**Заняття 4. Служба захисту інформації.**

**Вступ.**

**Питання 1. Правові та організаційні питання створення служби захисту інформації в автоматизованих системах.**

**Питання 2. Функціональні питання щодо захисту інформації.**

**Питання 3. Права, обов’язки, відповідальність, взаємодія.**

**Питання 4. Штатно-фінансові питання.**

**Вступ.**

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в АС» встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації (далі - СЗІ) - «Положення про СЗІ в ІТС».

Як правило, Положення складається з таких розділів:

* завдання і функції СЗІ;
* повноваження і відповідальність СЗІ;
* взаємодія СЗІ з іншими підрозділами організації та зовнішніми установами;
* штатний розклад і структура СЗІ;
* організація робіт СЗІ;
* фінансування СЗІ.

В залежності від конкретних завдань і умов функціонування СЗІ дозволяється, у разі необхідності, поєднувати окремі розділи в один, вводити нові розділи (підрозділи) або вилучати розділи, що не є актуальними.

До Положення у вигляді додатків можуть включатися нормативні документи, таблиці, схеми, графіки, необхідні для визначення заходів захисту інформації, плани об’єктів захисту з вказанням робочих місць та встановлених на них технічних засобів передачі, прийому, зберігання, обробки інформації, що підлягає захисту та ін. документи.

Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації. Положення затверджується наказом керівника організації або підрозділу, до якого структурно входить СЗІ.

**Питання 1.**

**Перший розділ.**

1. Положення є нормативним документом організації та визначає завдання, функції, штатну структуру СЗІ, повноваження та відповідальність співробітників служби, взаємодію з іншими підрозділами організації та зовнішніми організаціями.

2. СЗІ є штатним або позаштатним підрозділом організації. СЗІ є самостійним структурним підрозділом з безпосередньою підпорядкованістю керівнику організації або структурною одиницею іншого підрозділу (РСО, ТЗІ, служби безпеки) організації.

В організаціях, де штатним розкладом не передбачено створення СЗІ, заходи щодо забезпечення захисту інформації в ІТС здійснюють призначені наказом керівника організації окремі працівники. У цьому випадку посадові (функціональні) обов’язки цих працівників повинні включати положення, які б передбачали виконання ними вимог щодо діяльності СЗІ.

3. Метою створення СЗІ є організаційне забезпечення завдань керування КСЗІ в ІТС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в ІТС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в ІТС.

4. Правову основу для створення і діяльності СЗІ становлять Закон України «Про захист інформації в ІТС», «Правила забезпечення захисту інформації в ІТС», НД ТЗІ і накази Адміністрації Держспецзв’язку.

5. СЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, іншими нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, розпорядчими та іншими документами організації, а також цим Положенням.

СЗІ здійснює діяльність відповідно до «Плану захисту інформації в ІТС», календарних, перспективних та інших планів робіт, затверджених керівником організації.

6. Для проведення окремих заходів з захисту інформації в АС, які пов’язані з напрямком діяльності інших підрозділів організації, керівник організації своїм наказом визначає перелік, строки виконання та підрозділи для виконання цих робіт.

7. У своїй роботі СЗІ взаємодіє з підрозділами організації (РСО, ТЗІ, служби безпеки), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби, до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

# 

# Другий розділ: «Завдання СЗІ»

# захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;

* дослідження технології обробки інформації в ІТС з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;
* організація та координація робіт, пов’язаних з захистом інформації в ІТС, необхідність захисту якої визначається її власником або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;
* розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в ІТС;
* організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу ІТС;
* участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів ІТС з питань захисту інформації;
* формування у персоналу і користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

- організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в ІТС та проведення контрольних перевірок їх виконання.

# Питання 2.

# Третій розділ: «Функції СЗІ».

# Складається з 3-х таких підрозділів:

## - створення КСЗІ;

## - експлуатація КСЗІ;

## - організація навчання персоналу з питань забезпечення захисту інформації.

## 3.1. Функції під час створення КСЗІ:

* визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об’єктів захисту в ІТС, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в ІТС;
* розробка та коригування моделі порушника безпеки інформації та моделі загроз для інформації, політики безпеки інформації та плану захисту інформації в ІТС;
* визначення і формування вимог до КСЗІ, організація і координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах з створення КСЗІ;
* підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;
* організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;
* вибір організацій-виконавців робіт з створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з підрозділом ТЗІ (РСО, службою безпеки) погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт тощо);
* участь у розробці нормативних документів, чинних у межах організації і ІТС, які встановлюють дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;
* участь у розробці нормативних документів, чинних у межах організації і ІТС, які встановлюють правила доступу користувачів до ресурсів ІТС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій тощо).

## 3.2. Функції під час експлуатації КСЗІ:

* організація процесу керування КСЗІ;
* розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;
* вжиття заходів у разі виявлення спроб НСД до ресурсів ІТС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;
* забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;
* організація керування доступом до ресурсів ІТС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів тощо);
* супроводження та актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);
* спостереження (реєстрація та аудит подій в ІТС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;
* підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в АС, впровадження нових технологій захисту і модернізації КСЗІ;
* організація та проведення заходів з тестування, оперативного відновлення функціонування та модернізації КСЗІ після збоїв, відмов, аварій ІТС або КСЗІ;
* участь в роботах з модернізації ІТС - узгодженні пропозицій з введення до складу ІТС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;
* забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;
* проведення аналітичної оцінки поточного стану безпеки інформації в ІТС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз тощо);
* інформування власників інформації про технічні можливості захисту інформації в ІТС і типові правила, встановлені для персоналу і користувачів ІТС;
* негайне втручання в процес роботи ІТС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;
* регулярне подання звітів керівництву організації-власника (розпорядника) ІТС про виконання користувачами ІТС вимог з захисту інформації;
* аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обгрунтування пропозицій щодо придбання засобів для організації;
* контроль за виконанням персоналом і користувачами ІТС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за забезпеченням режиму секретності у разі обробки в ІТС інформації, що становить державну таємницю;
* контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;
* розробка і реалізація спільно з РСО (підрозділом ТЗІ, службою безпеки) організації комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів тощо, здійснення їхнього технічного та інформаційного забезпечення.

## 3.3. Функції з організації навчання персоналу з питань забезпечення захисту інформації:

* розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ІТС;
* розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в організації (ІТС), необхідний рівень її захищеності тощо;
* участь в організації і проведенні навчання користувачів і персоналу ІТС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;
* взаємодія з державними органами, учбовими закладами, іншими організаціями з питань навчання та підвищення кваліфікації;
* участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою тощо.

**Питання 3.**

# 4-й розділ «Повноваження та відповідальність СЗІ».

## 4.1. СЗІ має право:

- здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (ІТС) щодо виконання ним вимог нормативно-правових актів і нормативних документів з захисту інформації;

* подавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;
* складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;
* проводити службові розслідування у випадках виявлення порушень;
* отримувати доступ до робіт та документів структурних підрозділів організації (ІТС), необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;
* готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій;
* готувати пропозиції щодо забезпечення ІТС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;
* виходити до керівництва організації з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;
* узгоджувати умови включення до складу ІТС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів АС;
* надавати висновки з питань, що належать до компетенції СЗІ, які необхідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проектів, що потребують технічної підтримки з боку співробітників СЗІ;
* виходити до керівництва організації з пропозиціями щодо узгодження планів і регламенту відвідування ІТС сторонніми особами;
* інші права, які надані СЗІ у відповідності з специфікою та особливостями діяльності організації (ІТС).

## 4.2. СЗІ зобов’язана:

* організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в ІТС;
* вчасно і в повному обсязі доводити до користувачів і персоналу ІТС інформацію про зміни в галузі захисту інформації, які їх стосуються;
* перевіряти відповідність прийнятих в ІТС (організації) правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;
* здійснювати контрольні перевірки стану захищеності інформації в ІТС;
* забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в ІТС (організації);
* сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в ІТС;
* сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої організацією на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів та приватних осіб;
* періодично, не рідше одного разу на місяць, подавати керівництву організації звіт про стан захищеності інформації в ІТС і дотримання користувачами та персоналом АС встановленого порядку і правил захисту інформації;
* негайно повідомляти керівництво ІТС (організації) про виявлені атаки та викритих порушників;
* інші обов’язки, покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності ІТС (організації).

## 4.3. Відповідальність

1. Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов’язків, допущені ними порушення встановленого порядку захисту інформації в ІТС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників СЗІ визначається посадовими або функціональними інструкціями.

2. Відповідальність за діяльність СЗІ покладається на її керівника, який відповідає за:

* організацію робіт з захисту інформації в ІТС, ефективність захисту інформації відповідно до діючих нормативно-правових актів;
* своєчасне розроблення і виконання «Плану захисту інформації в ІТС»;
* якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених керівником організації;
* координацію планів діяльності підрозділів та служб ІТС (організації) з питань захисту інформації;
* створення системи навчання співробітників, користувачів, персоналу ІТС з питань захисту інформації;
* виконання особисто та співробітниками СЗІ розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

3. Співробітники СЗІ відповідають за:

* додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;
* повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в ІТС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції СЗІ;
* дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в ІТС, які включені до плану робіт СЗІ;
* якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;
* інші питання персональної відповідальності, які покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності ІТС (організації).

# У 5-му розділі «Взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми організаціями» викладаються такі питання:

1. СЗІ здійснює свою діяльність у взаємодії з науковими, виробничими та іншими організаціями, державними органами та установами, що займаються питаннями захисту інформації.

2. Заходи щодо захисту інформації в ІТС повинні бути узгоджені СЗІ з заходами охоронної та режимно-секретної діяльності інших підрозділів організації.

СЗІ взаємодіє, узгоджує свою діяльність та встановлює зв’язки з:

* внутрішніми підрозділами організації - службою безпеки; РСО; підрозділом ТЗІ; підрозділом інформаційних технологій та іншими підрозділами, виробнича діяльність яких пов’язана з захистом інформації або її автоматизованою обробкою;
* зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;
* іншими суб’єктами діяльності у сфері захисту інформації.

3. СЗІ координує свою діяльність з регіональним органом Держспецзв’язку під час проведення перевірок стану ТЗІ.

4. Взаємодію з іншими підрозділами організації з питань, що безпосередньо не пов’язані з захистом інформації, СЗІ здійснює у відповідності з наказами керівника організації.

**Питання 4.**

# У 6-му розділі «Штатний розклад та структура СЗІ» викладаються такі питання:

1. СЗІ є штатним або позаштатним підрозділом організації, безпосередньо підпорядкованим керівнику організації або його заступнику, що відповідає за забезпечення безпеки інформації. Або СЗІ є структурною (штатною або позаштатною) одиницею підрозділу ТЗІ (РСО або служби безпеки) організації.

2. Структура СЗІ, її склад і чисельність визначається фактичними потребами ІТС для виконання вимог політики безпеки інформації та затверджується керівництвом організації. Чисельність і склад СЗІ мають бути достатніми для виконання усіх завдань щодо захисту інформації в ІТС.

3. З метою ефективного функціонування та керування захистом інформації в ІТС СЗІ має штатний розклад, який включає перелік функціональних обов’язків усіх співробітників, необхідних вимог до рівня їхніх знань та навичок.

4. Безпосереднє керівництво роботою СЗІ здійснює її керівник. У випадку, коли СЗІ є структурною одиницею підрозділу ТЗІ (РСО або служби безпеки) – керівник цього підрозділу. Призначення та звільнення з посади керівника СЗІ здійснюється керівництвом організації за узгодженням з особами, що відповідають за забезпечення безпеки інформації.

На час відсутності керівника СЗІ (у зв’язку з відпусткою, службовим відрядженням, хворобою тощо) його обов’язки тимчасово виконує заступник керівника СЗІ, а у разі відсутності такої посади – найбільш кваліфікований співробітник СЗІ або керівник підрозділу ТЗІ (РСО або служби безпеки). Призначення на цю посаду позаштатних або тимчасово працюючих співробітників забороняється.

5. Штат СЗІ комплектується спеціалістами, які мають спеціальну технічну освіту або спеціальні курси підвищення кваліфікації у галузі ТЗІ та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації, а також реалізації організаційних, технічних та інших заходів з захисту інформації, знаннями і вмінням застосовувати нормативно-правові документи у сфері захисту інформації.

6. Функціональні обов’язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом ІТС (організації).

7. За посадами співробітники СЗІ поділяються на такі категорії (за рівнем ієрархії):

* керівник СЗІ;
* адміністратори (системи, мережі, безпеки, КСЗІ);
* спеціалісти різного фаху.

8. В залежності від обсягів і особливостей завдань СЗІ до її складу можуть входити спеціалісти різного фаху з таких питань:

* захисту інформації від витоку технічними каналами;
* захисту каналів зв’язку і комутаційного обладнання;
* налагодження і керування активним мережевим обладнанням;
* керування базами даних захисту;
* захищених технологій обробки інформації.

9. Зміна структури СЗІ здійснюється за рішенням керівництва організації та затверджується наказом керівника організації.

# У 7-му розділі «Організація роботи СЗІ» викладаються такі питання:

1. Трудові відносини в СЗІ будуються на основі законодавства України з урахуванням положень статуту організації, правил внутрішнього трудового розпорядку та встановлених в організації норм техніки безпеки праці, гігієни і санітарії, інших розпорядчих документів організації.

2. СЗІ здійснює реалізацію основних організаційних та організаційно-технічних заходів щодо створення та забезпечення функціонування КСЗІ у відповідності з планами робіт. Підставою для розроблення планів робіт є «План захисту інформації в ІТС».

До планів включаться такі основні заходи:

* разові (які виконуються за умови перегляду прийнятих рішень з захисту інформації або виникнення певних змін в ІТС чи зовнішньому середовищі);
* періодичні (які виконуються з заданим інтервалом часу);
* постійні (які виконуються безперервно або дискретно у випадковий чи заданий час).

Основними видами планів робіт СЗІ можуть бути:

* календарний план робіт (щодо реалізації заходів з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ та інших питань);
* план заходів з оперативного реагування на непередбачені ситуації (в тому числі надзвичайні та аварійні) та поновлення функціонування ІТС;
* поточний план робіт (на місяць, квартал, рік);
* перспективний план розвитку та удосконалення діяльності СЗІ з питань захисту інформації (до 5 років);
* план заходів з забезпечення безпеки інформації під час виконання окремих важливих робіт, при проведенні нарад, укладенні договорів, угод тощо.

Плани робіт складаються керівником СЗІ після обговорення на виробничій нараді СЗІ організаційно-технічних питань, що належать до її компетенції, і затверджуються керівником організації або керівником підрозділу, до складу якого входить СЗІ.

3. Реорганізація або ліквідація СЗІ здійснюється за рішенням керівництва організації. Реорганізаційна або ліквідаційна процедура здійснюється відповідною комісією, яка створюється за наказом керівника організації.

4. З метою забезпечення конфіденційності робіт, які виконуються співробітниками СЗІ, при прийомі на роботу (звільненні з роботи) вони дають письмові зобов’язання щодо нерозголошення відомостей, що становлять службову, комерційну або іншу таємницю, і які стали їм відомими в період роботи в організації.

5. Матеріально-технічну базу для забезпечення діяльності СЗІ складають належні їй на правах власності (оперативного управління, повного господарського відання) засоби захисту інформації, ПЗ, технічне і інженерне обладнання, засоби вимірювань і контролю, відповідна документація, а також інші засоби і обладнання, які необхідні для виконання СЗІ покладених на неї завдань.

Співробітники СЗІ відповідають за збереження майна, що є власністю або знаходиться у розпорядженні служби.

Засоби захисту інформації та захищені засоби, що використовуються співробітниками СЗІ при виконанні своїх службових обов’язків, повинні мати, одержаний у встановленому порядку документ, що засвідчує їхню відповідність вимогам НД ТЗІ.

Матеріально–технічне та інше спеціальне забезпечення СЗІ здійснюється відповідними підрозділами організації у встановленому порядку.

# У 8-му розділі «Фінансування СЗІ» вказується, що СЗІ фінансується за рахунок:

* коштів, що виділяються в організації на утримання органів управління;
* прибутку організації (ІТС) та інших коштів за рішенням керівництва організації або рішенням загальних зборів акціонерів;
* коштів, отриманих за виконання СЗІ договірних робіт та надання послуг;
* інших джерел фінансування, не заборонених законодавством.

**Контрольні питання**

Яку назву має НД ТЗІ, що визначає зміст і оформлення положення про СЗІ?

З яких розділів складається Положення про СЗІ в ІТС?

## З яких трьох частин складаються функції СЗІ?

## Які документи розробляє та коригує СЗІ під час створення КСЗІ?

Які заходи організовує та проводить СЗІ під час експлуатації КСЗІ після її збоїв?

## Про що СЗІ інформує власників інформації під час експлуатації КСЗІ?

## Які заходи організовує та проводить СЗІ у разі виявлення атаки на КСЗІ?

## Які права має СЗІ у випадках виявлення порушень?

## Яким документом визначається персональна відповідальність співробітника СЗІ?

## З якими внутрішніми підрозділами організації взаємодіє СЗІ?

## З яким органом координує свою діяльність СЗІ під час проведення перевірок стану ТЗІ?

На які категорії (за рівнем ієрархії) поділяються співробітники СЗІ за посадами?