ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 2025 року № ___

Методичні рекомендації щодо здійснення базових заходів з кіберзахисту

I. Загальні положення

1. Ці Методичні рекомендації розроблені відповідно до пункту 6 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, підпунктів 6, 95^4 пункту 4 та пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, з метою управління та зменшення ризиків кібербезпеки.

2. Методичні рекомендації щодо здійснення базових заходів з кіберзахисту (далі – Методичні рекомендації) розроблено з урахуванням документа NIST Cybersecurity Framework (CSF) 2, виданого у 2024 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology).

3. Ці Методичні рекомендації можуть використовуватися суб’єктами забезпечення кібербезпеки на об’єктах кіберзахисту будь-яких масштабів і секторів, включаючи промисловість, державний сектор, критичну інфраструктуру, наукові установи та неприбуткові підприємства, незалежно від рівня зрілості та спроможностей з кібербезпеки, у тому числі на об’єктах критичної інформаційної інфраструктури, в інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація, вимога щодо захисту якої встановлена законом.

4. Терміни вживаються у значеннях, наведених у Законах України «Про основні засади кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації», «Про стандартизацію» та Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Порядку формування переліку об’єктів критичної інформаційної інфраструктури, затвердженому постановою Кабінету Міністрів України від 09 жовтня 2020 року № 943, Загальних вимогах до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою

Кабінету Міністрів України від 19 червня 2019 року № 518, Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373.

5. Кожний захід кіберзахисту містить нормативні посилання та приклади їх виконання, які наведено в додатку 1 до цих Методичних рекомендацій. Нормативні посилання забезпечують можливість застосування положень стандартів, нормативних документів системи технічного захисту інформації, рекомендацій міжнародних організацій та спеціальних публікацій Національного інституту стандартів та технологій (NIST) США залежно від встановленого законодавством або обраного власником/розпорядником об’єкта кіберзахисту набору правил захисту інформації та/або кіберзахисту.

6. Власники або розпорядники об’єктів кіберзахисту, комплексні системи захисту інформації яких створені з використанням Базового профіля безпеки інформації, визначеного наказом Адміністрації Держспецзв'язку від 24 червня 2024 року № 317, а відповідність яких задекларована постановою Кабінету Міністрів України від 30 травня 2024 року № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації», можуть у разі потреби доповнювати цільовий профіль безпеки інформації, який ними розробляється, заходами безпеки, які наведені в цих Методичних рекомендаціях.

7. Якщо цільовий профіль безпеки інформації доповнюється відповідно до цих Методичних рекомендацій, власник/розпорядник об’єкта кіберзахисту може, пересвідчившись, обґрунтовано вважати, що проведення кожного базового заходу кіберзахисту підтверджується виконанням заходу безпеки цільового профілю безпеки інформації. Зіставлення заходів безпеки, визначених НД ТЗІ 3.6-006-24, застосованих у Базовому профілі безпеки інформації, затвердженому наказом Адміністрації Держспецзв'язку від 24 червня 2024 року № 317, та застосованих в Методичних рекомендаціях, наведено в додатку 2.

8. Ці Методичні рекомендації можуть застосовуватися для розроблення секторальних профілів кіберзахисту для секторів критичної інфраструктури та у разі потреби для профілів кіберзахисту для об’єднань підприємств, установ і організацій. При розробці таких профілів варто використовувати розділ IV Методичних рекомендацій або інші публікації, які видає Держспецзв’язку, або відповідні міжнародні організації, або окремі державні органи провідних країн світу, уповноважені видавати рекомендації у сфері кіберзахисту та кібербезпеки, які враховують відповідну специфіку об’єктів кіберзахисту або технологій, які в них застосовані.

9. Для визначення ступеня впровадження базових заходів кіберзахисту, а також профілів, зазначених у пункті 9 розділу I Методичних рекомендацій, доцільно здійснювати оцінювання поточного стану та складання поточного профілю кіберзахисту. Заходи, що рекомендується виконати для складання профілю кіберзахисту, наведено в розділі IV «Профіль кіберзахисту» цих Методичних рекомендацій.

10. Оцінювання стану кіберзахисту можна здійснювати суб'єктам забезпечення кібербезпеки шляхом самооцінки із залученням штатного навченого персоналу з підтвердженою кваліфікацією, або із залученням організацій, з якими укладені відповідні договори з урахуванням вимог щодо забезпечення конфіденційності інформації, яка отримана під час та за результатами проведення оцінювання, або аудиторів інформаційної безпеки, які відповідають Вимогам до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації), затвердженим наказом Адміністрації Держспецзв'язку від 30 квітня 2024 року № 228, зареєстрованим в Міністерстві юстиції України 11 червня 2024 року за № 880/42225, або відповідно до наказу Адміністрації Держспецзв'язку від 02 грудня 2014 року № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», зареєстрованого в Міністерстві юстиції України 28 січня 2015 року за № 90/26535.

11. Результати оцінювання стану кіберзахисту використовуються:

під час проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, порядок проведення якого затверджено постановою Кабінету Міністрів України від 11 листопада 2020 року № 1176;

під час проведення моніторингу рівня безпеки об'єктів критичної інфраструктури відповідно до Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 22 липня 2022 року № 821 (в частині кіберзахисту);

при щорічному поданні Адміністрацією Держспецзв'язку до Кабінету Міністрів України аналітичних матеріалів щодо стану захисту державних електронних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, відповідно до Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затвердженого постановою Кабінету Міністрів України від 03 серпня 2005 року № 688;

під час проведення заходів державного контролю за станом криптографічного та технічного захисту інформації.

12. Поточний профіль кіберзахисту можна використовувати для створення плану захисту об'єкта критичної інфраструктури. Для цього слід застосовувати форму плану захисту, розроблену для проєктної загрози національного рівня «кібератака/кіберінцидент», а також рекомендації з розроблення плану захисту, затверджені спільним наказом Служби безпеки України та Адміністрації Держспецзв'язку від 19 грудня 2024 року № 627/772. При цьому заходи з розділу 5 (таблиця 7) зазначеної форми можуть бути доповнені іншими заходами, наведеними у цих Методичних рекомендаціях.

13. План реагування на кіберінциденти та кібератаки слід розробляти з урахуванням вимог постанови Кабінету Міністрів України від 04 квітня 2023 року № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», а також наказу Адміністрації Держспецзв'язку від 03 липня 2023 року № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі». У разі використання комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем слід також враховувати положення постанови Кабінету Міністрів України від 23 грудня 2020 року № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».

14. План (плани) реагування на кіберінциденти та кібератаки та відновлення після них доцільно складати з урахуванням таксономії кіберінцидентів та можливої зміни рівня критичності кіберінцидентів, затверджувати розпорядчим актом власника/розпорядника об'єкта кіберзахисту, проводити регулярні тренування з його виконання із залученням персоналу організації та заінтересованих сторін, проводити його (них) регулярний перегляд та вносити за потреби відповідні обґрунтовані зміни.

II. Мета застосування та складові Методичних рекомендацій

1. Ці Методичні рекомендації описують базові заходи з кіберзахисту, як перелік впорядкованих та взаємопов'язаних заходів з кіберзахисту.

2. Базові заходи з кіберзахисту включають шість функцій – управління, ідентифікація, забезпечення захисту, виявлення, реагування та відновлення, які діляться на категорії та підкатегорії.

3. Впровадження базових заходів дозволить підвищити рівень забезпечення кібербезпеки спрямованого на зниження ризиків кібербезпеки, має інтеграційний характер та формує цикл управління кібербезпекою.

Такий перелік заходів не є контрольним переліком дій, які необхідно виконати для забезпечення кібербезпеки, вони є базовими для впровадження на об'єкті кіберзахисту з метою управління ризиками.

4. Функція «Управління» (GV) знаходиться в центрі циклу та забезпечує контроль суб’єктом забезпеченню кібербезпеки за функціонуванням всього циклу управління ризиками.

Функція «Управління» передбачає отримання результатів, які допоможуть суб’єктам забезпечення кібербезпеки визначити пріоритетність заходам інших п'яти класів в рамках впровадження системи управління ризиками на об’єкті кіберзахисту та виправдати очікування заінтересованих сторін.

Впровадження заходів функції «Управління» має вирішальне значення, оскільки передбачає включення питання забезпечення кібербезпеки в стратегію управління ризиками організації, яка охоплює положення організаційного контексту, управління ризиками кібербезпеки ланцюга постачання, ролі, обов'язки та повноваження співробітників організації, політику та контроль за виконанням стратегії кібербезпеки.

5. Впровадження функції «Ідентифікація» (ID) дозволяє суб’єкту забезпечення кібербезпеки пріоритизувати свої ресурси та можливості відповідно до стратегії управління ризиками та потреб об’єкта кіберзахисту, визначених в «Управлінні». «Ідентифікація» також включає заходи з вдосконалення політик, планів, процесів, процедур і практик об’єкта кіберзахисту, які підтримують управління ризиками кібербезпеки, з метою інформування про впроваджені заходи кіберзахисту за функціями «Управлінням», «Ідентифікацією», «Забезпеченням захисту», «Виявленням», «Реагуванням», «Відновленням».

6. Заходи функції «Забезпечення захисту» (PR) після того, як активи і ризики визначені та пріоритизовані в функції «Ідентифікації», спрямовані на підтримку здатності суб’єкта забезпечення кібербезпеки захистити ці активи, щоб запобігти або зменшити ймовірність впливу несприятливих подій у сфері кібербезпеки, а також підвищити можливості використання переваги новітніх розробок та здобутків у сфері кібербезпеки та кіберзахисту.

Впровадження заходів функції «Забезпечення захисту» включає управління ідентифікацією, автентифікацією та контролем доступу, забезпечення обізнаності та навчання співробітників, безпеку даних, безпеку фізичних та віртуальних (тобто, захист апаратного, програмного забезпечення, фізичної площини, віртуальної площини) та стійкість технологічної інфраструктури.

7. Функція «Виявлення» (DE) дозволяє своєчасно виявляти та аналізувати аномалії, індикатори компрометації та інші потенційно несприятливі події, які вказують на те, що відбуваються атаки та інциденти кібербезпеки. Ця функція підтримує успішне реагування на інциденти та заходи з відновлення.

8. Функція «Реагування» (RS) підтримує здатність стримувати наслідки інцидентів кібербезпеки, управляти ними, аналізувати та пом'якшувати наслідки, звітувати про виконанні дії та здійснювати ефективну комунікацію.

9. Функція «Відновлення» (RC) передбачає відновлення суб’єктом забезпечення кібербезпеки активів та операцій, що постраждали від інциденту кібербезпеки, спрямований на підтримку своєчасного відновлення нормальної роботи, щоб зменшити наслідки інцидентів кібербезпеки та забезпечити належну комунікацію під час відновлювальних робіт.

10. У випадку наявності КСЗІ з підтвердженою відповідністю або КСЗІ, підтвердження відповідності якої здійснюється шляхом декларації про побудову цільового профіля безпеки інформації для систем, які є об'єктами кіберзахисту, суб’єкт забезпечення кібербезпеки має доповнити КСЗІ заходами, передбаченими цими Методичними рекомендаціями.

III. Модель базових заходів з кіберзахисту

1. Модель базових заходів з кіберзахисту передбачає взаємозв’язки та взаємозалежність шести функцій одна від одної (рисунок 1). Наприклад, суб’єкт забезпечення кіберзахисту класифікує активи в рамках функції «Ідентифікації» та вживає заходів для захисту цих активів в рамках функції «Забезпечення захисту». Інвестиції в планування і тестування функцій «Управління» та «Ідентифікації» сприятимуть своєчасному виявленню неочікуваних подій у функції «Виявлення», а також забезпеченню реагування на інциденти та відновлення після інцидентів кібербезпеки у функціях «Реагування» та «Відновлення». Функція «Управління» знаходиться в центрі циклу, оскільки вона аналізує та описує те, як суб’єкт забезпечення кіберзахисту буде впроваджувати заходи інших п'яти класів.

Рисунок 1. Модель заходів з кіберзахисту

2. Базові заходи з кіберзахисту спрямовані на запобігання кіберінцидентам та забезпечують готовність суб’єкта забезпечення кібербезпеки до реагування на них та протидії їм.

3. Всі заходи шести функцій виконуються одночасно. Заходи функцій «Управління», «Ідентифікація», «Забезпечення захисту» і «Виявлення» повинні виконуватися безперервно, а заходи функцій «Реагування» і «Відновлення» повинні бути готовими в будь-який час виконуватися в разі виникнення інцидентів кібербезпеки. Усі базові заходи кіберзахисту відіграють важливу роль у реагуванні на інциденти кібербезпеки. Заходи функцій «Управління», «Ідентифікація», «Забезпечення захисту» сприяють запобігання інцидентам і готовність суб'єкта забезпечення кібербезпеки до них, тоді як заходи функцій «Управління», «Виявлення», «Реагування» та «Відновлення» допомагають суб'єкту забезпечення кібербезпеки виявляти та керувати інцидентами кібербезпеки на об'єкті кіберзахисту.

4. Назва кожного із шести функцій з кіберзахисту та категорій описує їх зміст. Кожна функція поділяється на категорії, які пов'язані із заходами кіберзахисту, які вони включають, кожна категорія поділяється на підкатегорію, які в свою чергу поділяються на більш конкретні заходи технічного та управлінського характеру. Підкатегорії містять приклади заходів, які не є вичерпними, але вони описують детальні результати, які підтримують досягнення кожного базового заходу кіберзахисту в кожній підкатегорії та категорії.

5. Шість функцій, їх категорії та підкатегорії застосовуються до всіх інформаційно-комунікаційних технологій, що використовуються на об'єкті кіберзахисту, включаючи інформаційні технології, Інтернет речей та операційні технології. Вони також застосовуються до всіх типів технологічних середовищ, включаючи хмарні, мобільні та системи штучного інтелекту.

6. У додатку 1 наведено розгорнуту характеристику базових заходів з кіберзахисту, надано нормативні посилання та приклади впровадження таких заходів.

Нормативні посилання відображають взаємозв'язки між підкатегоріями та різними стандартами, рекомендаціями, нормативно-правовими актами та іншими документами. Інформативні посилання допомагають визначити, як суб'єкт забезпечення кібербезпеки може досягти бажаних результатів кожного базового заходу з кіберзахисту. Інформативні посилання можуть бути специфічними для, наприклад, сектору критичної інфраструктури, об'єднань підприємств або для конкретної технології. Суб'єкт забезпечення кібербезпеки може визначити найбільш відповідні інформативні посилання при створенні профілю кібербезпеки.

Приклади впровадження надають уявні приклади лаконічних, дієвих кроків для досягнення результатів підкатегорій. Дієслова, які використовуються в прикладах: поділитися, задокументувати, розробити, виконати, контролювати, аналізувати, оцінювати, забезпечити, пересвідчитися тощо. Приклади не є вичерпним списком всіх можливих дій, які треба виконати суб'єкту забезпечення кібербезпеки для досягнення бажаного результату, і вони не являють собою

базовий набір обов'язкових дій для вирішення питання забезпечення кіберзахисту на об'єкті.

7. Суб'єкт забезпечення кібербезпеки при впровадженні базових заходів з кіберзахисту має враховувати свою місію та ризики об'єкта кіберзахисту.

З розумінням очікувань заінтересованих сторін та допустимого рівня ризику (як описано в функції «Управління») суб'єкт забезпечення кібербезпеки може пріоритизувати базові заходи з кіберзахисту для прийняття обґрунтованих рішень щодо витрат та дій.

Доцільним є впровадження в діяльність суб'єкта забезпечення кібербезпеки та ведення реєстру ризиків кібербезпеки (кіберризиків) критичної інформаційної інфраструктури об'єкта кіберзахисту або їх об'єднань.

Суб'єкт забезпечення кібербезпеки обирає спосіб обробки ризику: зменшення, передача, уникнення або прийняття негативних ризиків та реалізацію, спільне використання, підвищення або прийняття позитивних ризиків (залежно від потенційних наслідків та ймовірності). Суб'єкт забезпечення кібербезпеки може використовувати базові заходи з кіберзахисту як внутрішній інструмент для управління своєю кібербезпекою, так і зовнішній – для контролю або комунікації з третіми сторонами.

Приклад опису рекомендованих базових кроків для створення переліку кіберризиків (додаток 3) доцільно враховувати під час їх ідентифікації з урахуванням допустимого рівня ризику, оцінки ймовірності та впливу на функціонування об'єкта кіберзахисту, оцінки залишеного ризику та відповідних ризику заходів з управління кіберризиками.

8. Базові заходи з кіберзахисту передбачають покращення комунікації на об'єкті кіберзахисту щодо очікувань, планування та ресурсів у сфері кібербезпеки. Вони сприяють двосторонньому обміну інформацією між керівниками, які зосереджуються на пріоритетах та стратегічних напрямах функціонування об'єкта кіберзахисту, і менеджерами, які управляють конкретними кіберризиками, що можуть вплинути на досягнення цих пріоритетів. Також сприяють обміну між менеджерами та фахівцями, які впроваджують та експлуатують технології.

IV. Профіль кіберзахисту

1. Суб'єкт забезпечення кібербезпеки з метою оцінки стану захищеності власного об'єкта кіберзахисту та виявлення вразливостей на основі базових заходів з кіберзахисту розробляє профіль кіберзахисту.

2. Профіль кіберзахисту розробляється на основі базових заходів кіберзахисту та описує поточний та/або цільовий стан впроваджених суб'єктом забезпечення кібербезпеки заходів, які описуються у функціях «Управлінні», «Ідентифікації», «Забезпеченні захисту», «Виявленні», «Реагуванні» та «Відновленні» на об'єкті (об'єктах) кіберзахисту.

3. Профіль кіберзахисту використовується для розуміння суб’єктом забезпечення кібербезпеки кількості заходів кіберзахисту, які необхідно впровадити або адаптувати раніше впроваджені заходи на об’єкті кіберзахисту до шести класів системи кіберзахисту.

4. Профіль кіберзахисту – додатковий інструмент, який допоможе суб’єкту забезпечення кібербезпеки оцінити достатність ресурсів, визначити пріоритетні заходи, забезпечити поінформованість про результати з метою обізнаності всіх співробітників, враховуючи при цьому місії функціонування об’єкта кіберзахисту, очікування заінтересованих сторін, актуальні виклики та загрози, а також законодавчі вимоги у сфері інформаційної та кібербезпеки. Після цього суб’єкт забезпечення кіберзахисту має визначити пріоритетність своїх дій для досягнення конкретних результатів і донести цю інформацію до відома заінтересованих сторін.

5. Профіль кіберзахисту включає один або обидва з перелічених нижче пунктів:

1) поточний профіль відображає поточний стан кіберзахисту та визначає основні заходи, які суб’єкт забезпечення кібербезпеки наразі впровадив на об’єкті кіберзахисту (або впроваджує, є наявні для цього ресурси), який результат він має, а також характеризує, як і якою мірою виконується кожен етап впровадження заходу. Дані поточного профілю використовуються для оцінки поточного стану кіберзахисту об’єкта кіберзахисту;

2) цільовий профіль визначає бажані результати, які суб’єкт забезпечення кібербезпеки хоче отримати у майбутньому та визначив як пріоритетні, для досягнення своїх цілей з управління ризиками кібербезпеки. Цільовий профіль враховує очікувані зміни в системі кібербезпеки на об’єкті кіберзахисту, такі як нові вимоги, впровадження нових технологій, тенденції розвитку загроз.

6. Створення та використання профілю кіберзахисту складається з таких етапів:

Етап 1. Визначення сфери застосування профілю кіберзахисту.

Для визначення сфери застосування профілю кіберзахисту необхідно окреслити цілі та завдання, наявні та необхідні ресурси, кінцеву мету впровадження базових заходів з кіберзахисту. Суб’єкт забезпечення кібербезпеки на об’єкті кіберзахисту може створювати декілька базових профілів, кожен з яких має різну сферу застосування. Наприклад, один профіль може стосуватися всього об’єкта кіберзахисту або обмежуватися системами, які обробляють інформацію щодо фінансів, чи протидією загрозам програм-вимагачів і реагуванням на інциденти, пов'язані із цими системами.

Етап 2. Збір актуальної інформації, яка необхідна для підготовки профілю кіберзахисту. До такої інформації належать існуючі політики, які описують структуру об’єкта кіберзахисту, його пріоритетні цілі, наявні ресурси для управління ризиками, профілі ризиків, дані в рамках аналізу впливу на функціонування об’єкта кіберзахисту, вимоги та стандарти кібербезпеки, яких

дотримується суб’єкт забезпечення кібербезпеки, практики та інструменти (наприклад, процедури та запобіжні заходи), а також робочі ролі.

Етап 3. Створення профілю на об’єкті кіберзахисту. Суб’єкт забезпечення кібербезпеки має визначити, яку інформацію слід внести до профілю для впровадження необхідних базових заходів з кіберзахисту, задокументувати необхідну інформацію, розглянути наслідки ризиків Поточного профілю для планування та визначення пріоритетів Цільового профілю.

Етап 4. Аналіз розбіжностей між поточним та цільовим профілями та розроблення плану дій. Цей етап передбачає проведення аналізу прогалин, щоб виявити та проаналізувати відмінності між поточним та цільовим профілями, а також розробити пріоритетний план дій (наприклад, реєстр ризиків, детальний звіт про ризики, план дій та етапи (POA&M) для усунення цих прогалин).

Етап 5. Впровадження плану дій та оновлення профілю кіберзахисту об’єкта кіберзахисту. Суб’єкт забезпечення кібербезпеки має дотримуватися плану дій, щоб усунути прогалини та наблизити об’єкт кіберзахисту до Цільового профілю. План дій може мати загальний дедлайн або бути безперервним.

7. З огляду на важливість постійного вдосконалення суб’єкт забезпечення кібербезпеки може повторювати ці кроки стільки разів, скільки потрібно.

Розроблені профілі кіберзахисту можна використовувати, як додатковий інструмент в діяльності об’єкта кіберзахисту. Наприклад, поточний профіль може бути використаний для документування та комунікації можливостей об’єкта кіберзахисту у сфері кібербезпеки та відомих можливостей для вдосконалення із зовнішніми заінтересованими сторонами, такими як партнери організації або потенційні клієнти. Цільовий профіль може допомогти сформувати вимоги та очікування суб’єкта забезпечення кібербезпеки щодо управління кіберризиками для постачальників, партнерів та інших третіх сторін як ціль для досягнення цими сторонами.

V. Рівні впровадження базових заходів з кіберзахисту

Суб’єкт забезпечення кібербезпеки для формування поточного та цільового профілю може використовувати рівні їх впровадження (зрілості). Рівні характеризують контроль та суворе дотримання практик управління ризиками кібербезпеки на об’єкті кіберзахисту, а також надають контекст того, як суб’єктом забезпечення кібербезпеки розглядаються ризики кібербезпеки та процеси, що застосовуються для управління цими ризиками.

1. Рівні відображають практики суб’єкта забезпечення кібербезпеки з управління ризиками кібербезпеки як часткові (Рівень 1), ризико-орієнтовані (Рівень 2), повторювані (Рівень 3) та адаптивні (Рівень 4). Рівні описують перехід від неформальних, ситуативних заходів реагування до підходів, які є гнучкими, заснованими на оцінці ризиків та постійно вдосконалюються. Вибір рівнів допомагає задати загальний тон тому, як суб’єкт забезпечення кібербезпеки керуватиме ризиками кібербезпеки.

2. Рівні доповнюють методологію управління ризиками кібербезпеки на об’єкті кіберзахисту, а не замінюють її. Наприклад, суб’єкт забезпечення кібербезпеки може використовувати рівні для внутрішнього спілкування як орієнтир для всього об’єкта кіберзахисту.

3. Перехід до вищих рівнів заохочується, коли ризики або повноваження є більшими або коли аналіз витрат і вигоди вказує на можливе та економічно ефективне зниження негативних ризиків кібербезпеки.

4. Рівні характеризують суворість практик організації з управління ризиками кібербезпеки («Управління») і практик управління ризиками кібербезпеки («Ідентифікація», «Забезпечення захисту», «Виявлення», «Реагування» та «Відновлення»).

5. Рівень 1: частковий. Застосування організаційної стратегії ризиків кібербезпеки управляється в індивідуальному порядку. Пріоритизація є випадковою і формально не базується на цілях чи середовищі загроз.

Обізнаність про ризики кібербезпеки на організаційному рівні обмежена.

Суб’єкт забезпечення кібербезпеки впроваджує управління ризиками кібербезпеки на нерегулярній основі, від випадку до випадку. Суб’єкт забезпечення кібербезпеки може не мати процесів, які дозволяють обмінюватися інформацією про кібербезпеку всередині об’єкта кіберзахисту. Суб’єкт забезпечення кібербезпеки, як правило, не знає про ризики кібербезпеки, пов’язані з його постачальниками та продуктами та послугами, які він придбав та використовує.

6. Рівень 2: поінформований про ризик.

Методи управління ризиками затверджуються керівництвом та можуть (не можуть) бути встановлені як загальна організаційна політика.

Пріоритизація діяльності з кібербезпеки та потреб у захисті безпосередньо залежить від цілей організаційних ризиків, середовища загроз або вимог організації, її місії.

Існує усвідомлення ризиків кібербезпеки на організаційному рівні, але загально-організаційного підходу до управління ризиками кібербезпеки не встановлено.

Врахування кібербезпеки в організаційних цілях і програмах може мати місце на деяких, але не на всіх рівнях об’єкта кіберзахисту. Оцінка ризиків кібербезпеки організаційних та зовнішніх активів об’єкта кіберзахисту здійснюється, але зазвичай не є повторюваною або періодичною.

Обмін інформацією про кібербезпеку на об’єкті кіберзахисту відбувається на неофіційній основі. Суб’єкт забезпечення кібербезпеки усвідомлює ризики кібербезпеки, пов’язані з її постачальниками та продуктами та послугами, які він придбав та використовує, але не діє послідовно чи формально у відповідь на ці ризики.

7. Рівень 3: повторюваний.

Практика управління ризиками об’єкта кіберзахисту офіційно затверджена та виражена як політика. Політики, процеси та процедури з урахуванням ризиків визначаються, впроваджуються за призначенням і переглядаються. Організаційні практики кібербезпеки регулярно оновлюються на основі застосування процесів управління ризиками до змін у вимогах організації, її місії, загрозах і технологічному ландшафті.

Існує загально-організаційний підхід до управління ризиками кібербезпеки. Інформація про кібербезпеку регулярно передається по всьому об’єкту кіберзахисту. Існують узгоджені методи для ефективного реагування на зміни ризику. Персонал володіє знаннями та навичками для виконання своїх призначених ролей і обов'язків.

Суб’єкт забезпечення кібербезпеки постійно та точно відстежує ризики кібербезпеки активів. Керівники вищої ланки з кібербезпеки та поза кібербезпекою регулярно спілкуються щодо ризиків кібербезпеки. Керівниками забезпечується врахування кібербезпеки на всіх напрямах діяльності на об’єкті кіберзахисту.

Стратегія ризиків об’єкта кіберзахисту ґрунтується на ризиках кібербезпеки, пов’язаних з його постачальниками, продуктами та послугами, які він придбав та використовує. Співробітники офіційно реагують на ці ризики за допомогою таких механізмів, як письмові договори, що визначають базові вимоги, структури управління (наприклад, відділ з управління ризиками), а також впровадження та моніторинг політики. Ці дії впроваджуються послідовно та за призначенням, а також постійно контролюються та переглядаються.

8. Рівень 4: адаптивний.

Існує загально-організаційний підхід до управління ризиками кібербезпеки, який використовує політику, процеси та процедури з урахуванням ризиків для вирішення потенційних подій кібербезпеки. Взаємозв’язок між ризиками кібербезпеки та цілями об’єкта кіберзахисту чітко розуміється та враховується під час прийняття рішень. Керівники контролюють ризики кібербезпеки в тому ж контексті, що й фінансові та інші організаційні ризики.

Бюджет об’єкта кіберзахисту формується з урахуванням аналізу поточного та прогнозованого середовища ризику, а також рівня прийнятної толерантності до ризику.

Функціональні підрозділи впроваджують виконавче бачення та аналізують ризики на системному рівні в контексті допустимих організаційних ризиків.

Управління ризиками кібербезпеки є частиною організаційної культури суб’єкта забезпечення кібербезпеки. Цей процес ґрунтується на аналізі попереднього досвіду діяльності та забезпеченні постійного моніторингу операцій у системах та мережах об’єкта кіберзахисту. Суб’єкт забезпечення кібербезпеки оперативно та ефективно адаптується до змін у цілях діяльності організації або завданнях, пов’язаних з основною місією. Це дозволяє своєчасно коригувати підходи до управління ризиками та інформувати про них відповідно до актуальних потреб організації та зовнішнього середовища.

Суб’єкт забезпечення кібербезпеки адаптує свої практики кібербезпеки на основі попередньої та поточної діяльності з кібербезпеки, включаючи отримані уроки та прогнозні показники.

Завдяки процесу безперервного вдосконалення, який включає передові технології та практики кібербезпеки, суб’єкт забезпечення кібербезпеки активно адаптується до мінливого технологічного ландшафту та своєчасно й ефективно реагує на складні загрози, що розвиваються.

Суб’єкт забезпечення кібербезпеки застосовує інформацію в реальному часі або максимально наближену до нього для оцінки ризиків кібербезпеки, пов’язаних із постачальниками, продуктами та послугами, які закуповуються та використовуються. Це дозволяє своєчасно і послідовно реагувати на виявлені загрози та мінімізувати потенційні ризики.

Інформація щодо кібербезпеки постійно розповсюджується в межах об’єкта кіберзахисту та передається уповноваженим третім сторонам у встановленому порядку.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку
лейтенант Ігор МАЛЬЧЕНЮК