернету). Для виконання зазначеного завдання можуть бути заплановані заходи:

- розробити та затвердити політику управління інформаційним потоком, яка забезпечує додатковий захист для запобігання та виявлення спроб використання для роботи інформаційних активів в мережі Інтернет;

- застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі політики управління інформаційним потоком;

- запровадити криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу;

- затвердити та забезпечити дотримання політики використання безпроводового доступу до системи, перш ніж будуть дозволені такі підключення.

Таблиця 9 у пункті 5 Плану захисту заповнюється шляхом описання виконання такого завдання із кіберзахисту:

Завдання. Визначити порядок проведення моніторингу загроз та застосування відповідних тактик, технік і процедур. Для виконання зазначеного завдання можуть бути заплановані заходи:

- розробити стратегію безперервного моніторингу безпеки та приватності й упровадити програму безперервного моніторингу безпеки та приватності, яка охоплює: встановлення показників безпеки та приватності, які необхідно відстежувати, перелік загроз і технік, тактик й процедур кіберзловмисників; встановлення постійного моніторингу та щорічного оцінювання ефективності заходів захисту; поточні оцінювання заходів захисту відповідно до стратегії безперервного моніторингу ОКІ; постійний моніторинг стану безпеки та приватності відповідно до встановлених метрик і відповідно до стратегії безперервного моніторингу ОКІ; зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу безпеки та приватності; дії реагування за результатами аналізу інформації, пов'язаної з безпекою та приватністю;

- проводити оцінювання ризику, включно з вірогідністю й величиною шкоди.

Таблиця 10 у пункті 5 Плану захисту заповнюється шляхом описання виконання таких завдань із кіберзахисту:

Завдання 1. Забезпечити інформування про кіберінциденти. Для виконання зазначеного завдання можуть бути заплановані заходи:

- вимагати від персоналу повідомляти про підозрілі кіберінциденти з безпеки та приватності відповідно до організаційної спроможності реагування на кіберінциденти впродовж визначеного періоду часу;

- повідомляти про вразливості системи, пов'язані із зареєстрованими кіберінцидентами безпеки та приватності визначеному персоналу;

встановити політику, порядок та процедури надання доповідей про всі підтверджені кіберінциденти.

повідомляти про кіберінциденти за допомогою автоматизованих механізмів (електронну пошту, публікацію на вебсайтах тощо);

надати інформацію про кіберінциденти безпеки та приватності постачальнику послуги;

передавати (публікувати) інформацію за межами встановленої межі системи за визначеними відповідними нормативними вказівками.

Завдання 2. Забезпечити використання результатів досліджень щодо вразливостей. Для виконання зазначеного завдання можуть бути заплановані заходи:

використовувати інструменти та методи сканування вразливості, які полегшують сумісність між інструментами та автоматизують частини процесу управління вразливостями, використовуючи стандарти для: обліку платформ, недоліків програмного забезпечення та неправильних конфігурацій; форматування контрольних списків і процедур тестування; вимірювання впливу вразливості;

аналізувати звіти про сканування вразливості та результати контрольних оцінювань;

заборонити привілейований доступ до системи користувачам, які не належать до ОКІ.

Завдання 3. Забезпечити розміщення файлів security.txt (стандарт безпеки вебсайтів, в рамках програми Bug Bounty) та опрацювання отриманої завдяки їм інформації. Для виконання зазначеного завдання можуть бути заплановані заходи:

отримувати системні попередження безпеки, рекомендації та директиви, що прописуються в файлі security.txt;

створити та інституціоналізувати контакти між обраними групами та асоціаціями зі спільнотами безпеки та приватності для підтримки ознайомленості з рекомендованими практиками безпеки інформації та приватності, техніками та технологіями.

Таблиця 11 у пункті 5 Плану захисту заповнюється шляхом описання виконання такого завдання із кіберзахисту:

Завдання 1. Затвердити плани відновлення після інцидентів. Для виконання зазначеного завдання можуть бути заплановані заходи:

забезпечити відновлення та відтворення системи до відомого стану після збою, компрометації або помилок невідкладно;

забезпечити захист компонентів системи, які використовуються для резервного копіювання та відновлення;

розробити план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації, який: визначає основні завдання, функції та пов'язані з ними вимоги щодо безперервної роботи; забезпечує цілі, пріоритети та відповідні показники відновлення функціонування; визначає ролі, обов'язки та відповідальних осіб з контактною інформацією; спрямований на підтримку основних завдань і функцій попри

системні збої, компрометації або помилки; спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації та персональних даних; вирішує питання обміну інформацією про надзвичайні ситуації;

протестувати план забезпечення безперервної роботи та відновлення функціонування системи щорічно, використовуючи тести, з метою визначення ефективності плану та організаційної готовності виконати план;

переглядати результати тестування плану;  
за необхідності ініціювати коригувальні дії.

7. Пунктом 6 Плану захисту передбачено включення відомостей про моніторинг рівня безпеки об'єкта критичної інфраструктури щодо нейтралізації загрози національного рівня «кібератака/кіберінцидент», де описуються зведені відомості щодо результатів моніторингу рівня безпеки з урахуванням вимог статті 17 Закону України «Про критичну інфраструктуру».

8. Таблиця 12 Плану захисту заповнюється (відповідальною особою за стан захисту інформації та кіберзахисту ОКІ) відомостями про внесення змін до Плану захисту, які не потребують погодження функціональними органами.

9. Після Таблиці 12 вказується відповідальна особа за заповнення Плану захисту (посада, прізвище та ініціали), підпис та дата підписання.

10. Оператори несуть відповідальність за достовірність відомостей, внесених до Плану захисту, відповідно до законодавства.

Т.в.о. начальника контррозвідального інтересів держави інформаційної безпеки України	Департаменту захисту у сфері Служби безпеки	Директор кіберзахисту Державної зв'язку та України	Департаменту Адміністрації спеціального захисту інформації
--	---	---	---

Володимир КАРАСТЕЛЬОВ

Ігор МАЛЬЧЕНЮК