КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРИСТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Правове забезпечення кібербезпеки суб'єктів владних повноважень

Спікер:
Олег ЗАЯРНИЙ,
професор кафедри інтелектуальної власності
та інформаційного права ННІ права
Київського національного університету
імені Тараса Шевченка,
д.ю.н., професор

План тренінгового заняття:

1. Що таке кібербезпека та які є основні її загрози?
2. Які суб’єкти владних повноважень забезпечують кібербезпеку та за якими критеріями здійснюється розмежування їхньої компетенції?
3. Які існують засоби забезпечення кібербезпеки суб’єктів владних повноважень та в чому виявляються особливості їх застосування?
4. Як забезпечити кібербезпеку посадових осіб суб’єктів владних повноважень?

Що таке кібербезпека суб’єкта владних повноважень?

Кібербезпека суб’єкта владних повноважень - захищеність життєво важливих інтересів та технологічної інфраструктури суб’єкта владних повноважень під час використання кіберпростору, з метою виконання покладених на нього обов’язків, за якої забезпечуються сталий розвиток інформаційного суспільства та електронного урядування, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Що таке кіберзагроза?

Кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів, п. 6 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України».

Які існують основні види загроз для кібербезпеки суб’єктів владних повноважень?

- ✓ Гібридна агресія російської федерації проти України у кіберпросторі
- ✓ Кіберзлочинність
- ✓ Організовані та спонсоровані урядами інших держав кібератаки

Які існують основні загрози для кібербезпеки посадових осіб суб’єктів владних повноважень?

- ✓ Видалення, блокування або зміна офіційного акаунта посадової особи у соціальних мережах
- ✓ Видалення, перехоплення або втручання в роботу офіційної електронрої пошти посадової особи
- ✓ Умисна зміна умов і способів авторизації посадової особи у публічних реєстрах, інших інформаційно-телекомунікаційних системах, які використовуються для виконання посадових обов’язків
- ✓ Умисна зміна інформації про посадову особу шляхом втручання в роботу публічних інформаційно-телекомунікаційних систем, соціальних мереж, тощо
- ✓ Підробка ключів електронних довірчих послуг
- ✓ Дизінформація у віртуальному просторі щодо посадової особи
- ✓ Кібершпигунство проти конкретної посадової особи
- ✓ Незаконна обробка персональних даних про посадову особу, що здійснюється у віртуальному просторі

Які органи державної влади забезпечують в Україні кібербезпеку суб’єктів владних повноважень?

- Президент України
- Рада національної безпеки і оборони України
- Служба безпеки України
- Департамент кіберполіції Національної поліції України
- Адміністрація Державної служби спеціального зв’язку та захисту інформації

За якими критеріями здійснюється розмежування компетенції державних органів, завданням яких є забезпечення кібербезпеки суб'єктів владних повноважень?

- **Зміст та маштаб кіберзагроз**
- **Ступень впливу на національні інтереси**
- **Напрям публічного управління, де має прояв конкретних кіберзагроз**
- **Види засобів протидії кіберзагрозам**

Які існують основні види засобів протидії кіберзагрозам суб’єктів владних повноважень?

- **Правові**
- **Технологічні**
- **Організаційні**

Які існують основні засоби засоби забезпечення кібербезпеки суб’єктів владних повноважень?

- ✓ Закони України
- ✓ Підзаконні нормативно-правові акти, перед усім положення про публічні інформаційні системи, реєстри, правила інформаційних обмінів, порядки технічного захисту інформації
- ✓ Засоби державного регулювання інформаційної діяльності: національні і міжнародні стандарти у сфері кібербезпеки, ліцензійні умови провадження окремих видів інформаційної діяльності, сертифікація, наприклад, обладнення для критичної інформаційної інфраструктури України, публічні закупівні для потреб національної безпеки
- ✓ Заходи юридичної відповідальності та заходи юридичного примусу, непов’язані із притягненням до юридичної відповідальності.

В чому виявляються особливості юридичних засобів забезпечення кібербезпеки?

- ✓ **Приймаються і застосовуються за встановленою законодавством України процедурою**
- ✓ **Можуть мати як нормативний, так і індивідуальний характер**
- ✓ **Визначають юридичні характеристики кіберзагроз та конкретні засоби їх запобігання**
- ✓ **Встановлюють юридичні вимоги до технічного захисту інформації та елементів публічної інформаційної інфраструктури**
- ✓ **Можуть застосовуватися за рішенням компетентного державного органу**

Які існують основні технологічні засоби протидії загрозм для кібербезпеки суб’єктів владних повноважень?

- **Спеціально створене програмне забезпечення**
- **Комплексна система захисту інформації**
- **Багаторівнева автентифікація користувачів публічних інформаційних ресурсів**
- **Хмарні сервіси та технології резенвування даних**
- **Багатокомпонентні паролі та ідентифікатори входу в систему**

В чому виявляються особливості технологічних засобів протидії кіберзагрозам суб’єктів владних повноважень?

- **Повинні узгоджуватися із завданнями діяльності конкретного суб’єкта владних повноважень**
- **Мають динамічний характер**
- **Застосовуються переважно адміінстраторами конкретних публічних інформаційних ресурсів**
- **Застосовуються за принципами проєктування і за замовчуванням**
- **Повинні відповідати конкретним адміністративним процедурам, що автоматизуються**
- **Повинні узгоджуватися з правовими режимами інформації, яка підлягаю захисту**

Які існують організаційні заходи протидії кіберзагрозам суб'єктів владних повноважень?

- **Рольовий розподіл доступу до публічних інформаційних ресурсів відповідно до посадових обов'язків**
- **Ведення автоматизованого журналу обліку кіберінциндентів по кожному реєстру, базі даних**
- **Призначення відповідальної особи або утворення окремого структурного підрозділу з питань забезпечення інформаційної безпеки та технічного захисту інформації**
- **Чітке розмежування функцій володільця і адміністратора інформаційної системи, реєстру, бази даних**
- **Постійне навчання і підвищення кваліфікації з питань кібербезпеки і кібергігієни**
- **Постійне удосконалення ІТ-архітектури публічних інформаційних ресурсів відповідно до існуючих та потенційнихї кіберзагроз**

В чому виявляються особливості застосування організаційних засобів протидії загрозам кібербезпеки суб’єктів владних повноважень?

- **Мають переважно внутрішній (службовий) характер**
- **Застосовуються на підставі наказу/розпорядження керівника суб’єкта владних повноважень**
- **Тягнуть за собою необхідні технологічні рішення**
- **Потребують постійного удосконалення**

Які заходи необхідно вжити для забезпечення кібербезпеки посадових осіб суб'єктів владних повноважень?

- ✓ **Автоматизований розподіл доступу до інформаційних систем**
- ✓ **Визначення за необхідності у посадових інструкціях обов'язків щодо забезпечення кібербезпеки суб'єкта владних повноважень**
- ✓ **Застосування виключно кваліфікованого електронно-цифрового підпису**
- ✓ **Використання для службових цілей лише корпоративної пошти**
- ✓ **Створення резервних копій службової документації у захищених хмарних сервісах**
- ✓ **Розповсюдження публічної інформації лише через офіційний сайт суб'єкта владних повноважень або шляхом використання офіційних сторінок у соціальних мережах**
- ✓ **Уникнення випадків електронних згадок про фізичних осіб без їхньої належної згоди, крім випадків, коли дозвіл на таку згадку наданий законом**
- ✓ **Використання дворівневої автентифікації при вході у службові сервіси**
- ✓ **Ведення журналів обліку подій у публічних інформаційних системах**

ДЯКУЮ ЗА УВАГУ!