МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
Кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Організаційне забезпечення захисту інформації. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 38 с.

Укладачі: КОРНІЄНКО СВІТЛАНА ПЕТРІВНА, доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук, доцент;
СИНЕНКО МАРИНА АНАТОЛІЇВНА, доцент кафедри кібербезпеки та математичного моделювання, кандидат фізико-математичних наук, доцент;
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор;
МЕХЕД ДМИТРО БОРИСОВИЧ, доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук, доцент

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – ПЕТРЕНКО ТАРАС АНАТОЛІЙОВИЧ,
доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук

ЗМІСТ

ПЕРЕДМОВА 4
1. РОЗРОБКА ПЛАНУ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ 9
2. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В АС 12
3. ОПИС КОМПОНЕНТІВ АС ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ 13
4. АНАЛІЗ РИЗИКІВ ТА ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ В АС 14
5. ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В АС 21
6. АНАЛІЗ І КОРИСТУВАННЯ СИСТЕМОЮ ДОКУМЕНТІВ З ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АС 34
7. РОЗРОБКА КАЛЕНДАРНОГО ПЛАНУ РОБІТ З ЗАХИСТУ ІНФОРМАЦІЇ В АС 35
СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ 38

ПЕРЕДМОВА

Метою викладання навчальної дисципліни «Організаційне забезпечення захисту інформації» є надання здобувачам вищої освіти знань з організаційних основ забезпечення інформаційної безпеки об’єктів інформатизації, принципів системного підходу до вирішення задачі забезпечення безпеки інформації, організаційно-правового забезпечення робіт з захисту інформації.

Основними завданнями вивчення дисципліни «Організаційне забезпечення захисту інформації» є закладення у студентів знань та умінь застосовувати діючу законодавчу базу в галузі інформаційної безпеки, необхідних для професійної діяльності, включаючи вміння впроваджувати організаційні заходи на об’єктах інформаційної діяльності на підприємствах та установах різної форми власності.

Під час вивчення дисципліни здобувач вищої освіти має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

Під час вивчення дисципліни здобувач вищої освіти має використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; використовувати сучасне програмно-апаратне забезпечення інформаційно комунікаційних технологій.

Згідно з вимогами освітньо-професійної програми здобувачі вищої освіти повинні:

знати:

- основні концептуальні положення системи захисту інформації;
- правову та організаційну основи забезпечення інформаційної безпеки;

- класифікацію загроз конфіденційній інформації;
- умови, що сприяють неправомірному оволодінню конфіденційною інформацією;
- особливості законодавчого рівня забезпечення інформаційної безпеки:
- особливості адміністративних методів захисту Інформації;
- особливості організаційних заходів щодо захисту інформації;
- особливості інженерно-технічного рівня захисту інформації;
- зміст правил автентифікації інформації і користувачів.

вміти:

- визначати загрози конфіденційній інформації;
- застосовувати положення правових актів для забезпечення інформаційної безпеки підприємства;
- розробляти основні положення політики безпеки і програму її реалізації;
- здійснювати ефективний контроль робіт із захисту інформації, реєструвати порушення режиму безпеки і складати звіти;
- планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем		Кількість годин для денної/заочної форми навчання									
		Всього		У тому числі							
				Лек.		Пр.		Лаб.		С.р.	
1	2	3	4	5	6	7	8	9	10	11	12
Змістовий модуль 1. Основні положення щодо організації системи захисту інформації.											
1	Базові терміни та визначення. Основні задачі забезпечення інформаційної безпеки. Джерела загроз інформаційній безпеці.	15		2		2				11	
2	Визначення інформаційних ресурсів, що підлягають захисту.	15		2		2				11	
Разом за змістовим модулем 1		**30**		**4**		4				**22**	
Змістовий модуль 2. Концепція побудови системи безпеки підприємства.											
3	Фізичний захист інформації.	15		2		2				11	
4	Організація допуску та доступу персоналу до конфіденційної інформації.	15		2		2				11	
5	Захист конфіденційної інформації.	15		2		2				11	
Разом за змістовим модулем 2		**45**		**6**		**6**				**33**	
Змістовий модуль 3. Служба захисту інформації підприємства.											
6	Організаційне забезпечення безпеки інформації обмеженого доступу	15		2		-				13	
7	Організація та функції служби захисту інформації підприємства.	15		2		2				11	
8	Організація контролю за безпекою інформації.	15		2		2				11	
Разом за змістовим модулем 3		**45**		**6**		**4**				**35**	
Усього годин за дисципліну		**120**		**16**		**14**				**90**	

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	Розробка плану захисту інформації в автоматизованій системі .	2
2	Класифікація інформації, що обробляється в АС.	2
3	Опис компонентів АС та технології обробки інформації.	2
4	Аналіз ризиків та загроз для інформації в АС	2
5	Формування політики безпеки інформації в АС	2

6	Аналіз і користування системою документів з забезпечення захисту інформації в АС.	2
7	Розробка календарного плану робіт з захисту інформації в АС .	2
Разом:		14

САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1	Нормативно-правова база України у сфері ОЗЗІ.	11
2	Державна таємниця і конфіденційна інформація, що є власністю держави. Звід відомостей, що становлять державну таємницю.	11
3	Види об'єктів захисту. Основні напрямки організаційного захисту інформації на підприємстві.	11
4	Розголошення інформації, яка захищається. Способи запобігання розголошення інформації, яка захищається	11
5	Комерційна таємниця та порядок її визначення. Організація робіт з інформацією, яка є комерційною таємницею.	11
6	Організація внутрішньооб'єктного режиму на підприємстві. Організація охорони об'єктів підприємства. Організація інженерно-технічної безпеки.	13
7	Організація інформаційно-аналітичної роботи. Етапи виконання інформаційно-аналітичних досліджень виробничих ситуацій. Методи виконання аналітичних досліджень.	11
8	Організація роботи з персоналом підприємства Підбір та підготовка кадрів. Перевірка персоналу на благонадійність. Укладання контрактів та домовленостей про секретність. Особливості звільнення співробітників, які володіють конфіденційною інформацією.	11
Разом:		90

1. РОЗРОБКА 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.

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:

- відкриту;
- з обмеженим доступом.

Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, 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. АНАЛІЗ РИЗИКІВ ТА ЗАГРОЗ 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, маскування 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 керованості АС.

4.2.4 Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, 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 маскування 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 керованості 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. ФОРМУВАННЯ ПОЛІТИКИ 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 частої модифікації (потреба частої 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 прийнятного 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 переводу 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, пожежогасіння, 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 (аналізатори трафіку, аналізатори 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. АНАЛІЗ І КОРИСТУВАННЯ СИСТЕМОЮ 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. РОЗРОБКА КАЛЕНДАРНОГО ПЛАНУ 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;
- обгрунтування 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.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна

1. Крижанівський В.Б. Безпека інформаційних систем. – Житомир: ЖДТУ, 2009. – 81 с.
2. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
3. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
4. Закон України “Про основи національної безпеки України”//
5. Урядовий кур’єр, 30 липня 2003 р.
6. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.
7. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
8. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2022 р.
9. Закон України “Про телекомунікації” від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.
10. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.
11. Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.
12. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.

Допоміжна

1. Авраменко В.Ф., Брудний Г.О.. Жлобін С.І., Лазарев Г.П.. Дорошко В.О. Правові основи охорони інформації.— К.: ТОВ «Полиграф Консалтинг». 2003.— 173 с.
2. Хорошко В.О. Основи комп’ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.
3. Коваленко М.М. Комп’ютерні віруси і захист інформації. Навчальний посібник / М.М. Коваленко. – К.: Наукова думка, 1999. – 268 с.