



НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

**Типове положення
про службу захисту інформації в
автоматизованій системі**

Департамент спеціальних телекомунікаційних систем та захисту
інформації Служби безпеки України

Київ 2000

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту спеціальних
телекомунікаційних систем та
захисту інформації Служби безпеки
України

від “ 04 ” грудня 2000 р. № 53

**Типове положення
про службу захисту інформації в
автоматизованій системі**

НД ТЗІ 1.4-001-2000

ДСТСЗІ СБ України

Передмова

1 РОЗРОБЛЕНО та ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

2 ВВЕДЕНО ВПЕРШЕ

Цей документ не може бути повністю чи частково відтворений, тиражований і розповсюджений без дозволу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

Зміст

1	Галузь використання	4
2	Нормативні посилання	4
3	Визначення	5
4	Позначення та скорочення	5
5	Призначення та структура	5
6	Загальні положення	6
7	Завдання служби захисту інформації	7
8	Функції служби захисту інформації	8
8.1	Функції під час створення комплексної системи захисту інформації:	8
8.2	Функції під час експлуатації комплексної системи захисту інформації:	9
8.3	Функції з організації навчання персоналу з питань забезпечення захисту інформації:	10
9	Повноваження та відповідальність служби захисту інформації	10
9.1	Права	10
9.2	Обов'язки	11
9.3	Відповідальність	11
10	Взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми організаціями	12
11	Штатний розклад та структура служби захисту інформації	13
12	Організація робіт служби захисту інформації	14
13	Фінансування служби захисту інформації	15
	Додаток	16

Типове положення про службу захисту інформації в автоматизованій системі

Чинний від 2000-12-15

1 Галузь використання

Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - "Положення про службу захисту інформації в автоматизованій системі".

НД ТЗІ призначений для суб'єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов'язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

Використання цього НД ТЗІ створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації її робіт з захисту інформації впродовж всього життєвого циклу автоматизованих систем в державних органах, на підприємствах, в установах та організаціях усіх форм власності (далі – організаціях).

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

- Закон України "Про інформацію";
- Закон України "Про захист інформації в автоматизованих системах";
- Закон України "Про державну таємницю";
- Кодекс законів про працю України (КЗпП);
- Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 08.10.97 р., № 1126;
- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229;
- Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах, затверджене постановою Кабінету Міністрів України від 16.02.98 р. № 180;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22;

- НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22;

- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22;

- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22;

- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99. р. № 22.

3 Визначення

У цьому НД ТЗІ використовуються терміни і визначення, що відповідають встановленим НД ТЗІ 1.1-003-99.

4 Позначення та скорочення

АС	— автоматизована система;
АРМ	— автоматизоване робоче місце;
ДКР	— дослідно-конструкторська робота;
ЕОМ	— електронно-обчислювальна машина;
ІзОД	— інформація з обмеженим доступом;
КЗпП України	— Кодекс законів про працю України;
КС	— комп'ютерна система;
КСЗІ	— комплексна система захисту інформації;
НД	— нормативний документ;
НД ТЗІ	— нормативний документ системи технічного захисту інформації;
НДР	— науково-дослідна робота;
НСД	— несанкціонований доступ;
ОС	— обчислювальна система;
ПЗ	— програмне забезпечення;
ПРД	— правила розмежування доступу;
РСО	— режимно-секретний орган;
СЗІ	— служба захисту інформації;
СКБД	— система керування базами даних;
ТЗІ	— технічний захист інформації.

5 Призначення та структура

5.1 Метою цього НД ТЗІ є надання організаціям, що володіють, користуються, розпоряджаються інформацією, що підлягає захисту згідно з нормативно-правовими актами, нормативно-методологічної бази для розроблення “Положення про службу захисту інформації в автоматизованій системі” (далі - Положення).

5.2 Цей НД ТЗІ передбачає під час розроблення Положення врахування специфіки діяльності організації, в АС якої створюється і функціонує служба захисту інформації, обсяги обробки інформації, встановлені в організації вимоги до конфіденційності, цілісності та доступності інформації, що обробляється, а також особливості технології її обробки.

Під час розроблення Положення використовуються тільки ті положення цього НД ТЗІ, які відповідають вимогам і умовам, притаманним для даної організації (АС).

5.3 В загальному випадку Положення повинно складатись з таких розділів:

- загальні положення;
- завдання служби захисту інформації;
- функції служби захисту інформації;
- повноваження і відповідальність служби захисту інформації;
- взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;
- штатний розклад та структура служби захисту інформації;
- організація робіт служби захисту інформації;
- фінансування служби захисту інформації.

В залежності від конкретних завдань і умов функціонування служби захисту інформації 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.

5.4 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.

Зміни суттєвого характеру вносяться до Положення на основі розпорядження або наказу керівника організації (підрозділу, до якого структурно входить СЗІ).

6 Загальні положення

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

6.2 СЗІ є штатним підрозділом організації (АС).

Або:

СЗІ є позаштатним підрозділом організації (АС).

СЗІ є самостійним структурним підрозділом з безпосередньою підпорядкованістю керівнику (заступнику керівника) організації.

Або:

СЗІ є структурною одиницею (підрозділу ТЗІ, служби безпеки, ...) організації.

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

6.3 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, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

6.4 Правову основу для створення і діяльності СЗІ становлять Закон України "Про захист інформації в автоматизованих системах", Положення про технічний захист інформації в Україні, Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах.

6.5 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 автоматизованій системі", календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) організації.

6.6 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.

6.7 У своїй роботі СЗІ взаємодіє з підрозділами організації (РСО, службою безпеки, підрозділом ТЗІ та ін.), 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.

7 Завдання служби захисту інформації

Завданнями СЗІ є:

- 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 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 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 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.

8 Функції служби захисту інформації

8.1 Функції під час створення комплексної системи захисту інформації:

- 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 організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією 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 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 організації) погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);
- участь у розробці нормативних документів, чинних у межах організації і АС, 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 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 та ін.).

8.2 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 – паролів, привілеїв, ключів та ін.);
- супроводження і актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об'єктів, ідентифікатори користувачів 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 в роботах з модернізації АС - узгодженні пропозицій з введення до складу АС 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 АС (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 та ін.);
- інформування власників 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;
- регулярне подання звітів керівництву організації-власника (розпорядника) АС про виконання користувачами АС вимог з захисту інформації;
- аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для організації;
- 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 режиму секретності у разі обробки в АС 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 та ін., здійснення їхнього технічного та інформаційного забезпечення.

8.3 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 організації (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, 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 та ін.

9 Повноваження та відповідальність служби захисту інформації

9.1 Права

ЗІ має право:

- здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (АС) 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 (АС), 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, які мають ліцензії на відповідний вид діяльності;
- 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;
- 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 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 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 АС сторонніми особами;
- інші права, які надані СЗІ у відповідності з специфікою та особливостями діяльності організації (АС).

9.2 Обов'язки

СЗІ зобов'язана:

- організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з 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 (організації) 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 (організації);
- сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в АС;
- 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 (інший термін), подавати керівництву організації звіт про стан захищеності інформації в АС і дотримання користувачами та персоналом АС встановленого порядку і правил захисту інформації;
- негайно повідомляти керівництво АС (організації) про виявлені атаки та викритих порушників;
- Інші обов'язки, покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності АС (організації).

9.3 Відповідальність

9.3.1 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 посадовими (функціональними) інструкціями.

9.3.2 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 керівником організації;

- координацію планів діяльності підрозділів та служб АС (організації) з питань захисту інформації;

- створення системи навчання співробітників, користувачів, персоналу АС з питань захисту інформації;

- виконання особисто та співробітниками СЗІ розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

9.3.3 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 АС (організації).

10 Взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми організаціями

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

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

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

- РСО організації;

- підрозділом ТЗІ організації;

- адміністрацією АС та іншими підрозділами організації, виробнича діяльність яких пов'язана з захистом інформації або її автоматизованою обробкою;

- службою безпеки організації;

- зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;

- підрозділами служб безпеки іноземних фірм (що є для організації партнерами, користувачами, постачальниками, виконавцями робіт), їхніми представництвами (на договірних або інших засадах);

- іншими суб'єктами діяльності у сфері захисту інформації.

10.3 СЗІ координує свою діяльність з аудиторською службою під час проведення аудиторських перевірок.

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

11 Штатний розклад та структура служби захисту інформації

11.1 СЗІ є штатним 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 (служби безпеки) організації.

Штатність чи позаштатність СЗІ в організації визначається рішенням загальних зборів акціонерів або керівництвом організації.

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

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

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

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 – керівник одного з підрозділів або інший кваліфікований співробітник СЗІ. Призначення на цю посаду позаштатних або тимчасово працюючих співробітників забороняється.

11.5 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.

11.6 Функціональні обов'язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом АС (організації).

11.7 В залежності від обсягів і особливостей завдань СЗІ до її складу можуть

входити спеціалісти (групи спеціалістів, підрозділи та ін.) різного фаху:

- спеціалісти з питань захисту інформації від витоку технічними каналами;
- спеціалісти з питань захисту каналів зв'язку і комутаційного обладнання, налагодження і керування активним мережевим обладнанням;
- спеціалісти з питань адміністрування засобів захисту, керування базами даних захисту;
- спеціалісти з питань захищених технологій обробки інформації.

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

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

11.9 Зміна структури СЗІ здійснюється за рішенням загальних зборів акціонерів або керівництва організації і затверджується наказом (розпорядженням) керівника організації.

12 Організація робіт служби захисту інформації

12.1 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.

12.2 СЗІ здійснює свою роботу з реалізації основних організаційних та організаційно-технічних заходів з створення і забезпечення функціонування КСЗІ у відповідності з планами робіт. Підставою для розроблення планів робіт є "План захисту інформації в АС" (див. додаток).

До планів включаться 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).

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 АС;
- 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;
- бізнес-план створення і функціонування СЗІ.

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.

12.3 Реорганізація або ліквідація СЗІ здійснюється за рішенням загальних зборів акціонерів або керівництва організації. Реорганізаційна або ліквідаційна процедура здійснюється відповідною комісією, яка створюється за наказом (розпорядженням) керівника організації.

12.4 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 службу, комерційну або іншу таємницю, і які стали їм відомими в період роботи в організації.

12.5 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 нормативних документів.

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

13 Фінансування служби захисту інформації

СЗІ фінансується за рахунок:

- коштів, що виділяються в організації на утримання органів управління;
- прибутку організації (АС) 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.

Додаток

(рекомендований)

Методичні вказівки щодо структури та змісту Плану захисту інформації в автоматизованій системі

План захисту інформації в АС є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу АС. В окремих випадках план захисту інформації в АС може оформлятися одним документом.

План захисту інформації в АС (далі – План захисту) розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої політики безпеки інформації. План захисту визначає і документально закріплює об'єкт захисту інформації в АС, основні завдання захисту, загальні правила обробки інформації в АС, мету побудови та функціонування КСЗІ, заходи з захисту інформації. План захисту має фіксувати на певний момент часу склад АС, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації та ін.

План захисту повинен регулярно переглядатися та при необхідності змінюватись.

Зміни та доповнення до Плану захисту затверджуються на тому ж рівні та в тому ж порядку, що і основний документ.

Для АС, в яких обробляється інформація, що становить державну таємницю, План захисту є обов'язковим документом. Склад і зміст Плану захисту для таких АС встановлено “Положенням про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах”.

План захисту рекомендується розробляти і для всіх інших АС, в яких обробляється інформація, що підлягає захисту згідно з законодавством України, користуючись зазначеними вимогами до його складу і змісту.

План захисту повинен складатись з наступних розділів:

- завдання захисту інформації в АС;
- класифікація інформації, що обробляється в АС;
- опис компонентів АС та технології обробки інформації;
- загрози для інформації в АС;
- політика безпеки інформації в АС;
- система документів з забезпечення захисту інформації в АС.

На підставі Плану захисту складається календарний план робіт з захисту інформації в АС.

1 Завдання захисту інформації в АС

Повинні бути визначені основні завдання і мета захисту інформації, об'єкти захисту.

1.1 Завданнями захисту інформації можуть бути:

- забезпечення визначених політикою безпеки властивостей інформації

(конфіденційності, цілісності, доступності) під час створення та експлуатації АС;

- своєчасне виявлення та знешкодження загроз для ресурсів АС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;

- створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні АС;

- ефективне знешкодження (попередження) загроз для ресурсів АС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

- керування засобами захисту інформації, керування доступом користувачів до ресурсів АС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів АС;

- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

- створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими) діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування АС.

1.2 Політика безпеки, яка реалізується КСЗІ для захисту інформації від потенційних внутрішніх та зовнішніх загроз, повинна поширюватись на наступні об'єкти захисту:

- відомості (незалежно від виду їхнього представлення), віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється в АС і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;

- інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси;

- обладнання АС та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення - робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби друку та буферизації для утворення твердих копій, накопичувачі інформації;

- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;

- користувачів (персонал) АС, власників інформації та АС, а також їхні права.

1.3 Забезпечення безпеки інформації в АС досягається:

- організацією та впровадженням системи допуску співробітників (користувачів) до роботи з інформацією, яка потребує захисту;

- організацією обліку, зберігання, обігу інформації, яка потребує захисту, та її носіїв;

- організацією і координацією робіт з захисту інформації, яка обробляється та передається засобами АС;

- здійсненням контролю за забезпеченням захисту інформації, яка обробляється засобами АС, та за збереженням конфіденційних документів (носіїв).

2 Класифікація інформації, що обробляється в АС

2.1 Повинні бути класифіковані всі відомості за режимом доступу, за правовим режимом, а також за типом їхнього представлення в АС. Класифікація є підставою для визначення власником (розпорядником) інформації або АС методів і способів захисту кожного окремого виду інформації.

2.2 За режимом доступу інформація в АС має бути поділена на:

- відкрити;
- з обмеженим доступом.

Відкрити інформацію слід поділити на відкрити, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкрити, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

2.3 За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну та конфіденційну.

До таємної інформації має бути віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю.

Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України “Про державну таємницю”.

2.4 Правила доступу до конфіденційної інформації, володіти, користуватися чи розпоряджатися якою можуть окремі фізичні, юридичні особи або держава, встановлює її власник. Конфіденційна інформація може мати велику цінність для її власника, втрата або передача якої іншим особам може завдати організації (власнику) значних збитків. З метою встановлення ПРД до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за ступенем цінності (критерії розподілу можуть бути визначені під час оцінки ризиків).

2.5 Для встановлення правил взаємодії активних і пасивних об’єктів АС інформація повинна бути класифікована за типом її представлення в АС (для кожної з визначених категорій встановлюються типи пасивних об’єктів комп’ютерної системи, якими вона може бути представлена).

3 Опис компонентів АС та технології обробки інформації

3.1 Повинна бути проведена інвентаризація усіх компонентів АС і зафіксовані всі активні і пасивні об’єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. Для кожного активного об’єкту АС має бути визначено перелік пасивних об’єктів, які з ним взаємодіють.

До об’єктів, що підлягають інвентаризації, можуть бути віднесені:

- обладнання - ЕОМ та їхні складові частини (процесори, монітори, термінали, робочі станції та ін.), периферійні пристрої;
- програмне забезпечення - вихідні, завантажувальні модулі, утиліти, СКБД, операційні системи та інші системні програми, діагностичні і тестові програми тощо;
- дані - тимчасового і постійного зберігання, на магнітних носіях, друковані, архівні і резервні копії, системні журнали, технічна, експлуатаційна і розпорядча документація та ін.;
- персонал і користувачі АС.

3.2 Окрім компонентів АС, необхідно дати опис технології обробки інформації в АС, що потребує захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних, або алгоритмів окремих процедур. Опис (як в цілому, так і для окремих компонентів) може бути неформальним або формальним.

При цьому рекомендується розробити структурну схему інформаційних потоків в АС, яка б відображала інформаційну взаємодію між основними компонентами АС (завданнями, об'єктами) з прив'язкою до кожного елемента схеми категорій інформації та визначених політикою безпеки рівнів доступу до неї.

4 Загрози для інформації в АС

4.1 Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

4.2 Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

4.2.1 Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскуванню під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

4.2.2 Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

- збої і відмови у роботі обладнання та технічних засобів АС;

- наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) АС під час експлуатації;

- навмисні дії (спроби) потенційних порушників.

4.2.3 Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керуваності АС.

4.2.4 Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неухважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних,

програм та ін.);

- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);
- наслідки некомпетентного застосування засобів захисту;
- інші.

4.2.5 Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);
- порушення режимів функціонування АС (обладнання і ПЗ);
- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскуванню під зареєстрованого користувача ("маскарад");
- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
- інші.

4.3 Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

- на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керуваності АС);
- джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

- можливі способи здійснення загроз.

4.4 У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС. Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

4.4.1 Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

4.4.2 Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

4.4.3 За рівнем знань про АС усіх порушників можна класифікувати як таких, що:

- володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;
- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;
- володіють інформацією про функції та механізм дії засобів захисту.

4.4.4 За використовуваними методами і способами порушників можна класифікувати як таких, що:

- використовують виключно агентурні методи одержання відомостей;
- використовують пасивні технічні засоби перехоплення інформаційних сигналів;

- використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;
- використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

4.4.5 За місцем здійснення дії можуть класифікуватись:

- без одержання доступу на контрольовану територію організації (АС);
- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;
- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;
- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);
- з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

5 Політика безпеки інформації в АС

5.1 Під політикою безпеки інформації (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

5.2 Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В АС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в АС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів АС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів АС політика безпеки стосується, а яких – ні).

5.3 Політика безпеки має бути розроблена таким чином, що б вона не потребувала частой модифікації (потреба частой зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АС кожного з цих видів.

5.4 Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;

- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

5.5 Політика безпеки повинна доказово давати гарантії того, що:

- в АС (в кожній окремій складовій частині, в кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування АС забезпечується оцінюваність і перевіряємість захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів АС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування АС;
- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;
- всі критичні з точки зору безпеки інформації технології (функції) АС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;
- враховані вимоги всіх документів, які регламентують порядок захисту інформації в АС (п. 6 додатку), та забезпечується їхнє суворе дотримання.

5.6 Політика безпеки розробляється на підготовчому етапі (НД ТЗІ 3.7-001-99) створення КСЗІ. Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції безпеки інформації в АС;
- аналіз ризиків;
- визначення вимог до заходів, методів та засобів захисту;
- вибір основних рішень з забезпечення безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС;
- документальне оформлення політики безпеки.

5.6.1 Концепція безпеки інформації в АС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної АС і виконується на підставі аналізу наступних чинників:

- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями АС;
- загроз, яким зазнають впливу ресурси АС, що підлягають захисту.
- За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в АС:
- мета і пріоритети, яких необхідно дотримуватись в АС під час забезпечення безпеки інформації;
- загальні напрями діяльності, необхідні для досягнення цієї мети;
- аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;
- відповідальність посадових осіб та інших суб'єктів взаємовідносин в АС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

5.6.2 Аналіз ризиків

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

5.6.2.1 Визначення компонентів і ресурсів АС, які необхідно враховувати при аналізі

Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси АС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об'єкти захисту). Для цього використовуються відомості п.3 додатку, одержані в результаті обстеження середовищ функціонування АС.

5.6.2.2 Ідентифікація загроз з об'єктами захисту

Встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) АС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс АС. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз.

5.6.2.3 Оцінка ризиків

Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

5.6.2.4 Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз

Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості АС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків - відсутня, низька, середня, висока, неприпустимо висока).

5.6.2.5 Вибір варіанту побудови КСЗІ

В залежності від конфіденційності інформації, яка обробляється в АС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника АС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти:

- досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в АС;

- досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в АС;
- досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в АС.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

5.6.2.6 Оцінювання витрат на КСЗІ

Здійснюється первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм “ефективність/вартість”), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється. Якщо залишковий ризик перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийняттого результату.

5.6.3 Визначення вимог до заходів, методів та засобів захисту

Вихідними даними є:

- завдання і функції АС;
- результати аналізу середовищ функціонування АС;
- модель загроз, модель порушників;
- результати аналізу ризиків.

На підставі цих даних визначаються компоненти АС (наприклад, окрема ЛВС, спеціалізований АРМ, Internet-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в АС.

Для кожного компонента та (або) АС в цілому формується перелік необхідних функціональних послуг захисту від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг (згідно з НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99). Визначені вимоги складають профіль захищеності інформації в АС (компоненті).

Для кожного компонента та (або) АС в цілому визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами.

5.6.4 Вибір основних рішень з забезпечення безпеки інформації

Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях:

- правовому;
- організаційному;
- технічному.

5.6.4.1 На правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

- системи нормативно-правового забезпечення робіт з захисту інформації в АС (організації);
- підтримки керівництвом організації заходів з забезпечення безпеки інформації в АС (організації), виконання правових та (або) договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників СЗІ;

- процедур доведення до персоналу і користувачів АС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

- системи контролю за своєчасністю, ефективністю і повнотою реалізації в АС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

5.6.4.2 На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

- застосування режимних заходів на об'єктах АС;
- забезпечення фізичного захисту обладнання АС, носіїв інформації, інших ресурсів;
- організації проведення обстеження середовищ функціонування АС;
- порядку виконання робіт з захисту інформації, взаємодії з цих питань з іншими суб'єктами системи ТЗІ в Україні;

- виконання робіт з модернізації АС (окремих компонентів);
- регламентації доступу сторонніх користувачів до ресурсів АС;
- регламентації доступу власних користувачів і персоналу до ресурсів АС;
- здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.);

- реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до АС, використання мереж передачі даних загального користування, зокрема Internet, використання несертифікованого ПЗ та ін.).

5.6.4.3 На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації. Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

- інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти АС, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

- реєстрація санкціонованих користувачів АС, авторизація користувачів в системі;
- керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

- виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

- перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в АС;

- забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;

- резервне копіювання критичних даних, супроводження архівів даних і ПЗ;

- відновлення роботи АС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;

- захист ПЗ, окремих компонентів і АС в цілому від внесення несанкціонованих доповнень і змін;

- забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

5.6.5 Організація проведення відновлювальних робіт і забезпечення неперервного функціонування АС

5.6.5.1 Повинні бути вироблені підходи щодо планування і порядку виконання

відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування АС в захищеному режимі. Під час планування цих робіт рекомендується враховувати наступні питання:

- виявлення критичних з точки зору безпеки процесів у роботі АС;
- визначення можливого негативного впливу надзвичайних ситуацій на роботу АС;
- визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;
- підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

5.6.5.2 План проведення відновлювальних робіт і забезпечення неперервного функціонування АС повинен описувати дії щодо улагодження інцидента, дії щодо резервування, дії щодо відновлення. Він включає в себе:

- опис типових надзвичайних ситуацій, які потенційно найбільш можливі в АС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;
- опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;
- опис процедур тимчасового переведення АС або окремих її компонентів на аварійний режим роботи;
- опис процедур поновлення нормальної виробничої діяльності АС або окремих її компонентів;
- порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

5.6.5.3 План проведення відновлювальних робіт і забезпечення неперервного функціонування АС підлягає перегляду у разі виникнення істотних змін в АС. Такими змінами можуть бути:

- встановлення нового обладнання або модернізація існуючого, включення до складу АС нових компонентів;
- встановлення нових систем життєзабезпечення АС (сигналізації, вентиляції, пожежогашіння, кондиціонування та ін.);
- проведення будівельно-ремонтних робіт;
- організаційні зміни у структурі АС, виробничих процесах, процедурах обслуговування АС;
- зміни у технології обробки інформації;
- зміни у програмному забезпеченні;
- будь-які зміни у складі і функціях КСЗІ.

5.7 Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів АС, складають правила розмежування доступу (ПРД). ПРД - це певним абстрактним механізмом, який виступає посередником при будь-яких взаємодіях об'єктів АС і є найбільш суттєвим елементом політики безпеки.

5.7.1 Як приклад, загальні ПРД можуть бути наступними (за припущення, що в АС визначено такі ієрархічні ролі – адміністратор безпеки АС, адміністратор, користувач):

- кожне робоче місце повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;
- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів АС, керування механізмами захисту здійснюється адміністратором безпеки АС;

- для попередження поширення комп'ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ – користувачі, адміністратор, в АС - адміністратор безпеки АС. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);
- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки АС. Такі роботи виконуються за його дозволом;
- кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки АС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;
- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів АС;
- атрибути користувачів періодично змінюються, а невикористовувані і скомпрометовані – видаляються;
- процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізatori трафіку, аналізatori безпеки мереж, засоби адміністрування та ін.), авторизовані і здійснюються під контролем адміністратора безпеки АС;
- усі користувачі повинні знати “Інструкцію користувача” (пройти відповідний курс навчання, скласти іспит);
- адміністратор безпеки АС і адміністратори повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

5.7.2 Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

5.8 Документальне оформлення політики безпеки

Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в АС. Структурно до політики безпеки (документів, що її складають) повинні входити наступні розділи:

- загальний, у якому визначається відношення керівництва АС (організації) до проблеми безпеки інформації;
- організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки та ін.);
- класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в АС, та необхідний рівень їхнього захисту;
- розділ, у якому визначаються ПРД до інформації;
- розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;
- розділ, у якому висвітлюються питання фізичного захисту;
- розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;
- розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;
- розділ, який регламентує порядок проведення відновлювальних робіт і

забезпечення неперервного функціонування АС;

- юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

6 Система документів з забезпечення захисту інформації в АС

Захист інформації в АС регламентується:

- законами України, іншими нормативно-правовими актами України;
- державними стандартами та іншими нормативними документами з стандартизації;
- нормативно-правовими актами і нормативними документами системи технічного захисту інформації в Україні;
- нормативними документами, що містять вимоги з захисту інформації в АС міністерств та інших центральних органів виконавчої влади, чинність яких поширюється на сферу управління цього органу;
- нормативними, організаційно-розпорядчими та іншими документами, чинними у межах АС або організації.

6.1 Закони України, інші нормативно-правові акти України, державні стандарти, нормативно-правові акти і нормативні документи системи технічного захисту інформації в Україні формують та впроваджують єдиний в державі порядок забезпечення захисту інформації в АС.

6.2 Нормативні документи з захисту інформації міністерств та інших центральних органів виконавчої влади, а також нормативні документи з стандартизації, що не є державними стандартами, враховують особливості, що існують у галузі.

6.3 Нормативні, організаційно-розпорядчі та інші документи, що використовуються у межах окремої організації або АС, враховують особливості та умови технології обробки інформації в цій організації або АС. Ці документи розробляються організацією, що є власником або розпорядником АС.

Такими документами можуть бути:

- положення про захист інформації в АС, положення про службу захисту інформації в АС, інші документи, що входять до Плану захисту інформації.;
- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту, інструкції про порядок введення в експлуатацію КСЗІ, про порядок її модернізації, про порядок обробки ІзОД в АС, про порядок використання криптографічних засобів та ін.;
- правила управління паролями в АС, правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу;
- інструкції, що встановлюють повноваження та відповідальність персоналу і користувачів;
- плани виконання робіт або здійснення окремих заходів з захисту інформації в АС.

Розробленню підлягають документи, визначені політикою безпеки інформації. При розробленні цих документів дозволяється поєднувати декілька з них у вигляді окремих розділів в одному документі.

7 Календарний план робіт з захисту інформації в АС

На підставі Плану захисту інформації в АС складається календарний план робіт з реалізації заходів захисту інформації в АС, який може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи.
- робота з кадрами.

7.1 Організаційні заходи з захисту інформації - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення захисту інформації. До плану можуть включатись заходи щодо:

- розробки документів (інструкцій, методик, правил, розпоряджень тощо) з різних напрямів захисту інформації в АС;
- внесення змін та доповнень до чинних в АС документів з урахуванням зміни умов (обставин);
- розробки та впровадження нових організаційних заходів з захисту інформації;
- обґрунтування необхідності застосування та впровадження нових засобів захисту інформації;
- координації робіт та взаємодії з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу АС;
- розгляду результатів виконання затверджених заходів та робіт з захисту інформації;
- інші.

7.2 До контрольно-правових заходів можуть бути віднесені:

- контроль за виконанням персоналом (користувачами) вимог відповідних інструкцій, розпоряджень, наказів;
- контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
- контроль за станом зберігання та використання носіїв інформації на робочих місцях;
- інші.

7.3 До профілактичних слід відносити заходи, спрямовані на формування у персоналу (користувачів) мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт та ін., а також на формування відповідного морально-етичного стану в колективі.

7.4 До інженерно-технічних слід відносити заходи, спрямовані на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування апаратних і програмних засобів захисту інформації від НСД, засобів захисту інформації від загроз її витоку технічними каналами, інженерне обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації, у тому числі в процесі капітального будівництва тощо.

7.5 Планування роботи з кадрами включає заходи з підбору та навчання персоналу

(користувачів) встановленим правилам безпеки інформації, новим методам захисту інформації, підвищення їхньої кваліфікації. Навчання персоналу (користувачів) може здійснюватись власними силами, з залученням спеціалістів зовнішніх організацій або в інших організаціях. Навчання повинно здійснюватися згідно з програмою, затвердженою керівництвом організації (АС). Навчальні програми повинні мати теоретичний і практичний курси. Доцільність і необхідність включення до програм окремих розділів визначається особливостями АС і технологіями захисту інформації, що використовуються в ній, функціональними завданнями спеціалістів, що входять до складу навчальних груп та іншими чинниками.