ПЛАН-КОНСПЕКТ

для проведення заняття в системі службової підготовки із середнім та старшим начальницьким складом (1,2 група) Вищого професійного училища Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Вид підготовки: профільна підготовка

Тема: №9 «Організація та забезпечення заходів технічного захисту інформації. Захист інформації в телекомунікаційних, інформаційних та інформаційно-телекомунікаційних системах органів та підрозділів цивільного захисту

Навчальна мета: Ознайомлення співробітників з поняттям заходів технічного захисту інформації. Захист інформації в телекомунікаційних, інформаційних та інформаційно-телекомунікаційних системах органів та підрозділів цивільного захисту.

Час проведення:2 академ. год. (90 хв.)

Місце проведення: Лекційний зал

Навчально-матеріальне забезпечення: план-конспект.

Нормативно-правові акти та література:

1. Наказ ДСНС України від 22.03.2019 року № 183 «Про використання відомчої електронної поштової системи».
2. Наказ ДСНС України від 19.07.2019 року № 425 «Про затвердження Порядку використання інформаційних та інформаційно- телекомунікаційних систем і Порядку використання та обліку комп'ютерних програм».
3. Наказ ДСНС 11.12.2013 № 755 Про затвердження Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій

Порядок проведення заняття:

1. Організаційні заходи - 5 хв.: перевірка присутніх; оголошення теми і мети заняття.
2. Викладення матеріалу теми - 75 хв.

Питання № 1 Організація та забезпечення заходів технічного захисту інформації.

Техні́чний за́хист інформа́ції (*ТЗІ*) — діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Система ТЗІ – сукупність суб’єктів, об’єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та їхня матеріально-технічна база.

Комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення.

Цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення.

Доступність - властивість інформації бути захищеною від несанкціонованого блокування.

3.2. Об'єкти та суб'єкти технічного захисту інформації

Організація технічного захисту інформації та відповідальність за його стан в апараті ДСНС України та Установах покладається на керівників.

До об'єктів технічного захисту належить інформація, вимога щодо захисту якої встановлена законом. До об'єктів захисту в ІТС, крім того, відноситься програмне забезпечення, що призначене для обробки цієї інформації.

Суб'єкти системи технічного захисту інформації:

- комісії з питань технічного захисту інформації;

- підрозділи технічного захисту інформації (підрозділи з питань телекомунікацій, інформаційних технологій та захисту інформації і підрозділи технічного захисту інформації, що призначені для виконання робіт з ТЗІ);

- служби захисту інформації в ІТС;

- режимно-секретні органи.

Комісія з питань технічного захисту інформації (далі - комісія з питань ТЗІ) призначається наказом керівника. Комісію з питань ТЗІ в апараті ДСНС очолює керівник окремого структурного підрозділу апарату, відповідальний за організацію виконання заходів з питань ТЗІ.

До складу комісії з питань ТЗІ обов'язково повинні входити керівники структурного підрозділу з питань телекомунікацій, інформаційних технологій та захисту інформації, режимно-секретного органу, штатної (позаштатної) служби захисту інформації в ІТС, документального забезпечення. До складу комісії з питань ТЗІ можуть включатися представники інших структурних підрозділів.

Головними завданнями комісії з питань ТЗІ є:

- підготовка пропозицій керівнику стосовно визначення завдань підрозділам, від яких залежить виконання у повному обсязі вимог ТЗІ;

- організація контролю за виконанням вимог з ТЗІ;

- обстеження умов інформаційної діяльності;

- визначення переліку об'єктів, на яких буде оброблятися інформація з обмеженим доступом за допомогою технічних засобів та (або) будуть проводитися заходи з озвучуванням такої інформації;

- проведення категоріювання об'єктів інформаційної діяльності (далі - ОІД);

розслідування випадків порушення встановлених норм та вимог з питань ТЗІ, що створюють загрозу конфіденційності, цілісності та доступності інформації.

3.3. Порядок здійснення контролю за станом ТЗІ

1. Відомчий контроль стану ТЗІ в Установах здійснюється фахівцями підрозділу з питань телекомунікацій, інформаційних технологій та захисту інформації апарату ДСНС України. До перевірок можуть залучатися фахівці з питань ТЗІ Установ.

2. Контроль за дотриманням вимог нормативних-правових актів підрозділами, що призначені для виконання робіт з ТЗІ, здійснює підрозділ з питань телекомунікацій, інформаційних технологій та захисту інформації апарату ДСНС України під час проведення перевірок стану ТЗІ, а також шляхом аналізу звітних документів, розроблених підрозділом ТЗІ за результатами проведених робіт і направлених за вказівкою до апарату ДСНС України.

3. Терміни проведення перевірок стану ТЗІ в Установах визначаються планом роботи ДСНС України на відповідний рік. Пропозиції щодо проведення таких перевірок та термінів їх проведення надаються підрозділом з питань телекомунікацій, інформаційних технологій та захисту інформації апарату ДСНС України, виходячи із загального стану ТЗІ в Установах (у тому числі за результатами звітів про стан ТЗІ, результатів попередніх перевірок, повноти виконання рекомендацій та усунення недоліків).

4. Перевірки проводяться відповідно до приписів, що підписуються Головою ДСНС України або одним із його заступників та завіряються гербовою печаткою.

5. За результатами перевірки складається звітний документ (акт, довідка), в якому відображаються стан технічного захисту інформації, виявлені в ході перевірки недоліки, даються рекомендації щодо їх усунення.

Ознайомлення керівника Установи, в якій проводилася перевірка, зі звітним документом про перевірку стану ТЗІ здійснюється під розпис.

Звітний документ про перевірку стану технічного захисту інформації складається у двох примірниках. Один примірник залишається в Установі, що перевірялася, другий примірник надсилається до апарату ДСНС України.

Доповідь про заходи, вжиті відповідно до наданих рекомендацій. та усунення виявлених у ході перевірки недоліків, має подаватися відповідно до термінів, зазначених у звітному документі про перевірку стану ТЗІ.

6. У разі виявлення порушення, внаслідок якого створюється реальна загроза або передумови до порушення конфіденційності, зокрема, за рахунок витоку (просочення) технічними каналами та (або) цілісності й доступності інформації, вимога щодо захисту якої встановлена законом, вживаються такі заходи:

- особи, які перевіряють, негайно доповідають керівнику Установи, що перевіряється, про порушення для прийняття рішення про припинення інформаційної діяльності на відповідних об'єктах;

- призначається службове розслідування щодо відповідальних осіб;

- про факт порушення та заходи, вжиті з метою його усунення, повідомляють керівництву ДСНС України відповідно до розподілу обов'язків;

- інші заходи, передбачені чинним законодавством.

Дозвіл на відновлення інформаційної діяльності на відповідних об'єктах дає керівник Установи, після усунення порушень, перевірки достатності і ефективності вжитих заходів ТЗІ.

7. Керівник Установи, що перевірялася, зобов'язаний вжити невідкладних заходів щодо усунення виявлених порушень.

8. У структурних підрозділах апарату ДСНС України та Установи організовується внутрішній контроль за дотриманням вимог нормативно-правових та відомчих документів з питань технічного захисту інформації.

Контроль здійснюється фахівцями підрозділу з питань телекомунікацій, інформаційних технологій та захисту інформації відповідно до плану, затвердженого головою комісії з питань ТЗІ.

Доповідь голові комісії з питань ТЗІ про результати перевірок здійснюється письмово.

9. У разі порушення вимог щодо забезпечення технічного захисту інформації посадові особи несуть відповідальність згідно з чинним законодавством України.

Вимоги щодо документації на Системи

Питання № 2 Захист інформації в телекомунікаційних, інформаційних та інформаційно-телекомунікаційних системах органів та підрозділів цивільного захисту.

У разі впровадження Систем в установі мають бути розроблені та затверджені такі документи:

- положення про Систему;
- порядок оброблення інформації в Системі;
- схеми фізичного розташування обладнання, електроживлення
- серверного та комутаційного обладнання, комутаційних з'єднань
- усієї мережі та логічної взаємодії сервісів і служб у мережі;
- план захисту інформації в Системі;
- регламент функціонування Системи.

Регламент функціонування Системи включає такі правила:

- роботи в Системі (інструкції користувачів та адміністраторів);
- доступу до інформаційної інфраструктури установи;
- роботи з електронним документообігом, внутрішнім порталом,
- корпоративною поштою (поштовим сервером);
- ідентифікації користувачів у мережі та їх авторизованого доступу
- (монітор стану).

Також до регламенту входять політики безпеки (інформаційна, мережева, адміністративна), що визначають розмежування прав доступу користувачів до внутрішньої мережі та внутрішньої інфраструктури установи відповідно до їх повноважень (адміністратор, модератор, авторизований користувач тощо), а також порядок резервного копіювання інформації.

5.3. У політиці безпеки Системи мають бути розглянуті такі

- проблеми, як віддалений доступ, перелік критичних ресурсів,
- керування та конфігурація IP-адрес, безпека засобів
- телекомунікацій, процедура виявлення вторгнення у мережу.

VI. Вимоги щодо захисту інформації у Системах

6.1. Для забезпечення захисту інформації у Системах виконується

- комплекс організаційно-технічних заходів зі створення та
- впровадження комплексної системи захисту інформації з
- підтвердженою Державною службою спеціального зв'язку та
- захисту інформації України відповідністю вимогам нормативноправових документів технічного захисту інформації.

Захисту в Системах підлягає така інформація:

- відкрита інформація, яка відноситься до державних інформаційних
- ресурсів;
- інформація з обмеженим доступом, яка поділяється на
- конфіденційну, службову та секретну інформацію;
- технологічна інформація.

Для забезпечення функціонування комплексної системи

- захисту інформації у Системах призначаються посадові особи,
- відповідальні за експлуатацію, захист інформації, технічне
- обслуговування та модернізацію.

Організація обліку Систем

На всі інформаційні ресурси в установі має вестись

інформаційна картка за формою, що додається. За щорічне оновлення і зберігання інформаційних карток на Системи в установі відповідає Служба технічної підтримки.

Інформаційні картки мають бути в **актуальному стані і**

зберігатися в електронній формі.

4. Закріплення вивченого матеріалу - 10 хв.

Питання для закріплення:

1) Яке програмне забезпечення у системі ДСНС є пріоритетним ?