

ПЛАН-КОНСПЕКТ

для проведення заняття в системі службової підготовки із середнім та старшим начальницьким складом (3 група) Вищого професійного училища Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Вид підготовки: профільна підготовка

Тема: №10 «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 корпоративна культура та методами формування сприятливого психологічного клімату в колективі.

Час проведення: 2 год.

Місце проведення: Народознавча світлиця.

Навчально-матеріальне забезпечення: план-конспект.

Нормативно-правові акти та література:

1. Наказ ДСНС України від 11.12.2013 року № 755 «Про затвердження Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій».

Порядок проведення заняття:

1. Організаційні заходи - 10 хв.: перевірка присутніх; оголошення теми і мети заняття.
2. Викладення матеріалу теми - 60 хв.

№ п/п	Навчальні питання та їх зміст	Методичні вказівки
1	2	3
1	<p>Організація діяльності щодо технічного захисту інформації в ДСНС України регулюється Конституцією України, законами України, актами Президента України та Кабінету Міністрів України, нормативними та відомчими розпорядчими документами з питань ТЗІ, а також Положенням про технічний захист інформації у Державній службі України з надзвичайних ситуацій.</p> <p>Організація технічного захисту інформації та відповідальність за його стан в апараті ДСНС України та Установах покладається на керівників.</p> <p>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.</p> <p>Організаційно-технічні принципи, порядок здійснення заходів щодо технічного захисту інформації, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з ТЗІ визначаються нормативно-правовими актами з питань ТЗІ. Дія Положення не поширюється на системи і засоби, що базуються на криптографічних методах захисту інформації. Організація заходів протидії технічним розвідкам у ДСНС України регламентується нормативними документами Держспецзв'язку України.</p> <p>Техніко-економічне обґрунтування, проектування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення</p>	<p>Оголосити питання Розповісти Дати під запис</p>

інформаційно-телекомунікаційних систем, зразків спеціальної техніки, критичних і небезпечних технологій виконуються за технічними завданнями, до яких обов'язково повинні включатися вимоги з технічного захисту інформації, якщо під час виконання передбачених завданням робіт та у процесі функціонування зазначених об'єктів, систем, зразків і технологій циркулюватиме інформація, що підлягає захисту.

Відповідно до Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р., під час розроблення і впровадження заходів з технічного захисту інформації використовуються засоби, дозволені Держспецзв'язку України для застосування та включені до відповідних переліків.

Система технічного захисту інформації

Склад системи технічного захисту 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 апарату ДСНС України, Установи (далі - комісія з питань ТЗІ) призначається наказом керівника; очолює комісію з питань ТЗІ один із заступників керівника.

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.

Комісія з питань ТЗІ у своїй діяльності керується вимогами чинних нормативно-правових актів, нормативно-методичних та відомчих документів з питань ТЗІ.

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.

Підрозділ з питань телекомунікацій, інформаційних технологій та захисту інформації апарату ДСНС України.

Головне завдання підрозділу з питань телекомунікацій, інформаційних технологій та захисту інформації апарату ДСНС України за напрямком ТЗІ - методичне забезпечення та контроль впровадження в ДСНС України заходів технічного захисту інформації, вимога щодо захисту якої встановлена законом, а саме:

Розповіді

- розробка проектів відомчих організаційно-розпорядчих документів з питань ТЗІ;
- методичне забезпечення впровадження заходів ТЗІ в ДСНС України згідно з вимогами нормативно-правових актів з питань ТЗІ;
- організація впровадження заходів ТЗІ в апараті ДСНС України;
- координація діяльності підрозділів ТЗІ в ДСНС України;
- здійснення відомчого контролю за станом технічного захисту інформації в ДСНС України та внутрішнього контролю в апараті ДСНС України;
- участь у розслідуванні порушень вимог законодавства у сфері ТЗІ та підготовка пропозицій щодо попередження в майбутньому подібних випадків;
- аналіз виконання вимог нормативно-правових актів з питань технічного захисту інформації в ДСНС України та підготовка пропозицій керівництву щодо удосконалення стану ТЗІ;
- організація підготовки та підвищення кваліфікації спеціалістів технічного захисту інформації в ДСНС України;
- організація взаємодії з Держспецзв'язку України та підрозділами захисту інформації інших органів державної влади України з питань ТЗІ.

Підрозділ з питань телекомунікацій, інформаційних технологій та захисту інформації Установи.

Головне завдання підрозділу з питань телекомунікацій, інформаційних технологій та захисту інформації Установи за напрямком ТЗІ - організація та контроль впровадження в Установі та у підпорядкованих Установі підрозділах заходів технічного захисту інформації, вимога щодо захисту якої встановлена законом, а саме:

- аналіз функціонування ОІД, інформаційно-телекомунікаційних систем з метою визначення загроз інформації і розробка заходів захисту інформації;
- розробка пропозицій для комісії з питань ТЗІ щодо шляхів реалізації вимог нормативно-правових актів з питань ТЗІ;
- організація та координація заходів щодо впровадження заходів технічного захисту інформації на ОІД та в ІТС Установи;
- організація діяльності служби захисту інформації в ІТС;
- розробка та доведення до особового складу розпорядчих документів, інструкцій, методичних посібників, з питань ТЗІ;
- здійснення внутрішнього контролю за виконанням вимог нормативно-правових та відомчих документів з питань ТЗІ;
- участь у розслідуванні порушень вимог законодавства у сфері ТЗІ та підготовка пропозицій щодо попередження в майбутньому подібних випадків.

У разі відсутності в Установі штатного підрозділу ТЗІ наказом керівника утворюється позаштатний підрозділ ТЗІ.

До складу позаштатного підрозділу ТЗІ обов'язково включаються представники підрозділів з питань телекомунікацій та інформаційних технологій, РСО, також можуть включатися представники інших підрозділів. Підрозділи технічного захисту інформації, що призначені для виконання робіт з ТЗІ.

Це підрозділи Установ, укомплектовані засобами вимірювальної техніки, спеціальною пошуковою апаратурою та обладнанням і призначені для проведення робіт з ТЗІ в ДСНС України.

Головними завданнями цих підрозділів є:

- впровадження та атестація комплексів ТЗІ на ОІД;

- впровадження комплексних систем захисту інформації з обмеженим доступом в ІТС;
- виявлення закладних пристроїв на ОІД.

Додаткові завдання, функції та права таких підрозділів визначаються положенням про ці підрозділи, погодженим з підрозділом з питань телекомунікацій, інформаційних технологій та захисту інформації апарату ДСНС України. Дозвіл таким підрозділам на проведення відповідних видів робіт з ТЗІ надається відповідно до чинного законодавства.

Служба захисту інформації в ІТС.

Головними завданнями Служби захисту інформації в ІТС (апарату ДСНС України; Установи) є:

- розроблення та удосконалення Плану захисту інформації в ІТС, впровадження заходів, спрямованих на його реалізацію;
- супровід створення, впровадження та функціонування комплексних систем захисту інформації (далі - КСЗІ), у частині захисту інформації від несанкціонованого доступу, на всіх етапах життєвого циклу ІТС, забезпечення належного функціонування КСЗІ у процесі роботи ІТС;
- підтримка необхідного рівня захищеності інформаційних ресурсів та технологій в ІТС;
- розроблення проектів розпорядчих документів, згідно з якими повинен забезпечуватися захист інформації в ІТС;
- участь у контролі виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів щодо: захисту інформації в ІТС, правил користування інформаційними ресурсами, порядку експлуатації обладнання ІТС.

У разі відсутності в Установі штатної служби захисту інформації в ІТС виконання її завдань покладається на підрозділ інформаційних технологій. Функції служби захисту інформації в ІТС апарату ДСНС України визначаються у положенні про відповідний підрозділ ДСНС України. Завдання режимно-секретних органів стосовно технічного захисту інформації визначено чинним законодавством.

Організація впровадження заходів ТЗІ

Роботи з технічного захисту інформації в ДСНС України проводяться підрозділами ТЗІ. Організація діяльності таких підрозділів регламентується окремим відомчим наказом. Проведення робіт (надання послуг) з технічного захисту інформації в ДСНС України сторонніми організаціями здійснюється відповідно до чинного законодавства.

Порядок здійснення контролю за станом ТЗІ

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.

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.

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

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.

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

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

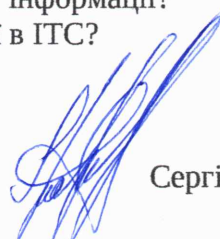
4. Закріплення вивченого матеріалу - 10 хв.

Питання для закріплення:

- 1) Чим регулюється організація діяльності щодо технічного захисту інформації в ДСНС України?
- 2) Хто є суб'єктами системи технічного захисту інформації?
- 3) Основні завдання служби захисту інформації в ІТС?

План-конспект склав:

Заступник начальника курсу
старший лейтенант служби цивільного захисту



Сергій ШАРГОРОДСЬКИЙ