Тема 4. Режим секретності та технічний захист інформації

Мета лекції: ознайомлення з нормативно-правовими засадами та практичними механізмами забезпечення режиму секретності, криптографічного та технічного захисту інформації в державних органах України, а також з організацію документообігу з грифованими документами, функціонуванням КСЗІ. Ознайомлення з основними ризиками електронних інформаційних ресурсів, зокрема каналами витоку інформації. З'ясування порядку допуску до державної таємниці та особливостями режиму секретності в умовах воєнного стану.

Зміст теми:

01

Документообіг з грифом «Таємно» та «ДСК»

Організаційні вимоги до роботи з грифованими документами, порядок їх обліку, зберігання та знищення.

02

Криптографічний захист зв'язку

Засоби та методи криптографічного захисту інформації при передачі каналами зв'язку.

03

Фельд'єгерський та спеціальний зв'язок

Правила використання спеціальних каналів доставки документів та відповідальність за порушення.

04

КСЗІ — Комплексна система захисту інформації

Архітектура, складові та принципи побудови комплексної системи захисту інформації на об'єктах.

05

Технічні канали витоку інформації

Класифікація та характеристика технічних каналів, методи їх нейтралізації.

06

Допуск, доступ та воєнний стан

Порядок оформлення допуску до державної таємниці та специфіка режиму секретності в умовах воєнного стану.

Організація документообігу з грифом «Таємно» та «ДСК»

Гриф «Для службового користування» (ДСК)

Застосовується до службової інформації, що не є державною таємницею, але потребує обмеженого поширення. Документи з грифом ДСК обліковуються в спеціальних журналах, передаються лише визначеним особам під підпис, не підлягають розголошенню та копіюванню без дозволу керівника. Строк дії грифу — до зняття відповідним рішенням.

Гриф «Таємно» та «Цілком таємно»

Документи з грифом «Таємно» та «Цілком таємно» є носіями державної таємниці. Їх обіг регулюється Законом України «Про державну таємницю» та відповідними підзаконними актами СБУ. До таких документів мають доступ виключно особи з оформленим допуском відповідної форми. Документи зберігаються у сертифікованих сейфах або спецсховищах, реєструються у секретних підрозділах та обліковуються пронумерованими журналами.

Ключові вимоги до документообігу

Суворий поаркушний облік та реєстрація всіх примірників

Передача лише через режимно-секретний підрозділ (РСП)

Заборона несанкціонованого копіювання та фотографування

Обов'язковий інструктаж виконавця перед наданням доступу

Знищення — лише комісійно з оформленням актів

Нормативно-правова база

Основою режиму секретності та захисту інформації в Україні є низка законодавчих та нормативно-правових актів, які регулюють порядок поводження з документами та захист даних.

Закон України «Про державну таємницю»

Визначає правові основи охорони державної таємниці та порядок доступу до неї.

Переглянути на Zakon.rada.gov.ua

Закон України «Про інформацію»

Регулює відносини щодо збирання, обробки, зберігання та поширення інформації.

Переглянути на Zakon.rada.gov.ua

Закон України «Про захист інформації в ІТС»

Встановлює вимоги до захисту даних в інформаційно-телекомунікаційних системах.

Переглянути на Zakon.rada.gov.ua

Закон України «Про правовий режим воєнного стану»

Визначає особливості функціонування державних органів та режим інформації під час воєнного стану.

Переглянути на Zakon.rada.gov.ua

Закон України «Про Службу безпеки України»

Визначає повноваження СБУ у сфері охорони державної таємниці та захисту національної безпеки.

Переглянути на Zakon.rada.gov.ua

Звід відомостей, що становлять державну таємницю

Постанова КМУ, що визначає конкретні категорії відомостей, які відносяться до державної таємниці.

Переглянути на Zakon.rada.gov.ua

Криптографічний захист зв'язку

Криптографічний захист є одним із ключових елементів системи захисту інформації в державних органах. Він забезпечує конфіденційність, цілісність та автентичність інформації при її передачі відкритими та закритими каналами зв'язку.

Симетричне шифрування

Використовує один спільний ключ для шифрування та дешифрування. Застосовується для захисту великих обсягів даних. В Україні використовуються сертифіковані ДСТУ алгоритми, зокрема ДСТУ ГОСТ 28147-2009 та сучасні розробки ДСТСЗІ.

Асиметричне шифрування

Базується на парі ключів — відкритому та закритому. Використовується для захищеного обміну ключами та електронного підпису. Забезпечує автентифікацію сторін зв'язку та неможливість відмови від авторства.

Електронний цифровий підпис (ЕЦП)

Забезпечує підтвердження авторства та цілісності електронного документа. Використання кваліфікованого електронного підпису є обов'язковим при обміні грифованими документами в електронній формі через захищені канали.

Захищені канали передачі даних

VPN-тунелювання, протоколи TLS/SSL у сертифікованих реалізаціях, а також апаратні криптомодулі застосовуються для захисту урядових та відомчих мереж. Дозволу на застосування підлягають лише засоби криптографічного захисту, сертифіковані ДСТСЗІ СБУ.

Важливо: Використання несертифікованих засобів криптографічного захисту для передачі інформації з обмеженим доступом є грубим порушенням законодавства та тягне дисциплінарну або кримінальну відповідальність.

Фельд'єгерський та спеціальний зв'язок

Фельд'єгерський зв'язок

Фельд'єгерська служба України (ФСУ) є спеціальним державним органом, що забезпечує гарантовану доставку офіційної кореспонденції, у тому числі грифованих документів. Правовою основою є Закон України «Про фельд'єгерський зв'язок». Кореспонденція передається кур'єром особисто, у опломбованих і опечатаних пакетах. Адресат зобов'язаний розписатися у реєстрі доставки та перевірити цілісність упаковки.

Правила передачі

- Пакети здаються до ФСУ через РСП установи
- Обов'язкова нумерація та реєстрація відправлення
- Підтвердження отримання повертається відправнику
- Пошкоджена упаковка — підстава для складання акту

Спеціальний зв'язок

Спеціальний зв'язок здійснюється через захищені технічні засоби: урядовий зв'язок («Оберіг», «Базальт» тощо), захищені відеоконференції та шифровані телефонні лінії. Право на використання спеціального зв'язку мають лише посадові особи, включені до відповідних переліків та які мають допуск до державної таємниці.

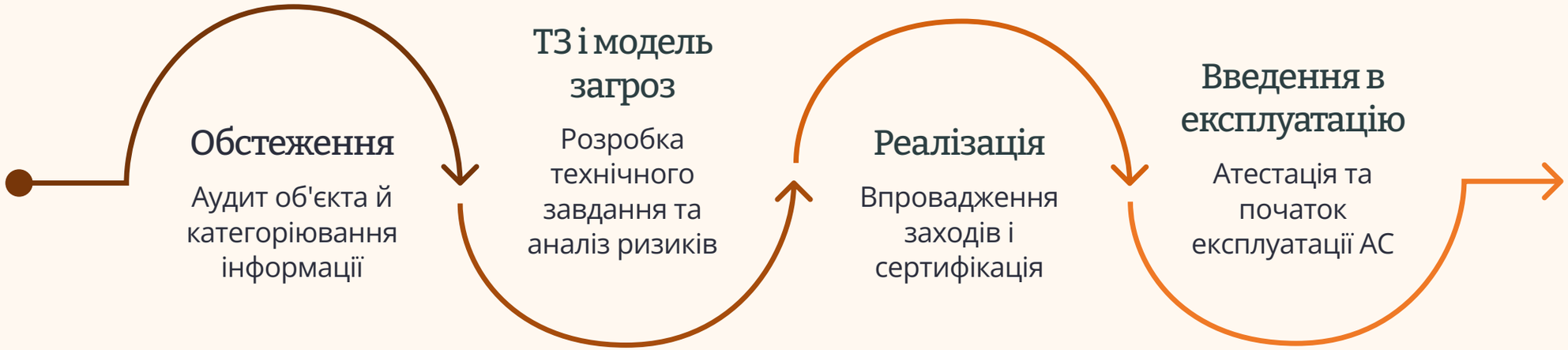
Заборонені дії

- Передача таємної інформації незахищеними засобами (Viber, WhatsApp, e-mail)
- Розмови про таємні відомості по відкритому телефону
- Передача грифованих документів стороннім особам без повноважень
- Самовільне копіювання та пересилання документів ДСК і «Таємно»

Захист інформаційних систем

Комплексна система захисту інформації (КСЗІ)

КСЗІ — це впорядкована сукупність організаційних та технічних заходів, засобів і методів, що забезпечують захист інформації в автоматизованих системах (АС) державних органів від несанкціонованого доступу, витоку та порушення цілісності.



Відповідно до НД ТЗІ 3.7-003-05, КСЗІ в АС державних органів підлягає обов'язковій атестації з видачею атестата відповідності. Без проходження атестації обробка інформації з обмеженим доступом в автоматизованій системі є незаконною.

Організаційні заходи КСЗІ

- Призначення адміністратора безпеки
- Розробка політики безпеки інформації
- Ведення журналів аудиту та доступу
- Навчання та інструктаж персоналу
- Контроль фізичного доступу до ресурсів АС

Технічні заходи КСЗІ

- Міжмережеві екрани та системи виявлення вторгнень (IDS/IPS)
- Засоби криптографічного захисту даних
- Антивірусне програмне забезпечення (сертифіковане)
- Захист від витоку по технічних каналах (ПЕМВН)
- Резервне копіювання та відновлення даних

Технічні канали витоку інформації

Технічний канал витоку інформації (ТКВІ) — це сукупність джерела інформативного сигналу, фізичного середовища його поширення та технічного засобу перехоплення. Розуміння природи ТКВІ є основою для побудови ефективної системи технічного захисту інформації (ТЗІ).

ПЕМВН (Побічні електромагнітні випромінювання та наводки) — один із найнебезпечніших каналів витоку. Комп'ютерна техніка випромінює електромагнітні сигнали, що можуть бути перехоплені на відстані до кількох сотень метрів спеціалізованою апаратурою. Захист — екранування приміщень, використання сертифікованої техніки класу «Ф».

Допуск та доступ до державної таємниці

Поняття «Допуск»

Допуск до державної таємниці — це оформлення права особи на доступ до секретної інформації, що здійснюється органами СБУ після проведення перевірочних заходів. Існують три форми допуску, що відповідають ступеням секретності: форма 1 — «Цілком таємно», форма 2 — «Таємно», форма 3 — «Для службового користування». Допуск оформлюється за ініціативою керівника установи і є обов'язковою передумовою для роботи з відповідними відомостями.

Поняття «Доступ»

Доступ до державної таємниці — це надання особі, яка має відповідний допуск, права на ознайомлення з конкретними таємними відомостями або на роботу з ними. Наявність допуску не означає автоматичного доступу до всіх відомостей — доступ надається лише в межах службової необхідності (принцип «необхідно знати»).

Підстави для відмови або скасування допуску

Судимість

Наявність незнятої або непогашеної судимості за умисні злочини

Психічні розлади

Встановлені медичними органами психічні розлади або наркотична залежність

Зв'язки за кордоном

Постійне проживання близьких родичів за кордоном або систематичні контакти з іноземними громадянами

Порушення режиму

Попередні факти розголошення таємниці або порушення режиму секретності

Відмова від перевірки

Відмова особи від проходження перевірочних заходів або надання неправдивих відомостей

Воєнний стан

Особливості режиму секретності в умовах воєнного стану

Введення воєнного стану в Україні (лютий 2022 — по теперішній час) суттєво вплинуло на правовий режим захисту інформації та порядок роботи з державною таємницею. Закон України «Про правовий режим воєнного стану» та Укази Президента України передбачають посилення заходів інформаційної безпеки та встановлюють додаткові обмеження.

Розширення переліку таємних відомостей

В умовах воєнного стану значно розширюється перелік відомостей, що відносяться до державної таємниці. Додатково засекречуються відомості про переміщення військ, втрати, дислокацію об'єктів критичної інфраструктури, плани оборони та мобілізаційні ресурси.

Прискорений порядок оформлення допуску

Для осіб, залучених до виконання завдань в умовах воєнного стану, може застосовуватися спрощений та прискорений порядок оформлення допуску до державної таємниці з подальшим проведенням повної перевірки після нормалізації обстановки.

Посилена відповідальність

Кримінальна відповідальність за розголошення державної таємниці в умовах воєнного стану суттєво посилюється. Відповідно до ч. 3 ст. 328 КК України, розголошення, що спричинило тяжкі наслідки, в умовах воєнного стану карається позбавленням волі на строк від 10 до 15 років.

→ Заборона публікацій у соціальних мережах

Військовослужбовцям та цивільним особам, які мають доступ до чутливої інформації, заборонено публікувати в соціальних мережах та месенджерах відомості про переміщення техніки, місця дислокації, втрати та будь-яку іншу інформацію, що може становити тактичну або стратегічну цінність для противника.

→ Посилений контроль засобів зв'язку

На об'єктах критичної інфраструктури та у режимних установах вводяться додаткові обмеження на використання особистих мобільних телефонів з камерами, введення в дію несертифікованих засобів зв'язку та будь-яких пристроїв, здатних передавати інформацію за межі контрольованої зони.

→ Взаємодія з органами СБУ та ГУР

В умовах воєнного стану керівники режимно-секретних підрозділів зобов'язані негайно повідомляти органи СБУ про будь-які факти або підозри щодо витоку інформації, вербування персоналу чи несанкціонованих спроб отримання доступу до засекречених відомостей.

Підсумки теми

Ключові висновки та практичні рекомендації

Режим документообігу

Суворе дотримання правил обліку, зберігання та передачі грифованих документів є особистим обов'язком кожного виконавця та керівника режимно-секретного підрозділу.

Технічний захист

Побудова ефективної КСЗІ та нейтралізація технічних каналів витоку є системним завданням, що потребує поєднання організаційних та технічних заходів.

Допуск і доступ

Принцип «необхідно знати» є фундаментальним: наявність допуску не дає права знайомитися з усіма секретними матеріалами — лише з тими, що потрібні для виконання службових обов'язків.

Воєнний стан

В умовах воєнного стану вимоги режиму секретності різко посилюються, а відповідальність за їх порушення зростає до рівня тяжкого кримінального злочину проти національної безпеки.

Висновок: Захист державної таємниці — це не бюрократична формальність, а реальний внесок кожного працівника у забезпечення національної безпеки та обороноздатності України. Недбалість або умисне порушення режиму секретності в умовах збройного конфлікту може мати незворотні наслідки для держави та людських життів.

Електронна ідентифікація

Використання КЕП у службовому документообігу

Кваліфікований електронний підпис (КЕП) є обов'язковим інструментом ідентифікації у службовому електронному документообігу державних органів України. Його застосування регулюється Законом України «Про електронні довірчі послуги» № 2155-VIII від 05.10.2017.

Що таке КЕП

Кваліфікований електронний підпис — це електронний підпис, створений за допомогою засобу кваліфікованого електронного підпису та базується на кваліфікованому сертифікаті відкритого ключа.

Юридична сила

КЕП має таку саму юридичну силу, як власноручний підпис, та є обов'язковим при підписанні електронних документів у державних органах.

Акредитовані постачальники

Кваліфіковані довірчі послуги надають акредитовані центри сертифікації ключів (АЦСК): ДП «ДІЯ», АЦСК органів юстиції, АЦСК СБУ, АЦСК Мінцифри та інші.

Сфери застосування

Підписання наказів, звітів, службових записок в електронній формі; обмін документами через СЕД; подання звітності до державних органів.

Вимоги до КЕП у грифованому документообігу

- КЕП для роботи з документами ДСК має бути виданий акредитованим АЦСК
- Для документів з грифом «Таємно» використовуються лише сертифіковані ДСТСЗІ засоби ЕП
- Ключові носії (токени) зберігаються у режимно-секретному підрозділі
- Заборонено використання іноземних засобів електронного підпису
- Обов'язкова перевірка чинності сертифіката перед підписанням

Порядок отримання КЕП

1. Звернення до акредитованого АЦСК з пакетом документів
2. Ідентифікація особи (особиста присутність або через Дія)
3. Генерація ключової пари та отримання сертифіката
4. Отримання захищеного носія (токен/смарт-карта)
5. Реєстрація у системі електронного документообігу установи

Відповідно до Закону України «Про електронні довірчі послуги», використання некваліфікованого електронного підпису замість КЕП у службовому документообігі державних органів є порушенням і може призвести до визнання документа недійсним.

Відповідальність за порушення режиму секретності

Законодавство України передбачає сувору юридичну відповідальність за порушення режиму секретності та вимог щодо захисту інформації. Залежно від характеру правопорушення, тяжкості наслідків та умов скоєння, до порушників застосовуються різні види стягнень та покарань.

- Кримінальна відповідальність
- Адміністративна відповідальність
- Дисциплінарна відповідальність
- Цивільно-правова відповідальність

Кримінальна відповідальність (КК України)

Ст. 328 — Розголошення державної таємниці

Позбавлення волі: 2–5 років (ч. 1); 5–10 років (ч. 2, тяжкі наслідки); 10–15 років (ч. 3, воєнний стан).

Ст. 329 — Втрата документів

Обмеження або позбавлення волі на строк до 3 років.

Ст. 330 — Передача або збирання відомостей

Позбавлення волі на строк від 2 до 5 років.

Ст. 111 — Державна зрада (шпигунство)

Позбавлення волі від 12 до 15 років або довічне ув'язнення.

Адміністративна відповідальність (КУпАП)

Ст. 212-2 — Порушення законодавства про інформацію

Штраф від 5 до 10 неоподатковуваних мінімумів доходів громадян.

Ст. 212-5 — Порушення порядку обліку та зберігання

Адміністративна відповідальність за порушення правил поводження з носіями інформації.

Електронна ідентифікація

Доступ до ЄРДР: хто має право входу

Єдиний реєстр досудових розслідувань (ЄРДР) — це державна інформаційна система, доступ до якої суворо обмежений і здійснюється виключно з використанням кваліфікованого електронного підпису (КЕП). Несанкціонований доступ або спроба входу без КЕП є грубим порушенням законодавства.

Слідчі та детективи

Слідчі органів досудового розслідування (Національна поліція, ДБР, НАБУ, СБУ, БЕБ) та детективи, які безпосередньо ведуть кримінальне провадження. Доступ надається виключно в межах проваджень, що перебувають у їх провадженні.

Прокурори

Прокурори, які здійснюють процесуальне керівництво досудовим розслідуванням. Мають право перегляду матеріалів проваджень, що перебувають під їх наглядом, та внесення відповідних відомостей.

Керівники органів

Керівники органів досудового розслідування та їх заступники в межах повноважень, визначених КПК України та відомчими нормативними актами.

Вимоги до КЕП для входу в ЄРДР

- КЕП має бути виданий акредитованим АЦСК відповідного відомства
- Сертифікат повинен містити атрибути посади та підрозділу
- Обов'язкова наявність чинного допуску до роботи з реєстром
- Вхід фіксується в журналі аудиту системи
- Заборонено передавати облікові дані та КЕП іншим особам

Правова основа

1. КПК України — ст. 214 (порядок внесення відомостей до ЄРДР)
2. Наказ Генерального прокурора № 139 від 06.04.2016 — Положення про ЄРДР
3. Закон України «Про електронні довірчі послуги» № 2155-VIII
4. Наказ МВС, ДБР, НАБУ, СБУ, БЕБ про порядок доступу до ЄРДР

⚠ **Вхід до ЄРДР без КЕП або з використанням чужого підпису є незаконним.** Усі дії в реєстрі протоколюються та можуть бути використані як доказ у дисциплінарному або кримінальному провадженні.

Нормативно-правові акти та рекомендована література

Список джерел

Законодавчі акти

Конституція України (ст. 17, 32, 34)

Основи інформаційної безпеки та державної таємниці.
Переглянути →

Закон України «Про державну таємницю»

№ 3855-XII від 21.01.1994. **Переглянути →**

Закон України «Про інформацію»

№ 2657-XII від 02.10.1992. **Переглянути →**

Закон «Про захист інформації в ІТС»

№ 80/94-ВР від 05.07.1994. **Переглянути →**

Закон «Про правовий режим воєнного стану»

№ 389-VIII від 12.05.2015. **Переглянути →**

Закон «Про Службу безпеки України»

№ 2229-XII від 25.03.1992. **Переглянути →**

Кримінальний кодекс України (ст. 111, 328, 329, 330)

Відповідальність за порушення у сфері держтаємниці.
Переглянути →

Кодекс України про адміністративні правопорушення (ст. 212-2, 212-5)

Відповідальність за порушення режиму захисту. **Переглянути →**

Підзаконні нормативні акти

Звід відомостей, що становлять державну таємницю

Постанова КМУ. **Переглянути →**

НД ТЗІ 3.7-003-05

Порядок проведення робіт із створення КСЗІ в ІТС (ДСТСЗІ СБУ).

ДСТУ 9311:2024 Інформаційні технології. Криптографічний захист інформації. Алгоритм криптографічного перетворення

Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за додержанням порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни : Наказ Центрального управління Служби безпеки України 18.08.2017 № 471

Рекомендована література

Ліпкан В.А. «Інформаційна безпека України в умовах євроінтеграції»

К.: КНТ, 2006.

Гуцалюк М.В. «Захист інформації: організаційно-правові засади»

К., 2010.

Офіційний сайт Верховної Ради України

База нормативно-правових актів. **Переглянути →**

Офіційний сайт ДСТСЗІ СБУ

Технічний захист інформації. **Переглянути →**