

ЗАТВЕРДЖЕНО

Розпорядження голови
Дубенської районної
державної адміністрації –
начальника Дубенської районної
військової адміністрації
01.05.2025 № 57

ПОЛОЖЕННЯ

про службу захисту інформації в автоматизованій системі Дубенської районної державної адміністрації

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про службу захисту інформації в автоматизованій системі Дубенської районної державної адміністрації (далі – Положення) розроблене на підставі Типового положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000), затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 року № 53.

1.2. Положення є нормативним документом Дубенської районної державної адміністрації (далі – РДА) і визначає завдання, функції, штатну структуру служби захисту інформації (далі – СЗІ), повноваження та відповідальність співробітників служби, взаємодію з іншими підрозділами РДА та зовнішніми організаціями.

1.3. Зміни суттєвого характеру вносяться до Положення на основі розпорядження голови Дубенської районної державної адміністрації.

1.4. Метою створення СЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (далі – КСЗІ) автоматизованої системи (далі – АС) РДА та здійснення контролю за її функціонуванням. СЗІ є позаштатним підрозділом РДА.

1.5. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

1.6. Правову основу для створення і діяльності СЗІ становлять Закон

України «Про захист інформації в інформаційно-комунікаційних системах», Положення про технічний захист інформації в Україні, Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

1.7. 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 автоматизованій системі», календарних, перспективних та інших планів робіт, затверджених головою Дубенської районної державної адміністрації.

1.8. У своїй роботі СЗІ взаємодіє з підрозділами РДА, 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.

2. ГАЛУЗЬ ВИКОРИСТАННЯ

2.1. Положення призначене для використання службою захисту інформації Дубенської районної державної адміністрації. Вимоги цього документу є обов'язковими до виконання під час створення та функціонування КСЗІ в АС РДА.

2.2. Використання Положення створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень СЗІ, а також організації її роботи із захисту інформації впродовж всього періоду функціонування АС РДА.

3. ВИЗНАЧЕННЯ, ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

СЗІ – служба захисту інформації;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ТЗІ – технічний захист інформації.

4. ЗАВДАННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

Завданнями СЗІ є:

- захист законних прав щодо безпеки інформації Дубенської районної державної адміністрації, структурних підрозділів, співробітників, користувачів в процесі інформаційної діяльності та взаємодії між собою;
- дослідження технології обробки інформації в АС 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 АС, необхідність захисту якої визначається чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій, розроблення проектів нормативних і розпорядчих документів, чинних у межах РДА, згідно з якими повинен забезпечуватися захист інформації в АС;
- організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу АС;
- участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів АС 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 АС та проведення контрольних перевірок їх виконання.

5. ФУНКЦІ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

5.1. Функції під час створення КСЗІ:

- визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в АС, класифікація інформації за вимогами до її конфіденційності або важливості для РДА, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в АС; – розроблення та коригування моделі загроз і моделі захисту інформації в АС, політики безпеки інформації в АС;
- 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, 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 розробленні нормативних документів, чинних у межах РДА і АС, які встановлюють дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;
- участь у розробленні нормативних документів, чинних у межах РДА і АС, які встановлюють правила доступу користувачів до ресурсів АС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій тощо).

5.2. Функції під час експлуатації комплексної системи захисту інформації:

- 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 АС, 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 АС (розподілення між користувачами необхідних реквізитів захисту інформації – ідентифікаторів, паролів, привілеїв, ключів тощо);
- спостереження (реєстрація і аудит подій в АС, 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 модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій АС або КСЗІ;

- участь у роботах з модернізації АС – узгодженні пропозицій з введення до складу АС нових компонентів, нових функціональних завдань і режимів опрацювання інформації, заміни засобів обробки інформації тощо;
- забезпечення супроводження й актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;
- проведення аналітичного оцінювання поточного стану безпеки інформації в АС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації й реалізованої політики безпеки поточній моделі загроз та ін.);
- інформування володільців інформації про технічні можливості захисту інформації в АС і типові правила, встановлені для персоналу і користувачів АС;
- негайне втручання в процес роботи АС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;
- інформування керівництва РДА про виконання користувачами АС вимог із захисту інформації; – аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання цих засобів;
- контроль за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації;
- контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту; – розроблення й реалізація 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 та ін., здійснення їхнього технічного та інформаційного забезпечення.

5.3. Функції з організації навчання персоналу з питань забезпечення захисту інформації:

- розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу АС;
- розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в АС, необхідний рівень її захищеності та ін.; – участь в організації і проведенні навчання користувачів і персоналу АС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;
- взаємодія з державними органами, навчальними 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 та ін.

6. ПОВНОВАЖЕННЯ ТА ВІДПОВІДАЛЬНІСТЬ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

6.1. Права.

СЗІ має право:

- здійснювати у встановленому порядку контроль за діяльністю будь-якого структурного підрозділу РДА щодо виконання ним вимог нормативно-правових актів і нормативних документів із захисту інформації;
- подавати керівництву РДА 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 РДА акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;
- брати участь у службових розслідуваннях у випадках виявлення порушень;
- отримувати доступ до робіт та документів структурних підрозділів РДА, необхідних для оцінювання вжитих заходів із захисту інформації в АС та підготовки пропозицій щодо їхнього подальшого удосконалення;
- готувати пропозиції щодо залучення на договірній основі до виконання робіт із захисту інформації інших організацій;
- готувати пропозиції щодо забезпечення АС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;
- надавати керівництву РДА пропозиції щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;
- узгоджувати умови включення до складу АС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийнятну політику безпеки або рівень захищеності ресурсів АС;
- надавати висновки з питань, що належать до компетенції СЗІ, які необхідні для здійснення діяльності РДА;
- інші права, які надані СЗІ у відповідності зі специфікою та особливостями діяльності РДА.

6.2. Обов'язки.

СЗІ зобов'язана:

- організувати забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації в АС;
- вчасно і в повному обсязі доводити до користувачів і персоналу АС інформацію про зміни в галузі захисту інформації, які їх стосуються;
- перевіряти відповідність прийнятих в АС правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;
- здійснювати контрольні перевірки стану захищеності інформації в АС;
- забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в АС РДА;
- сприяти, і у разі необхідності, брати безпосередню участь у проведенні відповідними службами перевірок стану захищеності інформації в АС;
- сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої РДА на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів та приватних осіб;
- негайно повідомляти керівництву РДА про виявлені атаки та викритих порушників;
- інші обов'язки, покладені на керівника та співробітників СЗІ у відповідності зі специфікою та особливостями діяльності АС РДА.

6.3. Відповідальність.

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

Персональна відповідальність керівника та співробітників СЗІ визначається їх посадовими (функціональними) інструкціями.

6.3.2. Відповідальність за діяльність СЗІ покладається на її керівника.

Керівник СЗІ відповідає за:

- організацію робіт з захисту інформації в АС, ефективність захисту інформації відповідно до діючих нормативно-правових актів;
- своєчасне розроблення і виконання «Плану захисту інформації в автоматизованій системі»;

- якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених головою РДА;
- координацію планів діяльності підрозділів та служб РДА з питань захисту інформації;
- створення системи навчання співробітників, користувачів, персоналу АС з питань захисту інформації;
- виконання особисто та співробітниками СЗІ розпоряджень керівництва РДА, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

6.3.3. 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 АС, 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 АС, 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 РДА.

7. ВЗАЄМОДІЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ З ІНШИМИ ПІДРОЗДІЛАМИ РДА ТА ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ

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

7.2. Заходи з захисту інформації в АС повинні бути узгоджені СЗІ із заходами охоронної діяльності РДА.

7.3. СЗІ взаємодіє, узгоджує свою діяльність та встановлює зв'язки з:

- іншими підрозділами РДА, діяльність яких пов'язана із захистом інформації або її автоматизованою обробкою;

- зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;
- іншими суб'єктами діяльності у сфері захисту інформації.

7.4. Взаємодію з іншими підрозділами РДА з питань, що безпосередньо не пов'язані з захистом інформації, СЗІ здійснює у відповідності з наказами та (або) розпорядженнями керівництва РДА.

8. СКЛАД ТА СТРУКТУРА СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

8.1. Структура СЗІ, її склад і чисельність визначається фактичними потребами АС для виконання вимог політики безпеки інформації та затверджується встановленим порядком головою РДА. Чисельність і склад СЗІ мають бути достатніми для виконання усіх завдань з захисту інформації в АС.

8.2. Функціональні обов'язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом РДА.

8.3. Безпосередню організацію роботи СЗІ здійснює її керівник. Призначення чи звільнення з посади керівника СЗІ здійснюється головою РДА.

8.4. На час відсутності керівника СЗІ (у зв'язку з відпусткою, службовим відрядженням, хворобою тощо) його обов'язки тимчасово виконує його заступник, або інший кваліфікований співробітник СЗІ.

8.5. Штат СЗІ комплектується спеціалістами, які мають спеціальну технічну освіту (вищу, середню спеціальну, спеціальні курси підвищення кваліфікації у галузі ТЗІ тощо) 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.

8.6. За посадами співробітники СЗІ поділяються на такі категорії (за рівнем ієрархії): – керівник СЗІ;

- адміністратори захисту АРМ (безпеки баз даних, безпеки системи);
- спеціалісти служби захисту.

8.7. Зміна складу СЗІ здійснюється за рішенням керівництва РДА і затверджується наказом голови РДА.

9. ОРГАНІЗАЦІЯ РОБІТ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

9.1. СЗІ здійснює свою роботу з реалізації основних організаційних та організаційно-технічних заходів зі створення та забезпечення функціонування

КСЗІ у відповідності з планами робіт. Підставою для розроблення планів робіт є «План захисту інформації в АС».

9.2. До планів включається наступні основні заходи:

- разові (одноразово виконувані, необхідність у повторенні яких виникає за умови повного перегляду прийнятих рішень з захисту інформації);
- постійно виконувані (заходи, що потребують виконання неперервно або дискретно у випадковий чи заданий час);
- періодично виконувані (з заданим інтервалом часу);
- виконувані за необхідності (заходи, що потребують виконання під час здійснення або виникнення певних змін в АС чи зовнішньому середовищі).

9.3. Основними видами планів робіт СЗІ є:

- 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 АС.

9.4. Плани робіт складаються керівником СЗІ після обговорення на виробничій нараді СЗІ організаційно-технічних питань, що належать до її компетенції, і затверджуються головою РДА.

9.5 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.

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

9.7. 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 нормативних документів. Матеріально-технічне та інше спеціальне забезпечення СЗІ здійснюється відповідними підрозділами РДА у встановленому порядку.