Адміністрація Держспецзв’язку

Директор Департамент державного контролю у сфері захисту інформації та кіберзахисту Адміністрації Держспецзв’язку

СТЕЛЬНИК Ігор Валерійович

Державна служба спеціального зв'язку та захисту інформації України

ПОРЯДОК ОЦІНЮВАННЯ СТАНУ КІБЕРЗАХИСТУ

1. Хто підпадає під дію

Органи державної влади, державні органи, органи місцевого самоврядування, підприємства, установи, організації, які є власником або розпорядниками:

- Інформаційних, електронних, комунікаційних та інформаційно-комунікаційних систем, в яких оброблюється державні інформаційні ресурси або інформація, вимоги щодо захисту якої встановлено законом
- Об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури

2. Що оцінюється

- Інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи, в яких обробляється державні інформаційні ресурси або інформація, вимоги щодо захисту якої встановлена законом
- Об’єкти критичної інфраструктури, об’єкти критичної інформаційної інфраструктури
- Процеси та процедури, пов’язані із системами та об’єктами (у випадку оцінювання поточного стану кіберзахисту)

Крім систем та об’єктів банків

3. Суб’єкти оцінювання (оцінювачі)

- Юридичні особи, фізичні особи – підприємці або фізичні особи, що мають право на проведення відповідного виду оцінювання відповідно до вимог до суб’єктів оцінювання стану кіберзахисту та внесені до електронного каталогу оцінювачів стану кіберзахисту.
- Посадові особи, працівники органів державної влади, державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що є власниками або розпорядниками об’єктів оцінювання, та відповідають вимогам до оцінювачів для певного виду оцінювання на підставі дозволу на проведення робіт із кіберзахисту та захисту інформації, виданому власнику або розпоряднику об’єкту оцінювання*
- ДЦКЗ* та юридичні, фізичні особи приватного сектору (оцінювання (оцінка) стану захищеності)

* інформація про таких осіб не вноситься до електронного каталогу оцінювачів стану кіберзахисту

4. Сфера застосування

- Підтвердження впровадження цільових профілів з безпеки системи
- Дотримання вимог законодавства у сфері кіберзахисту
- Виявлення недоліків або порушень вимог законодавства у сфері кіберзахисту
- Формування поточного та цільового профілів стану кіберзахисту в організації, складення планів кіберзахисту
- Надання рекомендацій та вимог щодо усунення таких порушень
- Виявлення вразливостей та реагування

ВИДИ ТА ЧАСТОТА ЗДІЙСНЕННЯ ОЦІНЮВАННЯ

Оцінювання дотримання вимог цільових профілів безпеки системи	▪ 1 раз на рік ▪ При зміні БПБ/ГПБ/ЦПБ
Оцінювання поточного стану кіберзахисту (самооцінювання)	▪ 1 раз на рік
Оцінювання поточного стану кіберзахисту (зовнішнє оцінювання)	▪ Виявлення кіберінциденту (критичний (червоний) або надзвичайний (чорний)) ▪ Виявлено недоліки повноти та правильності впровадження заходів захисту або ознаки недотримання вимог законодавства у сферах кіберзахисту та захисту інформації під час заходів реагування відповідним CSIRT в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози ▪ 1 раз на 3 роки – зобов'язання для операторів КІ та/або власників або розпорядників ОКІ, ОКІІ ▪ За власним рішенням ▪ Інші випадки, визначені законодавством (наприклад, за рішенням суду)
Оцінювання на відповідність національним стандартам в сфері кіберзахисту та захисту інформації	▪ Відповідно до стандарту, відповідність якого підтверджується
Оцінювання (оцінка) стану захищеності	▪ Не частіше, ніж 1 раз на три роки (планове оцінювання стану захищеності) ▪ За зверненням власника/розпорядника

ВИМОГИ ДО ОЦІНЮВАЧІВ/СУБ’ЄКТІВ ОЦІНЮВАННЯ

Сертифікат відповідності офіційному стандарту та професійній кваліфікації з оцінювання стану кіберзахисту (далі – сертифікат відповідності) видається кваліфікаційним центром інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки

Підтверджує достатній фаховий рівень підготовки оцінювача стану кіберзахисту (підтверджену кваліфікацію) за програмою базової підготовки

Фізичні особи, які мають вищу освіту відповідного рівня та ступеня (магістр, спеціаліст) у галузі знань «Інформаційна безпека», «Кібербезпека та захист інформації», «Електронні комунікації та радіотехніка», чинний сертифікат «Провідний аудитор інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)»

Виданий Кваліфікаційним центром або Органом із сертифікації персоналу

Має стаж роботи у галузі кіберзахисту за напрямом оцінювання стану кіберзахисту не менш як три роки

Пройшов навчання за програмою базової підготовки та успішно склав кваліфікаційний іспит

Для суб’єктів господарювання: у складі має працювати хоча б один оцінювач що має право на проведення відповідного виду оцінювання, та внесений до електронного каталогу суб’єктів оцінювання стану кіберзахисту

Внесення даних про оцінювачів/суб’єктів оцінювання до Електронного каталогу суб’єктів оцінювання стану кіберзахисту відбувається на підставі подання до Адміністрації Держспецзв’язку відповідної заяви про внесення даних до Каталогу.

ПОРЯДОК ЗДІЙСНЕННЯ ДЕРЖАВНОГО КОНТРОЛЮ ЗА ДОДЕРЖАННЯМ ВИМГ ЗАКОНОДАВСТВА У СФЕРІ КІБЕЗАХИСТУ

СУБ’ЄКТИ ДЕРЖАВНОГО КОНТРОЛЮ

Органи державної влади, державні органи місцевого самоврядування, підприємства, установи, організації, які є власниками або розпорядниками:

- Інформаційних, електронних, комунікаційних та інформаційно-комунікаційних систем, в яких оброблюється державні інформаційні ресурси або інформація, вимоги щодо захисту якої встановлено законом
- Об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури

Крім банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України

ОБ’ЄКТИ ДЕРЖАВНОГО КОНТРОЛЮ:

- Інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи
- Об’єкти критичної інфраструктури, об’єктів критичної інформаційної інфраструктури
- Процеси та процедури суб’єктів державного контролю

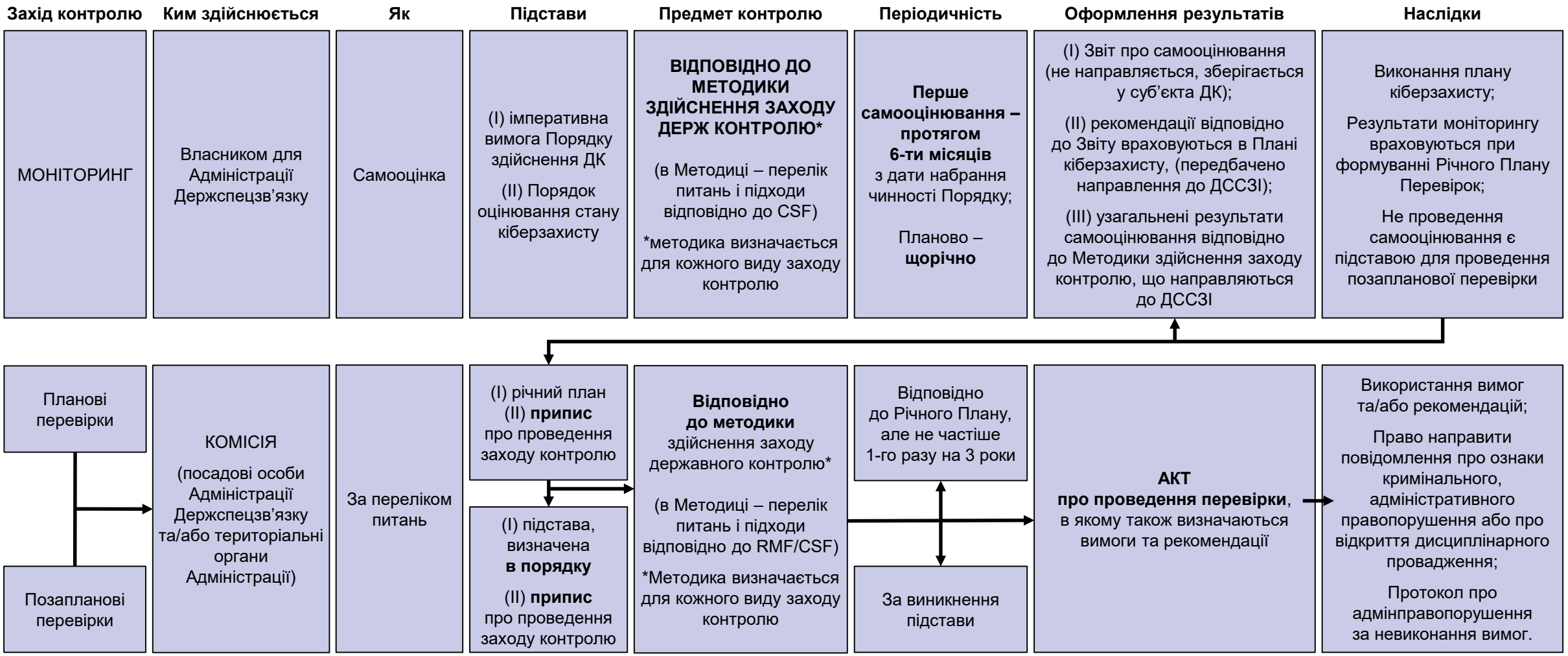
СФЕРА ЗАСТОСУВАННЯ::

- Дотримання вимог законодавства у сфері кіберзахисту
- Виявлення недоліків або порушень вимог законодавства у сфері кіберзахисту
- Надання рекомендацій та вимог щодо усунення таких порушень
- Запобігання таким порушенням у майбутньому

СПОСОБИ ЗДІЙСНЕННЯ	▪ Моніторинг стану кіберзахисту ▪ Перевірки проводяться у форматі планових або позапланових
ПІДСТАВИ ДЛЯ ЗДІЙСНЕННЯ (ПЛАНОВИХ) ЗАХОДІВ	▪ Збір та аналіз інформації про виконання заходів з оцінювання стану кіберзахисту (моніторинг стану кіберзахисту) ▪ Річний план здійснення заходів державного контролю (планові перевірки, не частіше, ніж 1 раз на 3 роки)
ПІДСТАВИ ДЛЯ ПОЗАПЛАНОВИХ ПЕРЕВІРОК	▪ Звернення суб'єкта ▪ Повідомлення органу державної влади, державного органу, правоохоронного або контррозвідувального органу, який встановив ознаки порушення вимог законодавства в сфері кіберзахисту ▪ Неотримання Адміністрацією Держспецзв'язку інформації про: • Проведення суб'єктом державного контролю планової або позапланової авторизації з безпеки системи • Проведення суб'єктом державного контролю щочного оцінювання стану кіберзахисту для цілей здійснення моніторингу • проведення суб'єктом державного контролю оцінювання поточного стану кіберзахисту на підставі рекомендацій, наданих у встановленому законодавством порядку відповідною CSIRT в рамках функціонування національної системи реагування на куберінциденти, кібератаки, кіберзагрози. • Виконання у встановлені терміни вимог, визначених в акті про проведення перевірки.

МЕТОДИ ПРОВЕДЕННЯ ПЕРЕВІРОК	▪ Метод дослідження – процес огляду, вивчення, інспектування, спостереження або аналізу авторизованих систем та ІКС ▪ Метод опитування – процес проведення опитування відповідальних осіб за кіберзахист та інформаційні технології щодо авторизованих систем та ІКС ▪ Метод випробування – сканування та тестування на вразливість ІКС ▪ Метод аналізу – процес детального вивчення та дослідження отриманих даних під час перевірки та вивчення фактичного стану захисту
РЕЗУЛЬТАТИ ПЕРЕВІРКИ	**Щодо дотримання вимог законодавства та достатності впроваджених заходів захисту цільових профілів безпеки в авторизованих системах** ▪ Загальна оцінка стану кіберзахисту ▪ Підтвердження авторизації з безпеки системи ▪ Формування/подальшого створення адаптованого профілю безпеки інформації та формування/уточнення планів кіберзахисту суб'єктом перевірки ▪ Подальші заходи впливу з метою усунення виявлених недоліків • Скасування авторизації з безпеки • Перевірка наявності ознак кримінальних, адміністративних правопорушень в діяльності власника (розпорядника) об'єкта державного контролю • Порушення дисциплінарних проваджень за наявності ознак невиконання або неналежного виконання посадових обов'язків в частині виконання функцій та завдань з кіберзахисту у власника (розпорядника) об'єкта державного контролю.
ЩОДО ДОТРИМАННЯ ВИМОГ БАЗОВИХ ЗАХОДІВ З КІБЕРЗАХИСТУ	▪ Визначення рівню кіберзахисту ▪ Вимоги до розробки/оновлення поточного та цільового профілів кіберзахисту ▪ Формулювання набору дій, що дозволять запровадити цільовий профіль кіберзахисту та визначення пріоритетів цільового профілю ▪ Вимоги до формування/уточнення планів захисту об'єкта оцінювання

ДЕРЖАВНИЙ КОНТРОЛЬ ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА В СФЕРІ КІБЕРЗАХИСТУ



Державна служба спеціального зв'язку та захисту інформації України