ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 20___ року № ___

Методичні рекомендації
щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування

I. Загальні положення

1. Методичні рекомендації щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування (далі – Рекомендації) розроблено на виконання частини третьої статті 5^1 Закону України «Про основні засади забезпечення кібербезпеки України» з урахуванням:

NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations;

NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide;

NIST SP 800-181 Rev.1: Workforce Framework for Cybersecurity (NICE Framework);

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги;

ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки.

2. Рекомендації можуть застосовуватися органами державної влади, операторами критичної інфраструктури, юридичними особами, що є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності, та органами місцевого самоврядування (далі – установи), що є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, у яких обробляються

державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури (далі – система).

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

4. У цих Рекомендаціях термін «керівник з кіберзахисту» вживається у такому значенні – це особа, яка здійснює керівництво, координацію та контроль з питань кіберзахисту відповідної установи, що є власником або розпорядником систем.

Інші терміни вживаються у значенні, наведеному в Законах України «Про основні засади забезпечення кібербезпеки України», «Про Державну службу спеціального зв’язку та захисту інформації України», «Про захист інформації в інформаційно-комунікаційних системах», «Про критичну інфраструктуру», Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 року № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» (далі – Національний план), Порядку призначення керівника з кіберзахисту на посаду в органі державної влади, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 року № 1516 (далі – Порядок).

ІІ. Підрозділи з кіберзахисту

1. Основні завдання та функції підрозділів з кіберзахисту, відповідальність, обов’язки та права його керівника визначаються положенням про підрозділ з кіберзахисту.

Підрозділи з кіберзахисту у своїй діяльності:

керуються законами України, актами Президента України, Кабінету Міністрів України, іншими актами законодавства у сферах кіберзахисту, технічного захисту інформації, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, положенням про підрозділ з кіберзахисту, організаційно-розпорядчими документами установи;

можуть застосовувати стандарти, настанови, рекомендації та інші документи, розроблені та прийняті іноземними та міжнародними організаціями з питань кіберзахисту та захисту інформації.

2. Типовими завданнями та обов’язками підрозділів з кіберзахисту можуть бути:

розробка внутрішніх політик кібербезпеки, регламентів та інструкцій з

кіберзахисту, контроль за їх виконанням;

розробка та забезпечення впровадження плану кіберзахисту установи;

визначення вимог до захисту інформації в системах;

здійснення заходів з кіберзахисту;

забезпечення технічного захисту інформації, кіберзахисту, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

забезпечення конфіденційності, цілісності та доступності інформації в системах;

забезпечення виконання встановлених законодавством умов обробки інформації в системах;

організація і забезпечення виконання робіт з авторизації систем з безпеки;

проведення заходів з управління ризиками кібербезпеки;

моніторинг подій кібербезпеки та оперативне реагування на кіберінциденти, кібератаки та кіберзагрози щодо власних систем;

контроль в установі за дотриманням вимог законодавства у сфері кіберзахисту;

проведення навчальних заходів для підвищення кваліфікації та обізнаності співробітників установи;

проведення інструктажів і систематичних тренінгів щодо кібергігієни;

інформування відповідної CSIRT про кіберінциденти, кібератаки та кіберзагрози з урахуванням положень Національного плану.

III. Керівник з кіберзахисту в органі державної влади, відповідальна особа, яка виконує функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органі місцевого самоврядування

1. Відповідно до пункту 1 Порядку керівник з кіберзахисту в органі державної влади не може бути посадовою особою, відповідальною за цифровий розвиток, цифрову трансформацію та цифровізацію в органі державної влади. Керівнику з кіберзахисту в органі державної влади підпорядковується підрозділ з кіберзахисту органу державної влади.

З метою швидкого та ефективного виконання відповідальною особою, яка виконує функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органі місцевого самоврядування (далі – відповідальна особа), покладених на неї завдань може бути визначено її пряме підпорядкування керівнику установи або особі, яка тимчасово виконує його обов’язки.

Не рекомендується призначати відповідальних осіб із числа осіб, на яких покладено виконання основних завдань і функцій, що не стосуються кіберзахисту та захисту інформації.

2. Вимоги, яким має відповідати керівник з кіберзахисту в органі державної влади, встановлені пунктом 3 Порядку.

Визначення рівня володіння компетентностями, професійними знаннями, необхідними для ефективного виконання обов'язків керівника з кіберзахисту, може встановлюватись наявністю підтвердженої професійної кваліфікації відповідно до професійного стандарту у сфері кібербезпеки та захисту інформації (процедура підтвердження відповідної професійної кваліфікації проводиться кваліфікаційними центрами, уповноваженими Національним агентством кваліфікацій).

3. Загальні вимоги, які можуть висуватися до відповідальної особи:

мати ступінь вищої освіти за однією із спеціальностей галузі знань "Інформаційні технології" (пріоритетна спеціальність "Кібербезпека та захист інформації"), спеціальністю "Управління інформаційною безпекою" галузі знань "Безпека та оборона", спеціальностями "Електроніка, електронні комунікації, приладобудування та радіотехніка", "Інформаційно-вимірювальні технології", "Автоматизація, комп'ютерноінтегровані технології та робототехніка" галузі знань "Інженерія, виробництво та будівництво", а також спеціальністю "Публічне управління та адміністрування" галузі знань "Бізнес, адміністрування та право", що визначені переліком галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затвердженим постановою Кабінету Міністрів України від 29 квітня 2015 року № 266;

мати досвід діяльності чи стаж роботи у сфері кібербезпеки, інформаційної безпеки, захисту інформації чи інформаційних технологій не менше трьох років, а також досвід роботи на керівних посадах;

володіти компетентностями, професійними знаннями, необхідними для ефективного виконання обов'язків за відповідною посадою державної служби (крім керівника з кіберзахисту в органі державної влади, яка заміщується військовослужбовцями, особами рядового і начальницького складу або особами, яким присвоюються спеціальні звання, вимоги до яких визначаються спеціальним законодавством).

наявність підтвердженої професійної кваліфікації відповідно до професійного стандарту у сфері кібербезпеки та захисту інформації (процедура підтвердження відповідної професійної кваліфікації проводиться кваліфікаційними центрами, уповноваженими Національним агентством кваліфікацій);

володіти знаннями законодавства України у сферах технічного захисту інформації, кіберзахисту, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

володіти знаннями стандартів, настанов, рекомендацій та інших документів у сфері кіберзахисту та захисту інформації, розроблених та прийнятих іноземними та міжнародними організаціями.

4. До завдань та обов’язків керівника з кіберзахисту може належати:

розробка положення про підрозділ з кіберзахисту;

організація розробки та впровадження в межах компетенції підрозділу з кіберзахисту планів розвитку у сфері кіберзахисту, вдосконалення структури установи у відповідних сферах;

організація розробки та впровадження в межах компетенції підрозділу з кіберзахисту внутрішніх політик кібербезпеки, регламентів та інструкцій з кіберзахисту, сприяння вдосконаленню структури управління у цій сфері;

організація та управління ризиками кібербезпеки;

організація та контроль за життєвим циклом системи управління інформаційною безпекою;

контроль за виконанням встановлених законодавством умов обробки інформації в системах;

контроль за виконанням робіт з авторизації систем з безпеки;

забезпечення розробки та здійснення плану кіберзахисту установи;

організація здійснення заходів з кіберзахисту, контроль за їх виконанням;

забезпечення технічного захисту інформації, кіберзахисту, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в системах;

контроль за станом захищеності інформації в системах;

організація роботи з реагування на кіберінциденти, кібератаки та кіберзагрози, контроль за цим;

контроль в установі за дотриманням вимог законодавства у сфері кіберзахисту;

організація вивчення та ефективного використання міжнародного досвіду в межах компетенції підрозділу з кіберзахисту;

організація навчань, інструктажів та систематичних тренінгів щодо кібергігієни та заходів для підвищення професійного рівня фахівців підрозділу з кіберзахисту та співробітників установи;

забезпечення інформування відповідної CSIRT про кіберінциденти, кібератаки та кіберзагрози з урахуванням положень Національного плану, тощо.

Т.в.о. директора Департаменту кіберзахисту
Адміністрації Держспецзв’язку
майор Дмитро ПАХОЛЬЧЕНКО