ЗАТВЕРДЖЕНО
Наказ Міністерства з питань
стратегічних галузей
промисловості України
_____ № _____

Положення про службу захисту інформації в автоматизованих системах класу «1», які призначені для обробки інформації з обмеженим доступом, що не становить державної таємниці

І. Загальні положення

1. Це Положення визначає завдання, функції, структуру служби захисту інформації (далі - СЗІ) в автоматизованих системах класу «1» (далі - АС), які призначені для обробки інформації з обмеженим доступом, що не становить державної таємниці, повноваження та відповідальність співробітників СЗІ, взаємодію з підрозділами Мінстратегпрому та іншими організаціями.

2. Метою створення СЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) в АС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проєктування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

3. СЗІ у своїй діяльності керується Конституцією України, законами України, 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 АС, календарних, перспективних та інших планів робіт в яких передбачається обробка інформації з обмеженим доступом, що не становить державної таємниці, затверджених керівником Мінстратегпрому.

4. У своїй роботі СЗІ взаємодіє з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

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

5. Істотні зміни до цього положення вносяться наказами Мінстратегпрому.

ІІ. Завдання СЗІ

1. Основними завданнями СЗІ є:

дослідження технології обробки інформації в АС з метою виявлення можливих каналів витоку інформації та інших загроз для безпеки інформації, формування моделі загроз, розробка політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

організація та координація робіт, пов'язаних із захистом інформації в АС, необхідність захисту якої визначається чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

організація робіт із створення та використання КСЗІ на всіх етапах життєвого циклу АС;

розроблення проєктів нормативних і розпорядчих документів, організаційно-технічних та інших документів, згідно з якими повинен забезпечуватись захист інформації в АС;

участь в організації навчання користувачів АС з питань захисту інформації при роботі в АС;

повсякденний контроль за забезпеченням захищеності ІзОД під час її обробки в АС.

ІІІ. Функції СЗІ

1. Під час створення КСЗІ СЗІ виконує такі функції:

визначення переліку відомостей, що підлягають захисту в процесі обробки в АС;

визначення порядку введення (виведення) та використання інформації в АС;

розробка 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 проєктування та розробки КСЗІ, безпосередня участь у проєктних роботах з створення КСЗІ;

участь у випробуваннях КСЗІ та проведенні її експертизи на відповідність вимогам нормативних документів з питань захисту інформації, введенні АС в експлуатацію;

участь у розробці нормативних документів, організаційно-технічних та інших документів, чинних у межах АС, які визначають правила доступу користувачів до ресурсів АС, порядок, норми, правила щодо захисту інформації та здійснення контролю за їх дотриманням;

2. Під час експлуатації КСЗІ СЗІ виконує такі функції:

організація процесу керування роботою АС (встановлення параметрів конфігурації системи;

контроль за вмістом змінних машинних носіїв;

зміна, у разі необхідності, власника документів; встановлення та зміна паролю, який захищає доступ до апаратних налаштувань; відстеження та аналіз критичних із точки зору безпеки подій;

контроль за функціонуванням КСЗІ та її компонентів, щоденний аналіз звітів про помилки та небезпечні події;

організація та проведення заходів оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій;

вжиття заходів у разі виявлення спроб несанкціонованого доступу, порушення правил експлуатації засобів захисту та інших порушень;

швидке реагування на вихід засобів захисту з ладу або порушення режимів функціонування АС;

організація та координація, у разі необхідності, ремонтних робіт технічних засобів з урахуванням вимог забезпечення захищеності інформації;

участь у роботах із модернізації АС, а саме: узгодження пропозицій щодо введення до складу АС нових компонентів, нових функціональних задач і режимів обробки інформації, заміни засобів обробки інформації тощо;

контроль за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за забезпеченням захищеності інформації у разі обробки в АС інформації, що становить ІзОД.

IV. Повноваження і відповідальність СЗІ

1. З метою виконання покладених завдань СЗІ має право:

здійснювати контроль за діяльністю користувачів АС щодо дотримання ними вимог нормативно-правових актів із питань захисту інформації під час обробки ІзОД;

подавати керівництву Мінстратегпрому пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушення політики безпеки або у випадку виникнення реальної загрози порушення безпеки;

складати і подавати керівництву Мінстратегпрому акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їх усунення;

готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій, які мають ліцензію на відповідний вид діяльності;

узгоджувати умови включення до складу АС нових компонентів та подавати керівництву Мінстратегпрому пропозиції щодо заборони їх включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів АС;

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.

2. Обов’язки СЗІ:

відстежувати всі зміни у нормативно-законодавчій базі з питань захисту інформації, перевіряти відповідність прийнятих в АС правил обробки інформації чинній нормативно-законодавчій базі з питань захисту інформації;

забезпечувати повне та якісне виконання заходів щодо захисту інформації в АС;

проводити експлуатацію КСЗІ відповідно до експлуатаційних документів;

здійснювати контрольні перевірки стану захищеності інформації в АС, сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в АС;

вести облікові картки користувачів та базу даних захисту;

вчасно і в повному обсязі повідомляти користувачів і персонал АС про зміни їх повноважень щодо доступу до інформації та зміни у нормативно-законодавчій базі з питань захисту інформації у частині, що їх стосується;

негайно повідомляти керівництву Мінстратегпрому про виявлені атаки та викриття порушників;

вживати заходи щодо забезпечення схоронності ІзОД у разі виникнення надзвичайних ситуацій;

забезпечувати конфіденційність робіт щодо монтажу, експлуатації та технічного обслуговування встановлених засобів захисту інформації.

3. Відповідальність за діяльність СЗІ покладається на її керівника.

4. Керівник СЗІ несе відповідальність за:

організацію робіт із захисту інформації в АС відповідно до чинних нормативно-законодавчих документів;

своєчасне розроблення і виконання плану захисту інформації в АС;

проведення експлуатації КСЗІ відповідно до експлуатаційних документів;

правильне оформлення та ведення службової документації КСЗІ;

навчання користувачів АС із питань захисту інформації;

ведення бази даних захисту;

встановлення параметрів роботи комплексу засобів захисту;

контроль за виконанням дій, які прямо чи опосередковано можуть вплинути на захищеність інформації;

своєчасне подання керівництву даних щодо виявлених порушень політики безпеки та рекомендації щодо їх усунення.

5. Співробітники СЗІ відповідають за належне виконання своїх функціональних обов'язків, своєчасне та якісне виконання доручень керівництва Мінстратегпрому та керівника СЗІ.

V. Взаємодія СЗІ з структурними підрозділами Мінстратегпрому та зовнішніми організаціями

1. Керівник Мінстратегпрому визначає перелік користувачів, які будуть працювати в АС.

2. СЗІ взаємодіє з структурними підрозділами Мінстратегпрому, які забезпечують дотримання вимог захищеності інформації під час роботи з ІзОД згідно з Інструкцією № 736.

3. СЗІ взаємодіє із зовнішніми організаціями, що займаються питаннями захисту інформації.

VI. Структура СЗІ

1. Структура СЗІ, її склад і чисельність визначається фактичними потребами АС щодо виконання вимог політики безпеки інформації. Особовий склад СЗІ визначається та затверджується наказом Мінстратегпрому.

2. Штат СЗІ комплектується спеціалістами, які мають 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.

3. Безпосереднє керівництво роботою СЗІ здійснює її керівник. На час відсутності керівника СЗІ (у зв’язку з відпусткою, службовими відрядженнями, хворобою тощо) його обов’язки тимчасово виконує адміністратор безпеки.

Начальник Відділу ІТ-підтримки
та захисту інформації **Олександр КУЗЬМЕНКО**