СУМСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ

ДЕРЖАВНИЙ АРХІВ СУМСЬКОЇ ОБЛАСТІ

НАКАЗ

23.06.2021 Суми **№ 25-ОД**

Про затвердження Положення про відповідального за технічний захист інформації в інформаційно-телекомунікаційній системі Державного архіву Сумської області

Відповідно до законів України «Про місцеві державні адміністрації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», нормативного документу системи технічного захисту інформації 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53, з метою організації та проведення робіт із захисту інформації в автоматизованій системі Державного архіву Сумської області:

НАКАЗУЮ:

1. Затвердити Положення про відповідального за технічний захист інформації в інформаційно-телекомунікаційній системі Державного архіву Сумської області (додається).
2. Контроль за виконанням цього наказу покласти на директора Державного архіву Сумської області Олійника Юрія Олександровича.

Заступник директора –
начальник відділу **Інна НАЗАРЕНКО**

ЗАТВЕРДЖЕНО
Наказ Державного архіву
Сумської області
23.06.2021 № 25-ОД

ПОЛОЖЕННЯ
про відповідального за технічний захист інформації в інформаційно-телекомунікаційній системі Державного архіву Сумської області

1. Терміни, визначення та скорочення

У цьому Положенні використовуються терміни і визначення:

ІТС – інформаційно-телекомунікаційна система;

ІТ АС 3 – інформаційно-телекомунікаційна автоматизована система Державного архіву Сумської області класу «3»;

І АС 1 – інформаційна автоматизована система Державного архіву Сумської області класу «1»;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

РСО – режимно-секретний орган Державного архіву Сумської області;

ТЗІ – технічний захист інформації.

Інші терміни, визначення та скорочення використовуються відповідно до НД ТЗІ 1.1-003-99.

2. Галузь використання

1. Положення про відповідального за технічний захист інформації в інформаційно-телекомунікаційній системі Державного архіву Сумської області (далі – Положення) регламентує діяльність відповідального за ТЗІ в ІТС Держархіву області.

2. Вимоги Положення є обов’язковими для відповідального за ТЗІ та окремих співробітників, які здійснюють діяльність, пов’язану зі створенням КСЗІ та підтримкою визначеного режиму роботи з інформацією, що циркулює і обробляється в ІТС.

3. Нормативні документи, якими врегульована діяльність відповідального за ТЗІ

1. Відповідальний за ТЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, розпорядчими та іншими документами Сумської обласної державної адміністрації, цим Положенням, а також нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, зокрема:

Законом України «Про інформацію»;

Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»;

Законом України «Про державну таємницю»;

Концепцією технічного захисту інформації в Україні, затвердженою постановою Кабінету Міністрів України від 08 жовтня 1997 р. № 1126;

Положенням про технічний захист інформації в Україні, затвердженим Указом Президента України від 27 вересня 1999 р. № 1229;

Положенням про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах, затвердженим постановою Кабінету Міністрів України від 16 лютого 1998 р. № 180;

Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженими постановою Кабінету Міністрів України від 26 березня 2006 р. № 373;

НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22 (із змінами);

НД ТЗІ 1.1-003-99 «Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22;

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22 (із змінами);

НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу», затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22 (із змінами);

НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі», затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22;

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», затвердженими наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53.

4. Загальні положення

1. Це Положення є нормативним документом з ТЗІ і визначає завдання, функції, повноваження та відповідальність особи, відповідальної за ТЗІ, взаємодію зі структурними підрозділами Держархіву області та зовнішніми організаціями.

2. Відповідальний за ТЗІ призначається наказом директора Державного архіву Сумської області.

3. Для цілей виконання цього Положення ІТС Держархіву області за режимом доступу складається з:

І АС 1 – інформаційна автоматизована система класу «1», яка призначена для обробки таємної інформації та інформації для службового користування;

ІТ АС 3 – інформаційно-телекомунікаційна автоматизована система класу «3», яка призначена для обробки відкритої, конфіденціальної інформації та державних інформаційних ресурсів, які не містять таємної інформації. ІТ АС 3 включає усі інформаційні та інформаційно-телекомунікаційні системи Державного архіву Сумської області (системи документообігу, обробки звернень громадян, консолідації звітності тощо).

4. У своїй роботі відповідальний за ТЗІ взаємодіє 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.

5. Відповідальний за ТЗІ здійснює координацію діяльності із захисту інформації в Державному архіві Сумської області, надає нормативну та методологічну допомогу працівникам, на яких покладено функції захисту інформації.

5. Мета та завдання відповідального за ТЗІ

1. Метою ТЗІ є організаційне забезпечення виконання завдань керування КСЗІ ІТС Держархіву області та здійснення контролю за її функціонуванням. На відповідальну особу за ТЗІ покладається: виконання робіт з визначення вимог із захисту інформації в ІТС, участь у проектуванні та розробленні, експлуатації, обслуговуванні, підтримка працездатності, проведення модернізацій КСЗІ ІТС Держархіву, а також контроль за станом захищеності інформації в ІТС.

2. Відповідальна особа за ТЗІ несе відповідальність за організацію заходів з захисту інформації на робочих станціях ІТС Держархіву. Зміст інформації, що

міститься на робочих станціях повинен відповідати рівню захисту інформації за режимом доступу. За розміщення інформації з обмеженим доступом в ІТС, яка не відповідає рівню захисту за режимом доступу несе особа, яка розмістила інформацію.

3. Відповідальний за ТЗІ надає структурним підрозділам Держархіву методологічну допомогу з питань організації захисту інформації в інформаційно-телекомунікаційних системах, що входять до ІТС Держархіву.

4. Завданнями відповідального за ТЗІ є:

1) захист інформації, що циркулює в ІТС Держархіву у процесі інформаційної діяльності та взаємодії із зовнішніми організаціями;

2) дослідження технології обробки інформації в ІТС Держархіву 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;

3) організація та координація робіт, пов’язаних із захистом інформації в ІТС Держархіву, підтримка необхідного рівня захищеності інформації, ресурсів і технологій, зокрема, робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу ІТС Держархіву;

4) розроблення нормативних і розпорядчих документів, чинних у межах ІТС Держархіву, згідно з якими повинен забезпечуватися захист інформації в ІТС Держархіву, здійснення контролю за виконанням користувачами вимог таких нормативних і розпорядчих документів;

5) розроблення нормативних і розпорядчих документів, чинних у межах Державного архіву Сумської області, згідно з якими повинен забезпечуватися захист інформації в інформаційно-телекомунікаційних системах структурних підрозділів архіву;

6) участь в організації професійної підготовки і підвищенні кваліфікації користувачів ІТС Держархіву з питань захисту інформації;

7) формування у користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

8) організація забезпечення виконання користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації в ІТС Держархіву.

6. Функції відповідального за ТЗІ

1. Основною функцією відповідального за ТЗІ є створення та належна експлуатація КСЗІ.

2. Функції під час створення КСЗІ:

1) визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об’єктів захисту в ІТС Держархіву, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розповсюдження інформації в ІТС Держархіву;

2) розробка та коригування моделі загроз і моделі захисту інформації, політики безпеки інформації в ІТС Держархіву;

3) визначення і формування вимог до КСЗІ;

4) організація і координація робіт із проектування та розробки КСЗІ, безпосередня участь у проектних роботах зі створення КСЗІ;

5) підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

6) організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;

7) вибір організацій-виконавців робіт зі створення КСЗІ, здійснення контролю за дотриманням установленого порядку проведення робіт із захисту інформації у взаємодії з підрозділом РСО, погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма, методика випробувань, плани робіт);

8) участь у розробці нормативних документів, чинних у межах Державного архіву Сумської області, які встановлюють правила доступу користувачів до ресурсів ІТС, визначають порядок, норми, правила із захисту інформації та здійснення контролю за їх дотриманням.

3. До виконання функцій під час створення КСЗІ може бути залучено організацію-виконавця робіт, що має ліцензію на відповідний вид діяльності у сфері захисту інформації.

4. Функції під час експлуатації КСЗІ:

1) організація процесу керування КСЗІ;

2) розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;

3) ужиття заходів у разі виявлення спроб НСД до ресурсів ІТС Держархіву, порушення правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

4) забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

5) організація керування доступом до ресурсів ІТС Держархіву (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);

6) супроводження й актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);

7) спостереження (реєстрація й аудит подій у системі, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

8) підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ІТС Держархіву, упровадження нових технологій захисту і модернізації КСЗІ;

9) організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС Держархіву або КСЗІ;

10) участь у роботах з модернізації ІТС Держархіву – узгодженні пропозицій з уведення до складу ІТС Держархіву нових компонентів, оновлення або заміни засобів обробки інформації тощо;

11) забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

12) проведення аналітичної оцінки поточного стану безпеки інформації в ІТС Держархіву (прогнозування виникнення нових загроз і їх урахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та інше);

13) аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів захисту інформації;

14) контроль за виконанням користувачами ІТС Держархіву вимог, норм, правил, інструкцій із захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за збереженням режиму секретності під час обробки в ІТС Держархіву інформації, що становить державну таємницю;

15) контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

16) розробка і реалізація спільно з РСО організації комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів, здійснення технічного та інформаційного забезпечення.

5. Проведення навчання користувачів ІТС Держархіву правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами.

7. Повноваження відповідального за ТЗІ

1. Відповідальний за ТЗІ має право:

1) здійснювати контроль за діяльністю працівників Державного архіву Сумської області щодо виконання ними вимог нормативно-правових актів із захисту інформації в ІТС Держархіву;

2) подавати директору архіву пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки у випадку виявлення порушень політики безпеки або реальних загроз її порушення;

3) інформувати керівництво архіву про факти виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;

4) ініціювати проведення службових розслідувань у випадках виявлення порушень;

5) готувати пропозиції з обґрунтуваннями щодо залучення на договірній основі до виконання робіт із захисту інформації інших організацій, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації;

6) готувати пропозиції щодо забезпечення КСЗІ необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні, з метою забезпечення інформаційної безпеки;

7) подавати пропозиції щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;

8) узгоджувати умови включення до складу ІТС Держархіву нових компонентів та подавати пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів ІТС Держархіву;

2. Відповідальний за ТЗІ зобов'язаний:

1) організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації в ІТС Держархіву;

2) вчасно і в повному обсязі доводити до користувачів ІТС Держархіву інформацію про зміни в галузі захисту інформації, які їх стосуються;

3) перевіряти на відповідність внутрішній політиці безпеки прийняті правила та інструкції щодо обробки інформації, здійснювати контроль за виконанням цих вимог;

4) здійснювати перевірки стану захищеності інформації в ІТС Держархіву;

5) забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, установлених в ІТС Держархіву;

6) сприяти і, у разі необхідності, брати безпосередню участь у проведенні уповноваженими органами перевірок стану захищеності інформації в ІТС Держархіву;

7) сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої на договірних, контрактних або інших підставах від організацій-партнерів та приватних осіб;

8) негайно інформувати керівництво архіву про виявлені атаки та викритих порушників.

3. Відповідальний за ТЗІ несе відповідальність згідно із законодавством України за невиконання або неналежне виконання своїх обов'язків та допущені ними порушення встановленого порядку захисту інформації в ІТС Держархіву.

4. Відповідальний за ТЗІ відповідає за:

1) організацію робіт із захисту інформації в ІТС Держархіву, ефективність захисту інформації відповідно до чинних нормативно-правових актів;

2) своєчасне виконання плану захисту інформації в ІТС Держархіву;

3) додержання вимог нормативних документів, що визначають порядок організації робіт із захисту інформації, інформаційних ресурсів та технологій;

4) повноту та якість розроблення і впровадження організаційно-технічних заходів із захисту інформації в ІТС Держархіву, точність та достовірність отриманих результатів і висновків з питань, що належать до його компетенції;

5) якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок.

8. Забезпечення діяльності відповідального за ТЗІ

1. Відповідальний за ТЗІ здійснює роботу з реалізації основних організаційних та організаційно-технічних заходів зі створення і забезпечення функціонування КСЗІ відповідно до плану робіт, який затверджується керівником архіву.

2. З метою забезпечення конфіденційності робіт відповідальний за ТЗІ дає зобов'язання щодо нерозголошення відомостей, що становлять службову або іншу таємницю, які стали йому відомими в період виконання своїх обов'язків.

3. Відповідальний за ТЗІ взаємодіє з:

1) відділом інформаційно-комп'ютерного забезпечення апарату Сумської обласної державної адміністрації з питань захисту інформації або її автоматизованої обробки;

2) зовнішніми організаціями, які є виконавцями робіт;

3) іншими суб'єктами діяльності у сфері захисту інформації.

4. Відповідальний за ТЗІ узгоджує свою діяльність з:

1) РСО;

2) органами Державної служби спеціального зв'язку та захисту інформації України.

4. Матеріально-технічну базу для забезпечення ТЗІ складають засоби захисту інформації, програмне забезпечення, технічне та інженерне обладнання, засоби контролю, відповідна документація, а також інші засоби і обладнання.

Провідний архівіст
відділу організаційної, кадрової
та режимно-секретної роботи **Олексій ПІСКУНОВ**